***Abstract*—Network security against possible attacks involves making decisions under uncertainty. Not only may one be ignorant of the place, the power or the time of potential attacks, one may also be largely ignorant of the attacker's purpose. To illustrate this phenomena this paper proposes a simple Bayesian game-theoretic model of allocating defense (scanning) effort among nodes of a network in which a network's defender does not know the adversary's motivation for intruding on the network - e.g., to bring the maximal damage to the network (for example, to steal credit card numbers or information on bank accounts stored there) or to infiltrate into the network for other purposes (for example, to corrupt nodes for a further DDoS (Distributed Denial of Service) botnet attack on servers). Due to limited defense capabilities the defender faces the dilemma of either (a) focusing on increasing defense of the most valuable nodes, and in turn, increasing the chance for the adversary to sneak into the network through less valuable nodes, or (b) taking care of defense of all the nodes, and in turn, reducing the level of defense of the most valuable ones. An explicit solution to this dilemma is suggested based on the information available to the defender, and it is shown how this information allows the authorities to increase the efficiency of a network's defense. Some interesting properties of the rivals' strategies are presented. Notably, the adversary's strategy has a node-sharing structure and the adversary's payoffs have a discontinuous dependence on the probability of the attack's type. This discontinuity implies that the defender has to take into account the human factor since some threshold values of this inclination in the adversary's behavior could make the defender's policy very sensitive to small perturbations, while in other situations it produces minimal impact.**

***Index Terms*—Bayesian equilibrium, Network Protection, Search, Scan, Computer networks, Infrastructure networks.**

Incorporating Attack-Type Uncertainty into Network Protection

Andrey Garnaev* *Member, IEEE*, Melike Baykal-Gursoy†, and H. Vincent Poor ‡ *Fellow, IEEE* * Saint Petersburg State University
St Petersburg, Russia, email: garnaev@yahoo.com †Department of Industrial and Systems Engineering, Rutgers University
New Brunswick, NJ, USA, email: gursoy@rci.rutgers.edu ‡Department of Electrical Engineering, Princeton University
Princeton, NJ, USA, email: poor@princeton.edu

I. Introduction

A danger to daily life, economic vitality and national security stems from the cyber intrusion which has increased dramatically over the last decade, disrupting critical operations, imposing high costs on the economy [1] and exposing sensitive personal and business information (say, the recent hacking of Bush family e-mails [2], theft of credit card numbers [3], and cracking into Wall Street Journal [4] and NASA computers [5], etc.).

The increasing number of successful cyber attacks calls for new approaches to developing security systems. An extended literature exists on the construction and modeling of different aspects of security systems for communication and network security [6], [7], [8], [9], [10], [11], security in wireless networks [12], [13] and cyber-security [14], [15], [16]. In [17] the readers can find a structured and comprehensive survey of the research contributions that analyze and solve security and privacy problems in computer networks via game-theoretic approaches.

Developing more reliable security systems requires developing advanced technologies and algorithms for intrusion detection. It is interesting to draw some parallels between failing to prevent cyber attacks, and the recent economic turmoil [18]. It has by now been realized that the economic models did fail to keep pace with the explosive growth in complex securities, the resulting intricate web of risk, and the dimensions of the resulting danger to the economy. However, the larger failure was human, namely, it was in how the risk models were applied, understood and managed. In this paper we show that in order for the security systems for networks to be efficient, besides improving technologically, they should also taken into account the possible human factor, namely, the motivations of the adversary to attack the network.

To demonstrate that such security systems can be more efficient than ones that do not take the adversary's objectives into account, we suggest a simple Bayesian game-theoretic model between a defender and an adversary. We focus on two types of possible threats:

(a) *Maximizing damage attacks.* Examples of such attacks can be the theft of credit card numbers [5], or corrupting nodes by key-logging bots, i.e. the bots listening for keyboard activity and reporting the keystrokes upstream to a bot herder. Some such bots can have built-in triggers to look for visits to particular websites where passwords or bank account information is entered.

(b) *Infiltration/harassment attacks.* Examples of infiltration attacks are those in which a hacker merely wants to demonstrate his or her ability to crack into a network, such as was the case in compromising the Wall Street Journal computers [4] and the NASA computers [5], or when computers are corrupted by DDoS botnets that can be further used to wage war on other computers on the Internet by completely saturating bandwidth or other resources. Another example is the cracking of the private Yahoo Mail account of Sarah Palin by a hacker shortly after midnight on September 16, 2008, [19], [20]. The hacker claimed he had read Palin's personal e-mails because he was looking for something that "would derail her campaign." However, he later confessed that he could not find any incriminating evidence. This attack on Yahoo Mail account can be considered as infiltration. The hacker was so proud about his ability to crack into a network that he bragged about his achievement on the Internet (that finally allowed the authorities to find, try and sentence him for felony). Since he has found nothing incriminating in the mailbox, perhaps one might say it even helped her election campaign. Not every infiltration attack can be so harmless. It can turn out to be damaging for the network's users as well as the network. Say, if the mailbox contained something incriminating, it could kill Sarah Palin's career, and it could also divert a lot of users from using Yahoo e-mail servers.

There is another area in which such game-theoretic models can improve the work of security, namely, infrastructure security. The September 11, 2001 attacks (which can be considered as an example of maximizing damage attacks) introduced the term *homeland security* into the public consciousness around the world. In the United States, this term is defined as "a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur" (Homeland Security Act 2002 [21]). There is an extended literature on the construction and modeling of different aspects of infrastructure security systems [22], [23], [24]. Note that in infrastructure security, the adversary can

also plan different types of attacks, say, perhaps the recent Boston Marathon bombings can be considered as an example of a harassment attack, and law enforcement may not know the exact motivation of the adversary. Such uncertainty about the type of attack can be considered as a sub-scale for threat levels which have been created to keep populations informed about the level of threat the public faces from terrorism at any given time [25]. This system helps police and other law enforcement agencies decide how to allocate their resources, e.g., police squads, video cams, sensors, etc. The threat level represents the likelihood of an attack in the near future. This paper shows that introducing into the threat levels a sub-scale specifying the likelihood of type of threat can increase efficiency of the defense's resource allocation, especially when the resources are scarce.

The organization of this paper is as follows: in Section II, we first define two auxiliary games with complete information about an attack's type. In Section III we formulate our problem with uncertainty about the attack's type and present its equilibrium strategies explicitly. In Section IV numerical illustrations are presented. Finally, in Sections V and VI discussions and the proofs of the results are offered.

II. Complete information about attack's type: two basic games

In this section and its two subsections, we describe two simple matrix games on network nodes with complete information about an attack's type. As a basic model we have in mind a computer or communication networks, nodes of which contain or transmit valuable data (which can be either stolen or eavesdropped). We assume that the network consists of N nodes. It is an abstract network composed of communication links and nodes that may contain data that need to be protected. In fact, some nodes may represent communication links. As such, the network does not correspond to any specific topology. The agent who wants to minimize the effects of an attack is called as the defender (say, it can be intrusion detection system (IDS)). The agent who wants to attack the network is called the adversary. A strategy of the defender is a normalized vector $\boldsymbol{x} = (x_1, \dots, x_N)$, where x_i is the search (scan, protection) resource (efforts) applied at node i, i.e. $\sum_{i=1}^{N} x_i = 1$. A strategy of the adversary is a normalized vector $\boldsymbol{y} = (y_1, \dots, y_N)$ where y_i is the attack resource applied to node i, i.e. $\sum_{i=1}^{N} y_i = 1$. Let $v_i(x_i, y_i)$ be the vulnerability of node i with x_i and y_i resources invested into its protection and attack. Each node is characterized by a value C_i (say, stored data). We assume that the damage to node i is equal to stolen data or casualties which is proportional to the value and vulnerability of the node: $R_i(x_i, y_i) = v_i(x_i, y_i)C_i$. We assume that the vulnerability of node i depends linearly on investments in defense and attack, namely, $v_i(x_i, y_i) = (1 - d_i x_i)y_i$, where $d_i \in (0, 1)$ is the node's defense characteristic.

