Computers & Industrial Engineering 90 (2015) 352–360

Contents lists available at ScienceDirect

Computers & Industrial Engineering

journal homepage: www.elsevier.com/locate/caie

How to deal with an intelligent adversary ☆

Andrey Garnaev [a,b,*], Melike Baykal-Gursoy [c,d], H. Vincent Poor [e]

[a] WINLAB, Rutgers University, North Brunswick, NJ 08901, USA
[b] Department of Computer Modelling and Multiprocessor Systems, Saint Petersburg State University, St. Petersburg 198504, Russia
[c] Department of Industrial and Systems Engineering, Rutgers University, Piscataway, NJ 08854-8018, USA
[d] Center for Advanced Infrastructure and Transportation, Rutgers University, Piscataway, NJ 08854-8018, USA
[e] Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA

ARTICLE INFO

Article history:
Received 3 May 2015
Received in revised form 29 August 2015
Accepted 6 October 2015
Available online 10 November 2015

Keywords:
Network protection
Equilibrium
Bayesian game

ABSTRACT

Traditionally, the design of network protection strategies is based on the answers of a protector and an adversary to the question "How?": how should the protector allocate its protection resources, and how should the adversary allocate its attacking resources? This paper considers a more sophisticated adversary, who, planning its malicious activities, considers two questions: "What for?" and "How?". Namely, what is the motivation for the attack? and how to attack based on the chosen motivation? To study this problem, a simple game-theoretic network protection model is considered, in which the adversary decides whether to intrude on the network to inflict maximal damage or to perform a reconnaissance mission, and based on this decision an intrusion strategy is designed. The solution to this game shows that such an adversary may try a feint to draw the protector's efforts away from the nodes that the adversary intends to attack. Taking into account this feature of the adversary's behavior allows improvements in the reliability of a protection strategy.

1. Introduction

Computer networks have come to serve a critical societal role, but this has created a new type of terrorism, namely, cyber-terrorism. So many critical activities, such as commerce, finance, energy, education and health care are online, that gaining control of or disrupting such online systems, by Rainie, Anderson, and Connolly (2014), can sow panic, cause damage or even lead to loss of life. For example, by Magnuson (2014), cyber-attacks on electric utilities can be devastating, since "taking down an electric grid, especially one that serves a major city, could do real damage to the economy and may indirectly cost lives". Testifying to the House of Representatives Intelligence Committee on cyber threats, Admiral Rogers (see, Zengerle, 2014) said that a few countries have the ability to invade and possibly shut down computer systems of U.S. power utilities, aviation networks and financial companies, and these capabilities can be used by nation-states, groups or individuals to take down these critical activities. Cyber threats are only one of the challenges homeland security has to meet. Despite trillion-dollars investments (see, Mueller & Stewart, 2011), the resources are still inadequate to respond to an increasing number of old and new threats as adversaries (criminals or terrorists) create new non-trivial methods of attack. For this reason, the National Research Council (see, NRC, 2008) has emphasized the importance of modeling terrorists as intelligent adversaries, and has proposed three possible techniques to assess the impact of an intelligent adversary, one of which is game-theoretic modeling. The problem of security involves many different aspects, see, for example, a recent review of Hausken and Levitin (2012), where 129 published research papers on different aspects of security were classified according to the system structure, defense measures, attack tactics and circumstances involved.

Numerous researchers have used game theory to study resource-allocation decisions for network protection, see for example, Manshaei, Zhu, Alpcan, Basar, and Hubaux (2013), Guikema (2009) and Baykal-Gursoy, Duan, Poor, and Garnaev (2014) that provide references of research contributions that analyze and solve security problems in networks via game-theoretic approaches. In these works, the main setting is one in which the protector and the adversary seek answers to the same question, "How?" Namely, how to best allocate protection resources? how to best allocate attacking resources? In this paper we examine network protection from a different point of view, and, consider a more sophisticated adversary, who plans an attack or an intrusion by asking two questions: "What for?" and "How?". Namely, what is the motivation for

☆ This material is based upon work supported by the National Science Foundation under Grant Numbers CMMI-1436288 and CMMI-1435778.