A. The adversary aims to inflict the maximal damage

We consider the scenario in which the adversary wants to inflict the maximal damage to the network. The payoff to the adversary is the total damage s/he can cause, so it is

$$u_A^1(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i=1}^{N} v_i(x_i, y_i)C_i = \sum_{i=1}^{N}(1 - d_i x_i)C_i y_i \quad (1)$$

and the payoff to the defender is $u_D^1(\boldsymbol{x}, \boldsymbol{y}) = -u_A^1(\boldsymbol{x}, \boldsymbol{y})$, i.e., here we deal with a zero-sum game. This matrix game is closely related to a search matrix game suggested in [26], [27]. We assume that that the rivals know the node's values C_i and defense characteristics d_i. Recall that $(\boldsymbol{x}_*, \boldsymbol{y}_*)$ is a saddle point (Nash equilibrium) if and only if the following inequalities hold [28],

$$u_D^1(\boldsymbol{x}, \boldsymbol{y}_*) \le u_D^1(\boldsymbol{x}_*, \boldsymbol{y}_*) \le u_D^1(\boldsymbol{x}_*, \boldsymbol{y}) \text{ for any } (\boldsymbol{x}, \boldsymbol{y}).$$

As a detailed example of the payoffs to the defender and the adversary in communication networks we consider a scenario where N users within a secure area communicate with other users outside of this area. Each user employs a separate channel for communication, so that no signal interference occurs. The adversary intends to eavesdrop this communication. For a particular time slot the adversary can eavesdrop only one user. The eavesdropping capacity [13] of user i by an adversary is $\ln(1 + h_{Ei}P_i/\sigma_E^2)$ where P_i is the transmission power of user i, h_{Ei} is the channel gain and σ_E^2 is the background noise of the channel. The defender, on the other hand, can jam the eavesdropping devices by applying jamming power J for one of the channels. Thus, if the adversary eavesdrops user i and the defender jams this eavesdropping, then the eavesdropping capacity reduces to $\ln(1 + h_{Ei}P_i/(\sigma_E^2 + g_{Ei}J))$ where g_{Ei} is the fading gain. We assume that the communication is performed in low signal-to-interference-plus-noise ratio (SINR) regime, so eavesdropping capacities can be approximated by SINR, namely, by $h_{Ei}P_i/\sigma_E^2)$ and $h_{Ei}P_i/(\sigma_E^2 + g_{Ei}J)$. A strategy $\boldsymbol{x}$ of the defender presents probabilities of jamming the corresponding channels, while a strategy $\boldsymbol{y}$ of the adversary is probabilities of eavesdropping the corresponding user. The adversary wants to maximize the expected eavesdropping capacity, thus, it is given as follows

$$\begin{aligned} u_A^1(\boldsymbol{x}, \boldsymbol{y}) &= \sum_{i=1}^{N} x_i \left(\frac{h_{Ei}P_i}{\sigma_E^2 + g_{Ei}J} y_i + \sum_{j=1, j\neq i}^{N} \frac{h_{Ej}P_j}{\sigma_E^2} y_j \right) \\ &= \sum_{i=1}^{N} \frac{h_{Ei}P_i}{\sigma_E^2} y_i \left(1 - \frac{g_{Ei}J}{\sigma_E^2 + g_{Ei}J} x_i \right) \\ &= \sum_{i=1}^{N} C_i y_i (1 - d_i x_i), \end{aligned} \quad (2)$$

with

$$d_i = \frac{g_{Ei}J}{\sigma_E^2 + g_{Ei}J} \text{ and } C_i = \frac{h_{Ei}P_i}{\sigma_E^2}. \quad (3)$$

Thus, C_i is un-jammed eavesdropping capacity and d_i is the contribution of faded jamming power into the total induced noise.

B. The adversary targets to infiltrate into the network/to perform a harassment attack

In the scenario where the adversary wants to infiltrate [29] the network undetected, from the adversary's point of view all the nodes have the same value C. These nodes differ only in terms of their defense levels. Thus, the payoff to the adversary is

$$u_A^2(\boldsymbol{x},\boldsymbol{y}) = C\sum_{i=1}^{N}(1-d_ix_i)y_i. \tag{4}$$

Since the fact that the attack was successful is also most damaging for the defender we take the defender's payoff as $u_D^2(\boldsymbol{x},\boldsymbol{y}) = -u_A^2(\boldsymbol{x},\boldsymbol{y})$. Here we again have a zero-sum game. We assume that that the rivals know the value, C and defense characteristics, d_i.

Note that this game is equivalent to a diagonal matrix game [30] with $\{Cd_i\}$ allocated along the main diagonal. Games with diagonal matrices can be found in the literature in different contexts, for example, in describing bandwidth scanning strategies to detect illegal use of applications in a network [31]. The harassment/infiltration attack in the eavesdropping context corresponds to curious eavesdropping when the adversary just intends to eavesdrop without paying attention to eavesdropping capacities.

III. Uncertainty about attack's type

In this section we consider scenarios in which the defender does not know the adversary's goal: (a) to inflict the maximal damage or (b) to infiltrate the network/to perform a harassment attack. This situation could also be interpreted as that of responding to two different types of adversaries. Let the adversary's goal be to inflict the maximal damage with probability q and to infiltrate the network with probability $1-q$. Let $\boldsymbol{y}^1$ and $\boldsymbol{y}^2$ be the corresponding strategies of the adversary.

In order to solve this problem we will apply a Bayesian approach. Note that Bayesian approaches have been widely employed in dealing with different problems in networks, for example, for hiding versus search [22], intrusion detection [10], [15], scanning bandwidth [31], [32] and transmission under incomplete information [16], [33], [34].

Under the strategies of the defender, $\boldsymbol{x}$, and the adversary, $(\boldsymbol{y}^1,\boldsymbol{y}^2)$, the expected payoff to the defender is given as follows:

$$u_D(\boldsymbol{x},(\boldsymbol{y}^1,\boldsymbol{y}^2)) = qu_D^1(\boldsymbol{x},\boldsymbol{y}^1) + (1-q)u_D^2(\boldsymbol{x},\boldsymbol{y}^2). \tag{5}$$

The payoff to the adversary of type k is $u_A^k(\boldsymbol{x},\boldsymbol{y}^k)$. We assume that the rivals know the node's values C_i, the value of the infiltration attack C, defense characteristics d_i and the probability q. We look for a Bayesian equilibrium. Recall that $(\boldsymbol{x}_*,(\boldsymbol{y}_*^1,\boldsymbol{y}_*^2))$ is a Bayesian equilibrium if and only if for any $(\boldsymbol{x},(\boldsymbol{y}^1,\boldsymbol{y}^2))$ the following inequalities hold:

$$\begin{aligned} u_D(\boldsymbol{x},(\boldsymbol{y}_*^1,\boldsymbol{y}_*^2)) &\le u_D(\boldsymbol{x}_*,(\boldsymbol{y}_*^1,\boldsymbol{y}_*^2)),\\ u_A^k(\boldsymbol{x}_*,\boldsymbol{y}^k) &\le u_A^k(\boldsymbol{x}_*,\boldsymbol{y}_*^k), k=1,2. \end{aligned} \tag{6}$$

For the sake of simplicity, we assume that all the nodes have different values, i.e. $C_i \neq C_j$ for $i \neq j$. Without loss of generality, we can assume that the nodes are arranged by their values in decreasing order:

$$C_1 > C_2 > \cdots > C_N. \tag{7}$$

The following theorem gives an explicit solution of this Bayesian game.

Theorem 1: Consider the game described above. Let k be an integer such that

$$\psi_k/(\psi_k+1/C) \le q \le \psi_{k+1}/(\psi_{k+1}+1/C), \tag{8}$$

with $\{\psi_s\}_{1\le s\le N+1}$ a strictly increasing sequence defined as

$$\psi_s = \frac{\displaystyle\sum_{j=1}^{s-1}1/(d_jC_j)}{\displaystyle\sum_{j=s}^{N}(1/d_j)}, 1\le s\le N, \psi_{N+1}=\infty. \tag{9}$$

Also, let m be such that

$$\varphi_m \le 1 < \varphi_{m+1}, \tag{10}$$

with $\{\varphi_s\}_{1\le s\le N+1}$ is a strictly increasing sequence defined as

$$\varphi_s = \sum_{j=1}^{s}(C_j - C_s)/(d_jC_j), \quad 1\le s\le N, \varphi_{N+1}=\infty. \tag{11}$$

(a) Let

$$k \le m. \tag{12}$$

Then the game has a unique Bayesian equilibrium $(\boldsymbol{x},(\boldsymbol{y}^1,\boldsymbol{y}^2))$, where

$$y_i^1 = \begin{cases} \dfrac{qd_kC_k+(1-q)d_kC}{q\Psi_kd_iC_i}, & i\le k-1,\\ 1-\dfrac{qd_kC_k+(1-q)d_kC}{q\Psi_k}\displaystyle\sum_{j=1}^{k-1}\frac{1}{d_jC_j}, & i=k,\\ 0, & i\ge k+1, \end{cases}$$

$$y_i^2 = \begin{cases} 0, & i\le k-1,\\ 1-\dfrac{qd_kC_k+(1-q)d_kC}{(1-q)\Psi_k}\displaystyle\sum_{j=k+1}^{N}\frac{1}{d_jC}, & i=k,\\ \dfrac{qd_kC_k+(1-q)d_kC}{(1-q)\Psi_kd_iC}, & i\ge k+1, \end{cases} \tag{13}$$

$$x_i = \begin{cases} \dfrac{1}{d_i}\left(1+\dfrac{\left(1-\displaystyle\sum_{j=1}^{N}(1/d_j)\right)d_kC_k}{\Psi_kC_i}\right), & i\le k,\\ \dfrac{1}{d_i}\left(1+\dfrac{\left(1-\displaystyle\sum_{j=1}^{N}(1/d_j)\right)d_k}{\Psi_k}\right), & i\ge k+1, \end{cases}$$

with

$$\Psi_k = 1 + \sum_{j=1}^{k-1} \frac{d_k C_k}{d_j C_j} + \sum_{j=k+1}^{N} \frac{d_k}{d_j}. \tag{14}$$

The payoffs to the adversary and the defender under the assumption in part (a) are

$$u_A^1 = \frac{\sum_{i=1}^{N}(1/d_i) - 1}{\sum_{i=1}^{k}(1/(d_i C_i)) + \sum_{i=k+1}^{N}(1/(d_i C_k))},$$

$$u_A^2 = \frac{\left(\sum_{i=1}^{N}(1/d_i) - 1\right) C/C_k}{\sum_{i=1}^{k}(1/(d_i C_i)) + \sum_{i=k+1}^{N}(1/(d_i C_k))},$$

$$u_D = \frac{(1 - \sum_{i=1}^{N}(1/d_i))(C_k q + (1-q)C)/C_k}{\sum_{i=1}^{k}(1/(d_i C_i)) + \sum_{i=k+1}^{N}(1/(d_i C_k))}.$$

(b) Let

$$1 \le m \le k-1, \tag{15}$$

then the game has a unique equilibrium strategy for the defender and a continuum of equilibrium strategies for the adversary. Namely,

(b_1) Let $\xi_m \neq -C_m$ with

$$\xi_s = \frac{1 - \sum_{j=1}^{s}(1/d_j)}{\sum_{j=1}^{s} 1/(d_j C_j)}, \quad 1 \le s \le N. \tag{16}$$

Then, the defender and the first type adversary have unique equilibrium strategies $\boldsymbol{x}$ and $\boldsymbol{y}^1$, meanwhile the second type adversary has a continuum of equilibrium strategies $\boldsymbol{y}^2$:

$$x_i = \begin{cases} \dfrac{\dfrac{1}{d_i C_i}}{\sum_{j=1}^{m} \dfrac{1}{d_j C_j}} \left(1 - \sum_{j=1}^{m} \dfrac{C_j - C_i}{d_j C_j}\right), & i \le m, \\ 0, & i \ge m+1, \end{cases} \tag{17}$$

$$y_i^1 = \begin{cases} \dfrac{1/(d_i C_i)}{\sum_{j=1}^{m} 1/(d_j C_j)}, & i \le m, \\ 0, & i \ge m+1 \end{cases} \tag{18}$$

and $\boldsymbol{y}^2$ is any probability vector such that

$$y_i^2 \begin{cases} = 0, & i \le m, \\ \le \dfrac{q}{1-q} \dfrac{1/(d_i C)}{\sum_{j=1}^{m}(1/(d_j C_j))}, & i \ge m+1. \end{cases} \tag{19}$$

(b_2) If $\xi_m = -C_m$. Then, the game has a continuum of equilibria. Namely, the defender has the unique equilibrium strategy

$$x_i = \begin{cases} (1/d_i)\left(1 - C_m/C_i\right), & i \le m, \\ 0, & i \ge m+1 \end{cases};$$

meanwhile both types of the adversaries have continuum equilibrium strategies, namely, for harassment/infiltration type given by (19) and for maximizing damage type given as follows:

$$y_i^1 = \begin{cases} \epsilon/(d_i C_i) & i \le m-1, \\ 1 - \epsilon \sum_{j=1}^{m-1}(1/(d_j C_j)), & i = m, \\ 0, & i \ge k+1, \end{cases}$$

for any $\epsilon \in \left[1/\left(\sum_{j=1}^{m}(1/(d_j C_j))\right), 1/\left(\sum_{j=1}^{m-1}(1/(d_j C_j))\right)\right]$. Of course, these continuum of the adversary's equilibrium strategies are equivalent to each other, since they all bring the same payoff.