* Corresponding author at: WINLAB, Rutgers University, North Brunswick, NJ 08901, USA.
E-mail addresses: garnaev@yahoo.com (A. Garnaev), gursoy@rci.rutgers.edu (M. Baykal-Gursoy), poor@princeton.edu (H. Vincent Poor).

http://dx.doi.org/10.1016/j.cie.2015.10.001
0360-8352/

intruding on the network? and how to intrude based on the chosen motivation? Of course, answers to these questions might lead to completely different adversarial behavior, than answering only the question "How?"

Admiral Rogers (see, Zengerle, 2014), in his testimony, pointed out that in addition to some countries already having the ability to shut down valuable U.S. computer systems, some digital attackers have also been able to penetrate such systems and perform "reconnaissance" missions to determine how the networks are put together. Such adversaries, planning their intrusions, had to answer the question: What is the purpose of the intrusion: to shut down the system or to perform "reconnaissance"?, and then to act according to the answer.

As an example of other purposes for intrusion, see Levitin, Hausken, Taboada, and Coit (2012), where a problem to store information securely if an adversary may steal or destroy the information was considered. Non-dominated solutions to this information security problem were found based on a multiple objective genetic algorithm.

To gain insight into this type of situation, we suggest a simple game, in which an adversary can intrude on a network to corrupt its nodes, and design its intrusion plan based on the chosen motivation. We consider two basic motivations: (a) to inflict maximal damage, and (b) to perform reconnaissance. Note that, in Garnaev, Baykal-Gursoy, and Poor (2014), it was shown, that a protection strategy may depend essentially on the type of attack, and incorporating a priori knowledge of the attack's type, which is fixed but unknown to the protector, increases defense efficiency. In this paper, we extend this approach by allowing the adversary to be more sophisticated and skillful in designing the intrusion, namely, allowing the adversary to choose consciously its motivation for intrusion, and to optimize its intrusion accordingly. This allows us to incorporate a human factor into the adversary's strategy.

The main contributions of this paper are the following:

(a) Developing a game-theoretic resource allocation model for inflicting a maximal damage attack on a network and for an intrusion attack into network to perform a reconnaissance mission.
(b) Incorporating a human factor into the adversary's behavior allowing him to choose consciously one of the types of attack.
(c) Showing the difference in the principles that the intrusion strategy and the detection strategy have to be based on in order to be optimal. Namely, the intrusion strategy has to be based on a tactical decision making approach allowing sudden switching between strategies. Meanwhile, the protection strategy has to be based on a strategic decision making approach incorporating the possibility of such tactical adversary's decision making by a proper allocation of protection resources in advance.

The organization of this paper is as follows: in Section 2 and its four subsections, we first model two types of attack on a network by means of resource allocation games. In both games the type of attack is fixed, and known to the rivals. In Section 3 and its two subsections, we extend the model to allow for a sophisticated adversary to choose the type (motivation) of intrusion. In Section 4, discussions and conclusions are offered. In the appendix, the proofs of the obtained results are supplied.

2. Two types of attack

In this section and its four subsections, we describe two game-theoretic models describing two types of attack on a network: to inflict maximal damage and to perform a reconnaissance mission.

2.1. Strategies

The game is played on a network. Here we have in mind a computer or communication network consisting of N nodes. It is an abstract network composed of communication links and nodes that may contain data that need to be protected. As such, the network does not correspond to any specific topology. In the network two *agents* (players, rivals) are present. An agent who wants to minimize the effects of an attack is called the *protector* (say, it can be an intrusion detection system (IDS)). An agent who wants to intrude the network is called the *adversary*. We assume that each game is played in one time slot with a total duration Y, during which the intrusion has to be detected. If it is not detected, it could yield some serious consequences, say, loss of valuable data, or loss in the network's security due to successful "reconnaissance". During the time slot the adversary might intrude a single node, i.e., an adversary's strategy is a vector $\boldsymbol{x} = (x_1, \ldots, x_N)$, where x_i is the probability that the adversary intrudes node i, and $\sum_{i=1}^{N} x_i = 1$. The protector has a more sophisticated strategy, namely, during the time slot, the protector can switch from one node to another to scan. Thus, its strategy corresponds to the amount of time it has to spend scanning each selected node, i.e., a protector's strategy is a vector $\boldsymbol{y} = (y_1, \ldots, y_N)$, where y_i is the scanning time of node i, and $\sum_{i=1}^{N} y_i = Y$.