The payoffs to the adversary and the defender are given as follows:

$$u_A^1 = -\xi_m, \quad u_A^2 = C \text{ and } u_D = q\xi_m - (1-q)C.$$

Finally, note that since ψ_s and φ_s are increasing, by (10) the conditions (12) and (15) are equivalent respectively to

$$\varphi_k \le 1, \tag{20}$$

and

$$\varphi_k > 1. \tag{21}$$

Remark 1: Part (a) of Theorem 1: It is quite interesting that the defender's payoff depends on probability q explicitly while his strategy depends on probability q only implicitly by means of switching point k defined through equation (8). The same phenomena occurs in inverse order with the adversary, namely, the adversary's strategy depends on probability q explicitly, while his payoff depends on probability q only implicitly through k. Also, the adversary's strategies have explicitly the node sharing form, i.e., all nodes are under attack in such a way that the maximum damage attack targets the most valuable nodes, while less valuable nodes are under infiltration attack. The defender distributes defense efforts among all the nodes.

Part (b) of Theorem 1: Since ψ_s is increasing, by (8), k is decreasing on C, while, by (10), m does not depend on C. Thus, the condition (20) always holds for big enough C, while (21) does not hold. It means that the case (b) arises when the lost caused by infiltration attack (from the defender's point of view) is negligible compared to the one inflicted by the maximum damage attack. In this situation, the defender applies all defense effort as if s/he meets only with a maximum damage attack and infiltration attack is not expected at all. That is why the defender and the adversary strategies depend on probability q only implicitly by means of definition (8) of switching point k and (15).

Finally, note that the considered Bayesian game is equivalent to a zero-sum game with the same payoff to the defender as in Bayesian game. Thus, the equilibrium strategy of the defender is maximin strategy and gives the optimal behavior of the defender under the worst conditions.

IV. Numerical illustration

As a numerical example we consider jamming versus eavesdropping (2) and (3) interpretation of our model, where the adversary intends to jam eavesdropping capacities of the adversary trying to eavesdrop communication of $N = 4$ users using separate channels with other users allocated outside of the secure area. There are two types of the adversaries: maximizing eavesdropping damage adversary, and infiltration eavesdropping adversary, which correspond to the maximizing damage and harassment/infiltration attacks. We assume that the background noise is $\sigma_E^2 = 1$, channel fading gains $\{g_{Ei}, i = 1, ..., 4\} = (0.55, 0.77, 3.33, 9.9)$, faded eavesdropping power $\{h_{Ei}P_i/\sigma_E^2, i = 1, ..., 4\} = (1.7, 1.5, 0.8, 0.2)$ and $\{h_{Ei}P_i/\sigma_E^2, i = 1, ..., 4\} = (1, 1, 1, 1)$ for maximum eavesdropping and curious eavesdropping attack, respectively.

The payoff to the defender is continuous in probability q and jamming power J while the payoff to the adversary is piecewise-constant in probability q and piecewise-continuous in jamming power J (Figure 1). It is quite natural that the payoff to the defender and the adversary are increasing and decreasing on jamming power correspondingly. Of course, the payoff to the maximizing eavesdropping damage adversary is decreasing in q, since increasing q means that the defender has stronger belief that s/he meets such an adversary. The payoff to the infiltration eavesdropping adversary is increasing in q due to the same reason. It is quite interesting that the payoff to the defender in general is not monotonic with respect to probability q and can give an interior minimum on q. So, under some conditions, lack of complete information on real threat can cause a reduction in the defender's expected payoff.

The adversary, depending on the type of attack, applies channel sharing strategies (Figures 3 and 4), while the defender applies jamming effort (Figure 2) among all the channels (if the condition (12) of Theorem 1 holds) or only among the channels where maximizing eavesdropping damage attack can be inflicted (if the condition (15) of Theorem 1 holds). Figure 5(a) illustrate how the domain, where the defender has to respond to infiltration attack, increases with increasing value of such an attack. Figures 5(b) and (c) show coefficient of efficiency of the defender's strategy tuned for the possibility that both types of attacks can arise compared to the defender's strategy tuned to only one type of attack. Here the coefficient of efficiency is the ratio of the corresponding payoffs. Since defender's payoff is negative, smaller coefficient of efficiency means higher efficiency of the defender's strategy. Also, if this coefficient equals to one, then no improvements in efficiency occurs. Thus, in there domain where the condition (15) holds such coefficient versus maximizing eavesdropping damage attack equals to 1 (Figure 5(b)), since under this condition the defender does not consider infiltration attack essential and focuses on preventing only the maximizing damage attack. Coefficient of efficiency versus infiltration attack comes to 1 only when possibility of such an attack becomes dominative (so, when q is close to 0). Figure 6 illustrate how the rival's payoffs depend on the value of the infiltration attack. The expected payoff of the defender is continuous on C. Also, it shows that if the value of infiltration attack is small compared to the individual capacities of channels, then increasing the probability of the maximal damage attack, q, leads to a decrease in the defender's payoff. Alternatively, if the value of infiltration attack is large, then increasing q leads to an increase in the defender's payoff. Finally, if this quantity q has an intermediate value, then the payoff of the defender is convex in q. The payoff to the maximizing eavesdropping damage adversary is piecewise-constant, and infiltration eavesdropping adversary is piecewise-continuous on C and increasing on C. It is quite natural that it is increasing for the maximizing eavesdropping damage adversary although the payoff depends on C only implicitly. The matter is that increasing C implies that the defender has to pay more attention to the possibility of meeting infiltration type's attack, that causes the defender to become vulnerable to the maximizing damage type's attack.

V. Discussion

In this paper we have dealt with a dilemma that the defender of a network, due to limited resources, faces: either (a) to focus on increasing defense of the most valuable nodes which leads to increasing chance for the adversary to infiltrate the network through less valuable nodes, or (b) to defend all nodes while reducing the level of defense of the most valuable ones. To solve this problem most efficiently we have suggested a Bayesian game in which the probability of the attack's type can be considered as a sub-scale in the scale of threat levels. This sub-scale allows for better tuning of threat level and for more efficient allocation of the limited defense resources. We have shown that the defender has a unique equilibrium, while the adversary has a unique strategy only if all nodes are under attack. If the attacks effect only a subset of the nodes then a continuum of adversary equilibrium strategies could arise. The adversary's payoffs have a discontinuous dependence on the probability of the attack type. This discontinuity means that the defender has to take into account the human factor since some threshold values of this inclination in the adversary's behavior could increase sensitivity of the defender's strategy, while in other situations it produces only minimal impact.

Of interest for future research is an extension of this model to dynamical scenarios and the introduction of uncertainty about the attack tools employed and the number of attackers.

References

[1] Official website of the Department of Homeland Security, *Cybersecurity Overview*, 2012, http://www.dhs.gov/cybersecurity-overview

[2] Fahrenthold, D.A., Horwitz, S., *Secret Service Investigating Hack of Bush Family e-mails*. The Washington Post. Feb. 8, 2013.

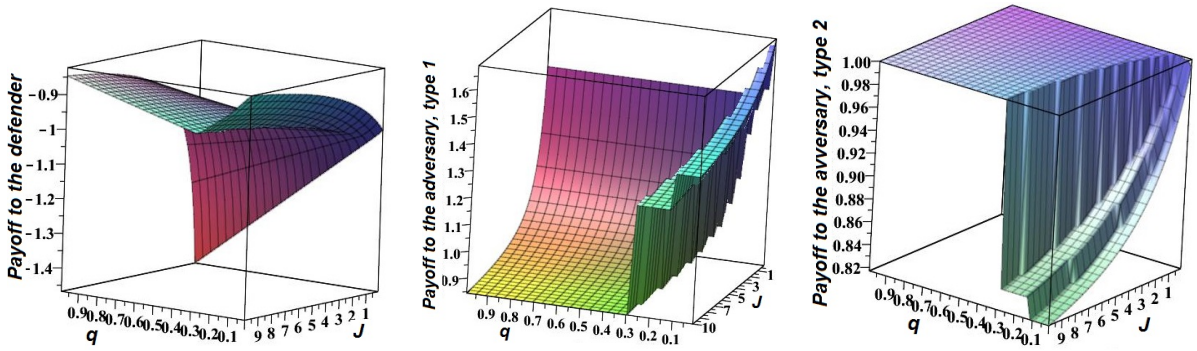
[3] Callaham, J., *50,000 credit card numbers stolen in Stratfor cyber attack*. http://www.neowin.net/news/50000-credit-card-numbers-stolen-in-stratfor-cyber-attack, Dec. 28, 2011.

[4] Mullen, J., *New York Times, Wall Street Journal say Chinese hackers broke into computers*. http://www.cnn.com/2013/01/31/tech/china-nyt-hacking, CNN, Jan. 31, 2013.

[5] *Hackers had full functional control of NASA computers. BBC News*. March 2, 2012.

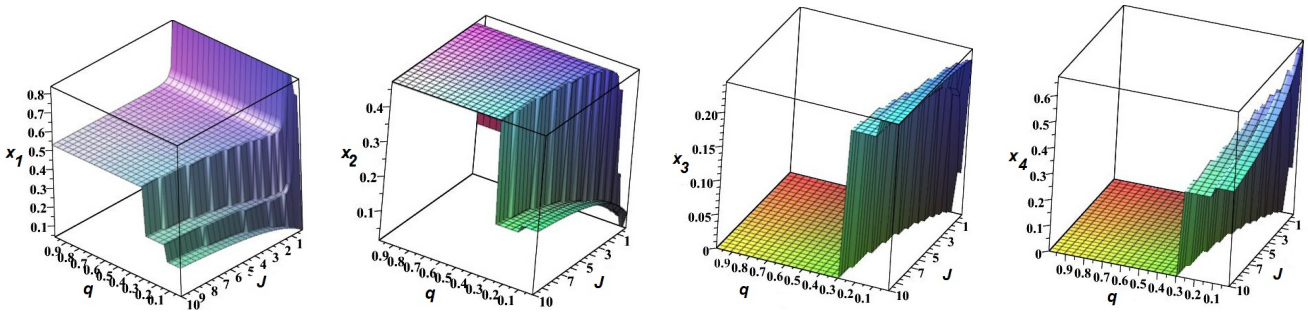
[6] Alpcan, T., and Basar, T., *A game theoretic approach to decision and analysis in network intrusion detection*. Proc. IEEE CDC 2003, pp. 2595-2600, 2003.

[7] Nguyen, K.C., Alpcan, T., and Basar, T., *Security Games with Incomplete Information*. Proc. IEEE ICC 2009, pp.1-6, 2009.



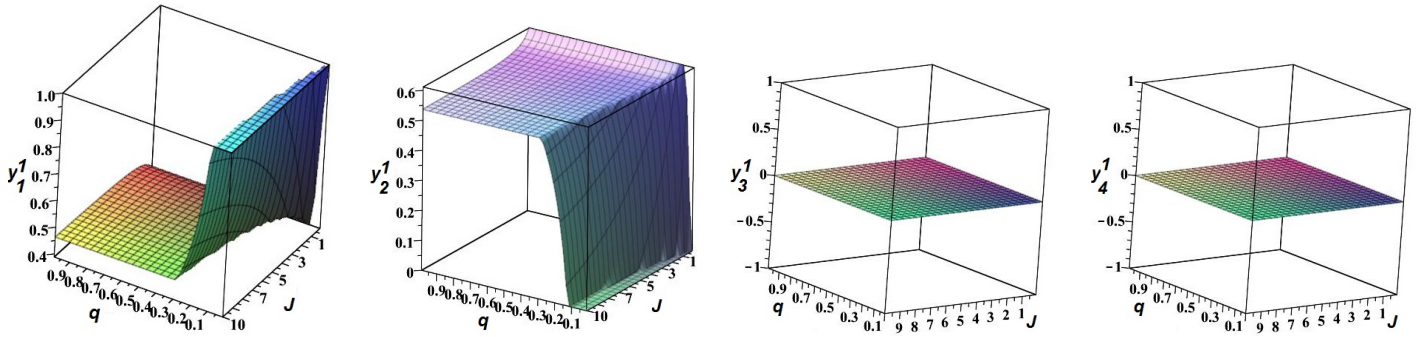
(a) (b) (c)

Fig. 1. (a) The payoff of defender, (b) The payoff of maximizing damage adversary's type, and (c) The payoff of infiltration adversary's type as functions of probability q and jamming power J



(Channel 1) (Channel 2) (Channel 3) (Channel 4)

Fig. 2. The equilibrium strategy of the defender for each channel as functions of probability q and jamming power J



(Channel 1) (Channel 2) (Channel 3) (Channel 4)

Fig. 3. The equilibrium strategy of the maximum damage adversary type for each channel as functions of probability q and jamming power J

[8] Hamilton, S.N., Miller, W.L., Ott, A., and Saydjari, O.S., *Challenges in applying game theory to the domain of information warfare*. Proc. ISW 2002.

[9] Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V., and Wu, Q., *A Survey of Game Theory as Applied to Network Security*. HICSS 2010, pp.1-10, 2010.

[10] Liu, Y., Comaniciu, C., and Man, H., *A Bayesian Game Approach for Intrusion Detection in Wireless Ad Hoc Networks*. Valuetools 2006.

[11] Comaniciu, C., Mandayam, N.B., and Poor, H.V., *Wireless Networks Multiuser Detection in Cross-Layer Design*, Springer, 2005.

[12] Mukherjee, A., and Swindlehurst, A.L. *Optimal Strategies for Countering Dual-Threat Jamming/Eavesdropping-Capable Adversaries in MIMO Channels*. Proc. IEEE MILCOM 2010, pp.1695-1700, 2010.

[13] Zhu, Q., Saad, W., Han. Z., Poor, H.V., and Basar, T., *Eavesdropping and Jamming in Next-Generation Wireless Networks: A Game-Theoretic Approach*. Proc. IEEE MILCOM 2011, pp.119-124, 2011.

[14] Kong-wei, L., and Wing, J., *Game strategies in network security*. International Journal of Information Security, 4, 2005 pp.71-86.

[15] Agah, A., Das, S.K., Basu, K., and Asadi, M., *Intrusion detection in sensor networks: A non-cooperative game approach*. Proc. IEEE NCA 2004, pp. 343–346, 2004.

[16] Han, Z., Marina, N., Debbah, M., and Hjrungnes, A., *Physical Layer Security Game: Interaction between Source, Eavesdropper, and Friendly Jammer*. EURASIP J. on Wireless Comm. and Networking, 2009.