2.2. Value of node and detection probability

Each node of the network is characterized by a value C_i (say, the amount of stored valuable data). We assume that the damage to node i equals to the value of the stolen data, and that all data stored in the corrupted node can be stolen, if the scanning failed. We consider only the direct cost of an attack including data loss, or financial losses caused. In addition to the direct cost, as suggested by Kumar and Liu (2014), indirect losses might arise, and they could be significantly higher than direct losses, since a successful attack could impact negatively on consumer behavior and investor confidence.

For simplicity we assume that the probability of not detecting the adversary depends exponentially on the scanning time, namely, it is $\exp(-\lambda_i y_i)$, if node i is corrupted, with λ_i as a scanning characteristic of node i. Thus, detection probability is $1 - \exp(-\lambda_i y_i)$. See, also Stone (2007), Iida, Hohzaki, and Sato (1994), Sakaguchi (1973), Lewis (2009), Baston and Garnaev (2000), Garnaev and Trappe (2014), as examples of using exponential dependence in network protection games.

2.3. Game with the maximal damage attack

In this section, we consider the scenario in which the adversary intrudes on the network to inflict maximal damage. The payoff to the adversary is the total expected damage this can cause, i.e., $v_A^D(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i=1}^{N} C_i x_i \exp(-\lambda_i y_i)$. The payoff to the protector is $v_P^D(\boldsymbol{x}, \boldsymbol{y}) = -v_A^D(\boldsymbol{x}, \boldsymbol{y})$. Thus, this is a zero-sum game (see, Fudenberg & Tirole, 1991). We assume that the rivals know the nodes' values C_i, the scanning characteristics λ_i for every node i, and the duration of the time slot Y. Recall that $(\boldsymbol{x}_*, \boldsymbol{y}_*)$ is an equilibrium (saddle point) of such a game if and only if $v_A^D(\boldsymbol{x}, \boldsymbol{y}_*) \leqslant v_A^D(\boldsymbol{x}_*, \boldsymbol{y}_*) \leqslant v_A^D(\boldsymbol{x}_*, \boldsymbol{y})$ for any $(\boldsymbol{x}, \boldsymbol{y})$.

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

$$C_1 > C_2 > \cdots > C_N. \tag{1}$$

Theorem 1. *The value of the game with a maximal damage attack is given as follows:*

$$\bar{v}_A^D = \exp\left(\frac{\sum_{j=1}^{k_D}(\ln(C_j)/\lambda_j) - Y}{\sum_{j=1}^{k_D}(1/\lambda_j)}\right), \tag{2}$$

where $k_D \in [1,N]$ *is such that*

$$\varphi_{k_D} \leqslant Y < \varphi_{k_D+1}, \tag{3}$$

with $\{\varphi_i\}$ *is strictly increasing on i such that*

$$\varphi_i = \sum_{j=1}^{i}(\ln(C_j/C_i)/\lambda_j), \quad i \in [1,N], \tag{4}$$

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

The adversary has a unique strategy given as follows:

$$\bar{y}_i^D = \begin{cases} \frac{1/\lambda_i}{\sum_{j=1}^{k_D}(1/\lambda_j)}\left(Y + \sum_{j=1}^{k_D}\frac{\ln(C_i/C_j)}{\lambda_j}\right), & i \leqslant k_D, \\ 0, & i \geqslant k_D+1. \end{cases} \tag{5}$$

If $\bar{v}_A^D \neq e^{C_{k_D}}$ *then the protector has a unique equilibrium strategy given by*

$$\bar{x}_i^D = \begin{cases} \frac{1/\lambda_i}{\sum_{j=1}^{k_D}(1/\lambda_j)}, & i \leqslant k_D, \\ 0, & i \geqslant k_D+1. \end{cases} \tag{6}$$

If $\bar{v}_A^D = e^{C_{k_D}}$ *then the protector has a continuum of equilibrium strategies given by*

$$\bar{x}_i^D = \begin{cases} \frac{\omega}{\lambda_i C_{k_D}}, & i \leqslant k_D-1, \\ 1 - \frac{\omega}{C_{k_D}}\sum_{j=1}^{k_D-1}\frac{1}{\lambda_j}, & i = k_D, \\ 0, & i \geqslant k_D+1, \end{cases} \tag{7}$$

for any $C_{k_D}/\sum_{i=1}^{k_D}(1/\lambda_i) \leqslant \omega \leqslant C_{k_D}/\sum_{i=1}^{k_D-1}(1/\lambda_i)$.