[17] Manshaei, M.H., Zhu, Q., Alpcan, T., Basar, T., and Hubaux J.-P., *Game theory meets network security and privacy*. ACM Computing Survey, 45(3), 2013.

[18] Lohr, S., *In Modeling Risk, the Human Factor Was Left Out*. The New York Times, Nov. 4, 2008.

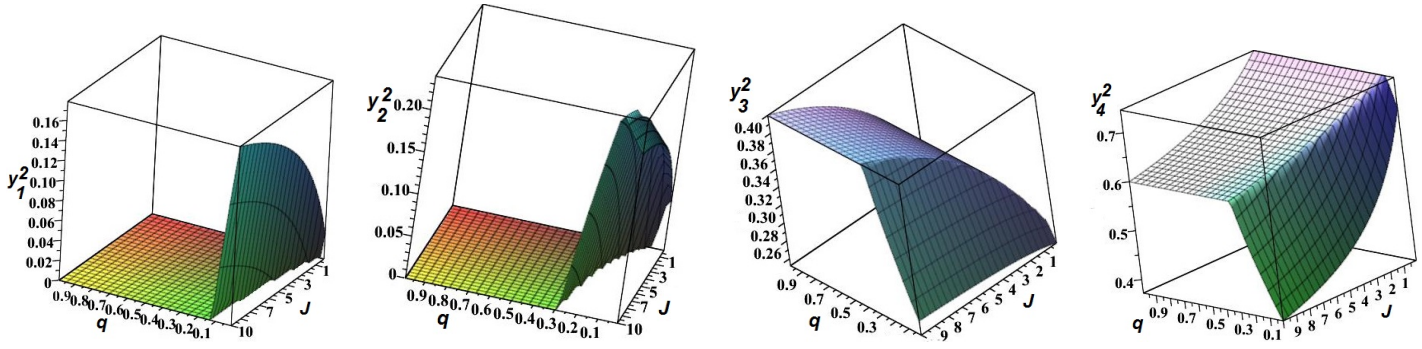
[19] *How Sarah Palin's Yahoo mailbox was so easily hacked.* The Guardian, Sep. 19, 2008.

[20] *Sarah Palin email hack*. Wikipedia.

[21] United States Congress, *Homeland Security Act of 2002*, Public Law, pp.107-296, 2002.

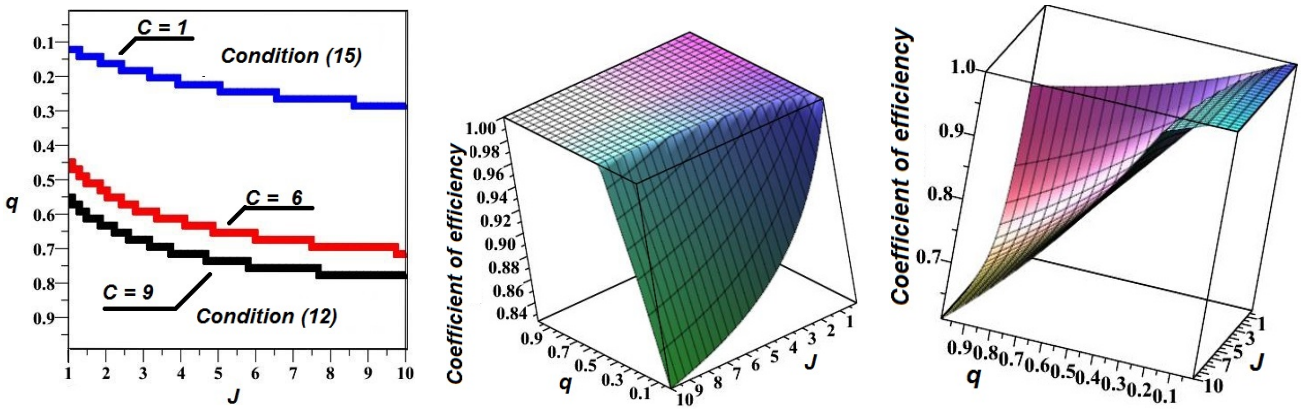
[22] Garnaev, A., and Fokkink, R., *A Searcher Versus Hider Game With Incomplete Information About Search Resources*. Asia-Pacific Journal of Operational Research, 30, 2013.

[23] Iida, K., Hohzaki, R., and Sato, K., *Hide-and-Search Game with the Risk Criterion*. Journal of Operations Research Society of Japan, 37, pp.287-296, 1994.



(Channel 1) (Channel 2) (Channel 3) (Channel 4)

Fig. 4. The equilibrium strategy of the infiltration adversary type for each channel as functions of probability q and jamming power J



(a) (b) (c)

Fig. 5. (a) Curves sharing the domains where either (12) or (15) condition from Theorem 1 holds as functions of probability q and jamming power J, (b) and (c) The coefficient of efficiency of the defender's strategy tuned to the expected threat compared to that tuned just to: (b) maximum damage attack and (c) infiltration attack.

[24] Baykal-Gürsoy, M., Duan, Z., Poor, H.V., and Garnaev, A., *Infrastructure Security Games*, under review, 2013.

[25] Home Office, *Current threat level*. http://www.homeoffice.gov.uk/counter-terrorism/current-threat-level/

[26] Neuts, M.F.,*A Multistage Search Game*. J. Soc. Indust. Appl. Math., 11, pp. 502-507, 1963.

[27] Sakaguchi, M., *Two-sided Search Games*. Journal of the Operations Research Society of Japan, 16, pp. 207-225, 1973.

[28] Owen, G., *Game Theory*. W.B.Sanders, Philadelphia, 1982.

[29] Garnaev, A., Garnaeva, G., and Goutal, P., *On the infiltration game*. International Journal of Game Theory, 26, pp. 215-221, 1997.

[30] Garnaev, A., *A Remark on a Helicopter and Submarine Game*. Naval Research Logistics, 40, pp.745-753, 1993.

[31] Garnaev, A., Trappe, W., and Kung, C.-T., *Dependence of Optimal Monitoring Strategy on the Application to be Protected*. Globecom 2012, pp. 1054-1059, 2012.

[32] Garnaev, A., Trappe, W., and Kung, C.-T., *Optimizing Scanning Strategies: Selecting Scanning Bandwidth in Adversarial RF Environments*. Crowncom 2013.

[33] Altman, E., Avrachenkov, K., and Garnaev, A., *Fair Resource Allocation in Wireless Networks in the Presence of a Jammer*. Performance Evaluation, 67, pp. 338-349, 2010.

[34] He, G., Debbah, M., and Altman, E., *K-Player Bayesian Waterfilling Game for Fading Multiple Access Channels.* Proc. CAMSAP 2009, pp.17-20, 2009.