Of course, all of these equilibrium strategies are equivalent, since they all return the same payoff.

2.4. Game with a reconnaissance mission

In this scenario, the adversary wants to invade the network for reconnaissance purposes. Here we assume that the purpose of the reconnaissance mission for the adversary should be to check the possibility of safe infiltration into the network. Thus, his payoff is proportional to the probability of being undetected. A proportionality coefficient C can be considered as the value of the reconnaissance mission. So, the payoff to the adversary is $v_A^R(\boldsymbol{x},\boldsymbol{y}) = C\sum_{i=1}^{N}x_i\exp(-\lambda_i y_i)$. The protector wants to minimize the adversary's payoff. Hence, its payoff is $v_P^R(\boldsymbol{x},\boldsymbol{y}) = -v_A^R(\boldsymbol{x},\boldsymbol{y})$, and this is again a zero-sum game. We assume that the rivals know the value of reconnaissance mission C, scanning characteristics λ_i and time slot duration Y.

Theorem 2. *The value of the game with a reconnaissance mission is* $\bar{v}_A^R = C\exp\left(-Y/\sum_{j=1}^{N}(1/\lambda_j)\right)$, *and it has a unique saddle point* $(\bar{\boldsymbol{x}}^R,\bar{\boldsymbol{y}}^R)$, *where*

$$\bar{x}_i^R = 1/\sum_{j=1}^{N}(\lambda_i/\lambda_j), \quad \bar{y}_i^R = Y/\sum_{j=1}^{N}(\lambda_i/\lambda_j) \text{ for } i \in [1,N].$$

Thus, in the reconnaissance intrusion all nodes always might be under attack, and so, all of them have to be under protection.

3. The adversary can select attack's type

Next, we extend the above discussed games for more sophisticated adversary who can choose the type (motivation) of intrusion, and attack accordingly.

3.1. Game with predesigned strategies

In this section, we assume that each of the rivals have two predesigned strategies for effort allocation. Namely, the adversary has two equilibrium strategies for intrusion ($\bar{\boldsymbol{x}}^D$ and $\bar{\boldsymbol{x}}^R$) motivated by the two basic games depending on what type of intrusion he intends to apply to. Thus, applying intrusion strategy $\bar{\boldsymbol{x}}^D$ means that the adversary performs maximal damage intrusion, and $\bar{\boldsymbol{x}}^R$ means reconnaissance intrusion. The protector also has two strategies of scanning to respond ($\bar{\boldsymbol{y}}^D$ and $\bar{\boldsymbol{y}}^R$). Applying scanning efforts $\bar{\boldsymbol{y}}^D$ means that the protector expects maximal damage intrusion, and $\bar{\boldsymbol{y}}^R$ means that it expects reconnaissance intrusion. Thus, here we assume that the maximal damage strategy and reconnaissance strategy are mutually exclusive, and thus cannot be used simultaneously. Which of these predesigned strategies should be chosen if each of the rivals does not know the choice of the other? To answer this question we consider the following zero-sum 2×2 matrix game, in which rows correspond to the adversary's strategies and columns to the protector's strategies:

$$\begin{array}{c|cc} & \bar{\boldsymbol{y}}^D & \bar{\boldsymbol{y}}^R \\ \hline \bar{\boldsymbol{x}}^D & v_A^D(\bar{\boldsymbol{x}}^D,\bar{\boldsymbol{y}}^D) & v_A^D(\bar{\boldsymbol{x}}^D,\bar{\boldsymbol{y}}^R) \\ \bar{\boldsymbol{x}}^R & v_A^R(\bar{\boldsymbol{x}}^R,\bar{\boldsymbol{y}}^D) & v_A^R(\bar{\boldsymbol{x}}^R,\bar{\boldsymbol{y}}^R) \end{array}. \tag{8}$$