VI. Appendix: Proof of Theorem 1

Since $u_D(\boldsymbol{x},(\boldsymbol{y}^1,\boldsymbol{y}^2))$ is linear in $\boldsymbol{x}$ and $u_A^k(\boldsymbol{x},\boldsymbol{y}^k)$ is linear in $\boldsymbol{y}^k$, by (6), $(\boldsymbol{x},(\boldsymbol{y}^1,\boldsymbol{y}^2))$ is an equilibrium if and only if the following conditions hold for some ν^1, ν^2 and ν:

$$(d_i x_i - 1)C_i \begin{cases} = \nu^1, & y_i^1 > 0, \\ \geq \nu^1, & y_i^1 = 0, \end{cases} \tag{22}$$

$$Cd_i x_i \begin{cases} = \nu^2, & y_i^2 > 0, \\ \geq \nu^2, & y_i^2 = 0, \end{cases} \tag{23}$$

$$q\left(d_i C_i y_i^1 - \sum_{j=1}^{N} C_j y_j^1\right) + (1-q)Cd_i y_i^2 \begin{cases} = \nu, & x_i > 0, \\ \leq \nu, & x_i = 0. \end{cases} \tag{24}$$

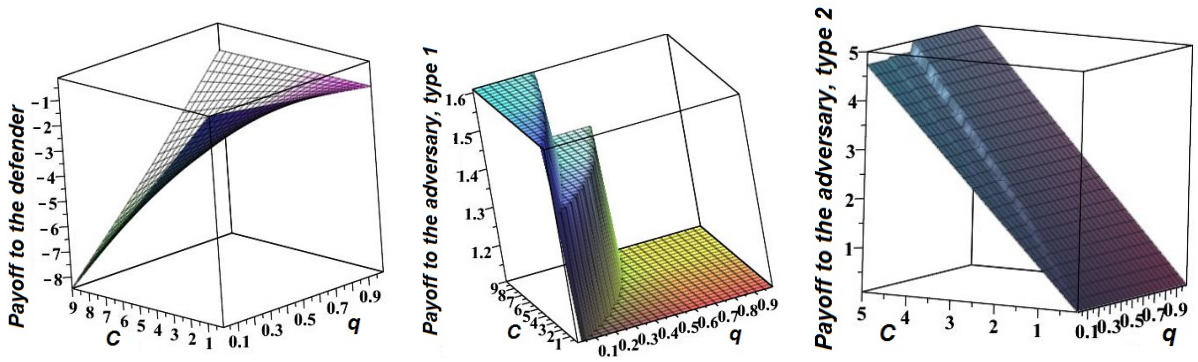
Since $\boldsymbol{x}$ is a probability vector and $d_i \in (0,1)$, by (23), $0 \leq \nu^2 < C$, and also (22) implies that $\nu^1 < 0$.

We will consider two cases separately: (A) $x_i > 0$ for any i, (B) there is an i such that $x_i = 0$. We will show these cases (A) and (B) relate to (a) and (b) correspondingly.

(A) Let $x_i > 0$ for any i. Then by (23) $\nu^2 > 0$. By (24) we have that for any i only three cases are possible: (i_1) $y_i^1 > 0$, $y_i^2 > 0$, (i_2) $y_i^1 > 0$, $y_i^2 = 0$ and (i_3) $y_i^1 = 0$, $y_i^2 > 0$.

(i_1) Assume that there exist i such that $y_i^1 > 0$ and $y_i^2 > 0$. Then by (22) and (23) we have that $C_i(d_i x_i - 1) = \nu^1$, $Cd_i x_i = \nu^2$. So,

$$C_i = -\frac{\nu^1}{1-\nu^2/C}, x_i = \frac{\nu^2}{Cd_i} = \frac{1}{d_i}\left(\frac{\nu^1}{C_i} + 1\right) \text{ for } y_i^1 y_i^2 > 0. \tag{25}$$



(a) (b) (c)

Fig. 6. (a) The payoff of the defender, (b) The payoff of the maximum damage adversary type, and (c) The payoff of the infiltration adversary type as functions of probability q and the value of attack, C.

(i_2) Let $y_i^1 > 0$ and $y_i^2 = 0$. Then by (22) and (23) we have that $C_i(1 - d_i x_i) = -\nu^1$, $Cd_i x_i \geq \nu^2$. So,

$$C_i \geq -\frac{\nu^1}{1-\nu^2/C}, x_i = \frac{(\nu^1/C_i)+1}{d_i} \text{ for } y_i^1 > 0, y_i^2 = 0. \tag{26}$$

(i_3) Let $y_i^1 = 0$ and $y_i^2 > 0$. Then by (22) and (23) we have that $C_i(1 - d_i x_i) \leq -\nu^1$, $Cd_i x_i = \nu^2$. So,

$$C_i \leq -\frac{\nu^1}{1-\nu^2/C}, x_i = \frac{\nu^2}{Cd_i} \text{ for } y_i^1 = 0, y_i^2 > 0. \tag{27}$$

By the assumption (7) and (25)–(27) we have that there is a k such that

$$C_k = -\nu^1/(1-\nu^2/C), \tag{28}$$

$$y_i^1 \begin{cases} > 0, & i \leq k-1, \\ \geq 0, & i = k, \\ = 0, & i \geq k+1, \end{cases} \qquad y_i^2 \begin{cases} = 0, & i \leq k-1, \\ \geq 0, & i = k, \\ > 0, & i \geq k+1 \end{cases} \tag{29}$$

and

$$x_i = \begin{cases} \frac{1}{d_i}\left(\frac{\nu^1}{C_i}+1\right), & i \leq k-1, \\ \frac{\nu^2}{Cd_k} = \frac{1}{d_k}\left(\frac{\nu^1}{C_k}+1\right), & i = k, \\ \frac{\nu^2}{Cd_i} = \frac{1}{d_i}\left(\frac{\nu^1}{C_k}+1\right), & i \geq k+1. \end{cases} \tag{30}$$

Then, by (24) and (29), we have that

$$y_i^1 = \begin{cases} \omega/(d_i C_i q), & i \leq k-1, \\ y_k^1, & i = k, \\ 0, & i \geq k+1, \end{cases} \qquad y_i^2 = \begin{cases} 0, & i \leq k-1, \\ y_k^2, & i = k, \\ \omega/(C(1-q)d_i), & i \geq k+1 \end{cases} \tag{31}$$

and

$$qd_k C_k y_k^1 + (1-q)d_k C y_k^2 = \omega, \tag{32}$$

with

$$\omega = \nu + q\sum_{j=1}^{N} C_j y_j^1. \tag{33}$$

Then by (31) since $\boldsymbol{y}^1$ and $\boldsymbol{y}^2$ are probability vectors

$$\begin{aligned} y_k^1 &= 1 - (\omega/q)\sum_{j=1}^{k-1} 1/(d_j C_j), \\ y_k^2 &= 1 - (\omega/(1-q))\sum_{j=k+1}^{N} 1/(d_j C). \end{aligned} \tag{34}$$

Substituting (34) into (32) allows to find ω as a function of k with Ψ_k given by (14):

$$\omega = (qC_k d_k + (1-q)Cd_k)/\Psi_k. \tag{35}$$

This allows us, by using (31) and (34), to get y^k in closed form as it is given in (13) as a function of k.