Let $\boldsymbol{\gamma} = (\gamma, 1-\gamma)$ and $\boldsymbol{\delta} = (\delta, 1-\delta)$ be mixed strategies for the adversary and the protector, respectively, i.e. the adversary employs pure strategies $\bar{\boldsymbol{x}}^D$ and $\bar{\boldsymbol{x}}^R$ with probabilities γ and $1-\gamma$, and the protector employs pure strategies $\bar{\boldsymbol{y}}^D$ and $\bar{\boldsymbol{y}}^R$ with probabilities δ and $1-\delta$. Then, the expected payoff to the adversary is given by

$$v(\boldsymbol{\gamma},\boldsymbol{\delta}) := \bar{v}_A^D\gamma\delta + v_A^D(\bar{\boldsymbol{x}}^D,\bar{\boldsymbol{y}}^R)\gamma(1-\delta) + v_A^R(\bar{\boldsymbol{x}}^R,\bar{\boldsymbol{y}}^D)(1-\gamma)\delta + \bar{v}_A^R(1-\gamma)(1-\delta).$$

We are looking for equilibrium strategies, i.e., for such $(\boldsymbol{\gamma}_*,\boldsymbol{\delta}_*)$ that for any $(\boldsymbol{\gamma},\boldsymbol{\delta})$ the following inequalities hold: $v(\boldsymbol{\gamma},\boldsymbol{\delta}_*) \leqslant v(\boldsymbol{\gamma}_*,\boldsymbol{\delta}_*) \leqslant v(\boldsymbol{\gamma},\boldsymbol{\delta}_*)$.

Let us introduce the following auxiliary notations:

$$a_{11} := \bar{v}_A^D, \quad a_{22} := \frac{\bar{v}_A^R}{C} = \exp\left(-Y\Big/\sum_{j=1}^{N}(1/\lambda_j)\right),$$

$$a_{12} := v_A^D(\bar{x}^D,\bar{y}^R) = \frac{\sum_{j=1}^{k_D}(C_j/\lambda_j)}{\sum_{j=1}^{k_D}(1/\lambda_j)}\exp\left(-Y\Big/\sum_{j=1}^{N}(1/\lambda_j)\right),$$

$$a_{21} := \frac{v_A^R(\bar{x}^R,\bar{y}^D)}{C} = \frac{\sum_{j=1}^{k_D}(\bar{v}^D/(\lambda_j C_j)) + \sum_{j=k_D+1}^{N}(1/\lambda_j)}{\sum_{j=1}^{N}(1/\lambda_j)},$$

where a_{ij} does not depend on C. Using this notation the matrix game has the following form:

$$\begin{array}{c|cc} & \bar{\boldsymbol{y}}^D & \bar{\boldsymbol{y}}^R \\ \hline \bar{\boldsymbol{x}}^D & a_{11} & a_{12} \\ \bar{\boldsymbol{x}}^R & Ca_{21} & Ca_{22} \end{array}. \tag{9}$$

Since $v_A^R(\bar{\boldsymbol{x}},\bar{\boldsymbol{y}})$ and $v_A^D(\bar{\boldsymbol{x}},\bar{\boldsymbol{y}})$ are strictly convex in $\bar{\boldsymbol{y}}$, and $(\bar{\boldsymbol{x}}^D,\bar{\boldsymbol{y}}^D)$ and $(\bar{\boldsymbol{x}}^R,\bar{\boldsymbol{y}}^R)$ are saddle points of the corresponding games we have that

$$a_{11} < a_{12} \text{ and } a_{22} < a_{21}. \tag{10}$$

By (10), $a_{11}/a_{21} < a_{12}/a_{22}$. Thus, the inequalities $a_{11} > Ca_{21}$ and $Ca_{22} > a_{12}$ cannot hold simultaneously for any enough small open interval of C. Thus, the following theorem holds.

Theorem 3. *The considered game has a unique equilibrium if* $C \notin \{a_{11}/a_{21}, a_{12}/a_{22}\}$.