How can k be found? It is defined by the condition that $\boldsymbol{y}^t (t = 1, 2)$ is a strategy (a probability vector), so $\sum_{j=1}^{N} y_j^t = 1$ (which holds by (31) and (34)) and $y_i^t \geq 0$ for $i \in \{1, \ldots, N\}$. Since $\omega > 0$ then by (13) $y_i^t \geq 0$ for $i \in \{1, \ldots, N\} \backslash \{k\}$. So, $\boldsymbol{y}^t, t = 1, 2$ are strategies if and only if $y_k^1 \geq 0$ and $y_k^2 \geq 0$. These conditions by (34) and (35) are equivalent to

$$(qd_k C_k + (1-q)d_k)/\Psi_k \leq \min\left\{ \frac{q}{\sum_{j=1}^{k-1} 1/(d_j C_j)}, \frac{1-q}{\sum_{j=k+1}^{N} 1/(d_j C)} \right\}.$$

These inequalities are equivalent to

$$\psi_k \leq q/(1-q) \leq \psi_{k+1}, \tag{36}$$

with ψ_s given by (9). The sequence $\{\psi_s\}$ is increasing since

$$\frac{\psi_{s+1}-\psi_s}{C}=\frac{\sum\limits_{j=s+1}^{N}1/(d_sd_jC_s)+\sum\limits_{j=1}^{s}1/(d_sd_jC_j)}{\sum\limits_{j=s+1}^{N}(1/d_j)\sum\limits_{j=s}^{N}(1/d_j)}.$$

Thus, k is uniquely defined by (36). Also, (36) is equivalent to (8), and $\boldsymbol{y}^1$ and $\boldsymbol{y}^2$ given by (13) are the unique equilibrium strategy of the adversary.

Now we have to find the defender strategy. To do so, we have to define ν^1 in such way that $\boldsymbol{x}$ given by (30) has to be a probability vector. Then, summing up (30) implies that the following equation has to hold:

$$F(\nu^1):=\sum_{i=1}^{k}\frac{1}{d_i}\left(1+\frac{\nu^1}{C_i}\right)+\sum_{i=k+1}^{N}\frac{1}{d_i}\left(1+\frac{\nu^1}{C_k}\right)=1. \tag{37}$$

By (7) and (30), $x_i\geq 0$ for $i\in[1,N]$ if and only if $-C_k\leq\nu^1\leq 0$. Since $F(\nu^1)$ is increasing and $F(0)>1$, there is a ν^1 such that (37) holds if and only if

$$F(-C_k)=\sum_{i=1}^{k}(1/d_i)\left(1-C_k/C_i\right)=\varphi_k\leq 1. \tag{38}$$

If (38) holds then ν^1 is given uniquely as follows:

$$\nu^1=\frac{1-\sum_{i=1}^{N}(1/d_i)}{\sum_{i=1}^{k}(1/(d_iC_i))+\sum_{i=k+1}^{N}(1/(d_iC_k))}. \tag{39}$$

Substituting (39) into (30) produces the unique equilibrium strategy of the defender.

To obtain the payoffs to the rivals note that by (28)

$$\nu^2=C(1+\nu^1/C_k). \tag{40}$$

By (22), (23), (29), (30) and definition of payoffs (1), (4) and (5) we have that

$$u_A^1=-\nu^1,$$

$$u_A^2=C-\nu^2=(\text{by }(40)=-C\nu^1/C_k,$$

$$u_D=-q\nu^1-(1-q)\nu^2,$$

and (a) follows.

(B) Let there exist an i such that $x_i=0$. Then, by (23), $\nu^2=0$, and so, $y_i^2=0$ for $x_i>0$. Following the proof of (i_1)–(i_3), (7) implies that there is a m such that

$$x_i\begin{cases}\geq 0, & i\leq m,\\ =0, & i\geq m+1,\end{cases} \tag{41}$$

$$y_i^1\begin{cases}\geq 0, & i\leq m,\\ =0, & i\geq m+1,\end{cases} \tag{42}$$

$$y_i^2\begin{cases}=0, & i\leq m,\\ \geq 0, & i\geq m+1.\end{cases} \tag{43}$$

Also, by (22),

$$Cx_id_i\begin{cases}=1+\nu^1/C_i, & y_i^1>0,\\ \geq 1+\nu^1/C_i, & y_i^1=0.\end{cases} \tag{44}$$

Consider two cases (B_1) $\xi_m\neq -C_m$ and (B_2) $\xi_m=-C_m$ separately. We will show that the case (B_1) corresponds to (b_1), and (B_2) corresponds to (b_2).

(B_1) Let $\xi_m\neq -C_m$. Then, by (22),

$$x_i=\begin{cases}(1/d_i)\left(1+\nu^1/C_i\right), & i\leq m,\\ 0, & i\geq m+1.\end{cases} \tag{45}$$

Since $\boldsymbol{x}$ has to be a probability vector, summing up x_i from (45) yields that $1=\sum_{i=1}^{m}(1/d_i)\left(1+\nu^1/C_i\right)$. Thus, $\nu^1=\xi_m$.

For switching point m by (7), (44) and (45) the following conditions have to hold: $-C_m\leq\nu^1<-C_{m+1}$. These conditions are equivalent to (11) with φ_i given by (10). Since $\nu^1=\xi_m\neq -C_m$ then $x_m>0$. So, by (7) and (45) $\{i:x_i>0\}=\{i:y_i^1>0\}=\{1,\dots,m\}$.
By (24)

$$y_i^1=\begin{cases}\omega/(qd_iC_i), & i\leq m,\\ 0, & i\geq m+1,\end{cases} \tag{46}$$

$$y_i^2\begin{cases}=0, & i\leq m,\\ \leq\omega/((1-q)d_iC), & i\geq m+1.\end{cases} \tag{47}$$

Since $\sum_{j=1}^{m}y_j^1=1$ then (46) implies (18) and that $\omega=q/\sum_{j=1}^{m}(1/(d_jC_j))$. Then since ψ_s is increasing and $m\leq k-1$ we have that

$$\begin{aligned}\sum_{i=m+1}^{N}\frac{\omega}{(1-q)d_iC}&=\frac{\sum_{i=m+1}^{N}(1/(d_iC))}{\sum_{j=1}^{m}(1/(d_jC_j))}\frac{q}{1-q}\\&=\frac{q}{(1-q)\psi_{m+1}}\geq\frac{q}{(1-q)\psi_k}\geq(\text{by }(8))\geq 1.\end{aligned} \tag{48}$$

So, $\boldsymbol{y}^2$ as a probability vector can be defined by (47) and the result follows.

(B_2) Let $\xi_m=-C_m$. Then, by (41)-(43) and (24), we have that

$$y_i^1\begin{cases}>0, & i\leq m-1,\\ \geq 0, & i=m,\\ =0, & i\geq m+1\end{cases} \tag{49}$$

and

$$x_i\begin{cases}>0, & i\leq m-1,\\ =0, & i\geq m\end{cases}$$

So, $\boldsymbol{x}$ is given by (45) with $\nu^1=-C_m$.
By (24) and (49)

$$y_i^1=\begin{cases}\frac{\omega}{qd_iC_i}, & i\leq k-1,\\ 1-\sum\limits_{j=1}^{k-1}\frac{\omega}{qd_jC_j}\leq\frac{\omega}{qd_kC_k}, & i=k,\\ 0, & i\geq k+1.\end{cases} \tag{50}$$

Thus, $\boldsymbol{y}^1$ given by (50) is a probability vector if and only $0 \leq y_k^1 \leq \min\{1, \omega/(qd_kC_k)\}$, this is equivalent to $1/(\sum_{j=1}^{k}(1/(d_jC_j)) \leq \omega/q \leq 1/(\sum_{j=1}^{k-1}(1/(d_jC_j))$, and putting $\epsilon = \omega/q$ implies (b_2), and the result follows. ■