(a) *If* $a_{12}/a_{22} < C$ *then* $(\bar{\boldsymbol{x}}^R, \bar{\boldsymbol{y}}^R)$ *is the unique equilibrium in pure strategies.*

(b) *If* $C < a_{11}/a_{21}$ *then* $(\bar{\boldsymbol{x}}^D, \bar{\boldsymbol{y}}^D)$ *is the unique equilibrium in pure strategies.*

(c) *If* $a_{11}/a_{21} < C < a_{12}/a_{22}$ *then* $(\boldsymbol{\gamma}, \boldsymbol{\delta}) := (\boldsymbol{\gamma}(C), \boldsymbol{\delta}(C))$ *is the unique equilibrium in mixed strategies, and* $v := v(C)$ *is the value of the game given as follows:*

$$\begin{aligned}\gamma(C) &= \frac{C(a_{21}-a_{22})}{C(a_{21}-a_{22})+a_{12}-a_{11}},\\ \delta(C) &= \frac{a_{12}-Ca_{22}}{C(a_{21}-a_{22})+a_{12}-a_{11}},\\ v(C) &= \frac{C(a_{21}a_{21}-a_{11}a_{22})}{C(a_{21}-a_{22})+a_{12}-a_{11}}.\end{aligned} \tag{11}$$

If $C = a_{11}/a_{21}$ *then two equilibria given by (b) and (c) arise. If* $C = a_{12}/a_{22}$ *then two equilibria given by (a) and (c) arise.*

The pure equilibrium is $(\bar{\boldsymbol{x}}^R, \bar{\boldsymbol{y}}^R)$ for large C, and it is $(\bar{\boldsymbol{x}}^D, \bar{\boldsymbol{y}}^D)$ for small C. Meanwhile for intermediate C the adversary tries to defeat the protector by diverting its scanning effort from more to less dangerous intrusion. Note that $\gamma(C) = 1$ for $C \uparrow a_{11}/a_{21}$, and $\gamma(C) = \frac{a_{21}-a_{22}}{(a_{12}/a_{11})a_{21}-a_{22}} < 1$ for $C \downarrow a_{11}/a_{21}$. Thus, the probability of using maximal damage intrusion drops down at $C = a_{11}/a_{21}$. This forces the protector to pay more attention to the possibility of reconnaissance intrusion, which was negligible before, and so the probability of using scanning efforts versus such intrusion monotonically increases with increasing C. Common sense may predict the increasing preference of the adversary for a reconnaissance intrusion. However, as it is shown, the adversary, instead, again increases preference for the maximal damage intrusion, while the protector keeps on increasing its expectation of reconnaissance intrusion. Finally, when the reconnaissance intrusion becomes unbeatably valuable, the adversary again switches to using only this intrusion. In spite of these jumps in the adversary's policy, the value of the game continuously increases in C (Fig. 1).

3.2. Game with flexible resource allocation response

In this section we describe a bi-level decision making scheme of the adversary with flexible resource allocation responses. Note that, bi-level decision making schemes are widely used in network security problems. See, for example, Konak, Kulturel-Konak, and Snyder (2015) for the reliable server assignment problem under attacks, and Tambe, Jiang, An, and Jain (2012) for infrastructure security problems.

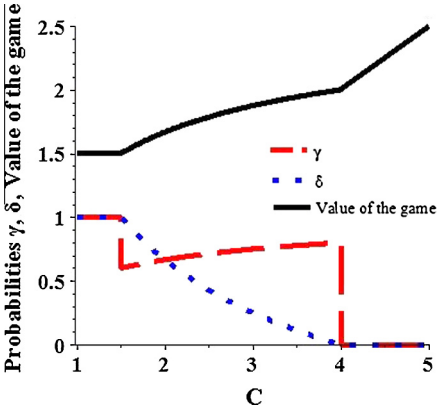

Fig. 1. Probabilities γ, δ, and the value of the game v as functions on C for $a_{11} = 1.5, a_{12} = 2, a_{21} = 1, a_{22} = 0.5$.

In the first step, the probability γ of intrusion to maximize damage is fixed and known to both rivals. A strategy of the adversary is $(\boldsymbol{x}^D, \boldsymbol{x}^R)$, where $\boldsymbol{x}^D$ and $\boldsymbol{x}^R$ are strategies for intrusion to maximize damage and to perform reconnaissance. The payoff to the adversary is $v_A((\boldsymbol{x}^D, \boldsymbol{x}^R), \boldsymbol{y}) = \gamma v_A^D(\boldsymbol{x}^D, \boldsymbol{y}) + (1-\gamma) v_A^R(\boldsymbol{x}^R, \boldsymbol{y})$. In this step the rivals choose the strategies $(\boldsymbol{x}^D(\gamma), \boldsymbol{x}^R(\gamma))$ and $\boldsymbol{y}(\gamma)$ as an equilibrium to the zero-sum game with payoff to the adversary v_A. Since, all the equilibrium strategies in a zero-sum game are equivalent to each other (they return the same payoffs), we will not focus specially on the problem of uniqueness of the equilibrium in the first step. Note that, the game, played in the first step for a fixed γ, is Bayesian. Bayesian games have been widely employed in dealing with different problems in networks, for example, Liu, Comaniciu, and Mani (2006), Agah, Das, Basu, and Asadi (2007) for intrusion detection, Garnaev and Trappe (2015) for spectrum coexistence, Garnaev, Trappe, and Kung (2012), Garnaev, Trappe, and Kung (2013) for scanning bandwidth, Li and Wu (2008) for malicious activity in mobile ad hoc networks, and Ren, Mo, and Shi (2014) for Denial of Service (DoS) attacks.

In the second step, the adversary finds γ to maximize his payoff, i.e., $\gamma = \arg_\gamma \max v_A((\boldsymbol{x}^D(\gamma), \boldsymbol{x}^R(\gamma)), \boldsymbol{y}(\gamma))$.

To formulate the main result (Theorem 4) we first formulate two auxiliary lemmas, where also auxiliary notation is introduced.

Lemma 1. *The inequality*

$$\psi_{k_D+1} \leqslant \frac{\bar{v}^D(\gamma)}{(1-\gamma)C} \tag{12}$$

is equivalent to

$$\gamma \geqslant \gamma_*, \tag{13}$$

where $\gamma_* \in (0,1)$ *is the unique root of the equation*

$$\frac{\bar{v}^D(\gamma)}{(1-\gamma)C} = \psi_{k_D+1} \tag{14}$$

with

$$\bar{v}^D(\gamma) = \exp\left(\frac{\sum_{j=1}^{k_D}(\ln(\gamma C_j)/\lambda_j) - Y}{\sum_{j=1}^{k_D}(1/\lambda_j)}\right), \tag{15}$$

and

$$\psi_m = \frac{\sum_{j=1}^{m-1}(1/\lambda_j)}{\sum_{j=m}^{N}(1/\lambda_j)} \text{ for } m \in [1,N], \tag{16}$$

with $\psi_1 = 0, \psi_{N+1} = \infty$.

Lemma 2. *Let*

$$\psi_{k_D+1} > \frac{\bar{v}^D(\gamma)}{(1-\gamma)C}. \tag{17}$$

Then

(a) *There exists a unique integer* $t_\gamma \in [1,N]$ *such that either*

$$\psi_{t_\gamma} \leqslant \frac{\gamma C_{t_\gamma}}{(1-\gamma)C} \leqslant \psi_{t_\gamma+1} \tag{18}$$

or

$$\frac{\gamma C_{t_\gamma+1}}{(1-\gamma)C} < \psi_{t_\gamma+1} < \frac{\gamma C_{t_\gamma}}{(1-\gamma)C}. \tag{19}$$

(b) *Also,*

$$t_\gamma \begin{cases} = k_D, & \text{if (19) holds,} \\ < k_D, & \text{if (18) holds.} \end{cases} \tag{20}$$

(c) *In particular, if (17) holds then* $t_\gamma \leqslant k_D$.

(d) *If* $t_\gamma = k_D$ *then*

$$\gamma_- < \gamma < \gamma_+, \tag{21}$$

where

$$\gamma_- = \frac{C\psi_{k_D+1}}{C\psi_{k_D+1} + C_{k_D}} \text{ and } \gamma_+ = \frac{C\psi_{k_D+1}}{C\psi_{k_D+1} + C_{k_D+1}}. \tag{22}$$

Using these auxiliary lemmas and notation we can formulate the main result of this section.

Theorem 4. *In the first step, for a fixed* γ *the game with flexible resource allocation responses has an equilibrium* $((\boldsymbol{x}^D(\gamma), \boldsymbol{x}^R(\gamma)), \boldsymbol{y}(\gamma))$, *and the value* $v_A(\gamma)$ *are given in the following three cases.*

(a) For $\gamma = 1$ the equilibrium strategies and the value of the game are $((\boldsymbol{x}^D(\gamma), \boldsymbol{x}^R(\gamma)), \boldsymbol{y}(\gamma)) = ((\bar{\boldsymbol{x}}^D, \boldsymbol{x}^R), \bar{\boldsymbol{y}}^D)$ and $v_A(\gamma) = \bar{v}_A^D$, where $\boldsymbol{x}^R$ is any probability vector and $\bar{\boldsymbol{x}}^D, \bar{\boldsymbol{y}}^D$ and $\bar{v}_A^D$ are given by Theorem 1.

(b) For $\gamma = 0$ the equilibrium strategies and the value of the game are $((\boldsymbol{x}^D(\gamma), \boldsymbol{x}^R(\gamma)), \boldsymbol{y}(\gamma)) = ((\boldsymbol{x}^D, \bar{\boldsymbol{x}}^R), \bar{\boldsymbol{y}}^R)$ and $v_A(\gamma) = \bar{v}_A^R$, where $\boldsymbol{x}^D$ is any probability vector and $\bar{\boldsymbol{x}}^R, \bar{\boldsymbol{y}}^R$ and $\bar{v}_A^R$ are given by Theorem 2.

(c) For $\gamma \in (0, 1)$ the equilibrium strategies and the value of the game are specified by three subcases (c_i)–(c_{iii}).

(c_i) *Let*

$$\gamma \geqslant \gamma_*. \tag{23}$$

Then the equilibrium strategies and the value of the game are given as follows:

$$\boldsymbol{x}^D(\gamma) = \bar{\boldsymbol{x}}^D, \tag{24}$$

$$x_i^R(\gamma) = \begin{cases} 0, & i \leqslant k_D, \\ \frac{1/\lambda_i}{\sum_{j=k_D+1}^N (1/\lambda_j)}, & i > k_D, \end{cases} \tag{25}$$

$$\boldsymbol{y}(\gamma) = \bar{\boldsymbol{y}}^D, \tag{26}$$

and

$$v_A(\gamma) = \bar{v}^D(\gamma) + (1-\gamma)C. \tag{27}$$

(c_{ii}) *Let*

$$\gamma < \gamma_* \text{ and } \gamma \notin (\gamma_-, \gamma_+). \tag{28}$$

Then, $t_\gamma < k_D$. *The equilibrium strategies and the value of the game are given as follows*

$$x_i^D(\gamma) = \begin{cases} \frac{1/\lambda_i}{\sum_{j=1}^N (1/\lambda_j)} \left(1 + \frac{(1-\gamma)C}{\gamma C_{t_\gamma}}\right), & i < t_\gamma, \\ 1 - \left(1 + \frac{(1-\gamma)C}{\gamma C_{t_\gamma}}\right) \frac{\sum_{j=1}^{t_\gamma - 1} (1/\lambda_j)}{\sum_{j=1}^N (1/\lambda_j)}, & i = t_\gamma, \\ 0, & i > t_\gamma, \end{cases} \tag{29}$$

$$x_i^R(\gamma) = \begin{cases} 0, & i < t_\gamma, \\ 1 - \left(1 + \frac{\gamma C_{t_\gamma}}{(1-\gamma)C}\right) \frac{\sum_{j=t_\gamma+1}^N (1/\lambda_j)}{\sum_{j=1}^N (1/\lambda_j)}, & i = t_\gamma, \\ \frac{1/\lambda_i}{\sum_{j=1}^N \lambda_j} \left(1 + \frac{\gamma C_{t_\gamma}}{(1-\gamma)C}\right), & i > t_\gamma, \end{cases} \tag{30}$$

$$y_i(\gamma) = \begin{cases} \frac{Y + \sum_{j=1}^{t_\gamma} (1/\lambda_j) \ln(C_i/C_j)}{\sum_{j=1}^{t_\gamma} (1/\lambda_j)}, & i \leqslant t_\gamma, \\ \frac{Y + \sum_{j=1}^{t_\gamma} (1/\lambda_j) \ln(C_{t_\gamma}/C_j)}{\sum_{j=1}^{t_\gamma} (1/\lambda_j)}, & i > t_\gamma \end{cases} \tag{31}$$

and

$$v_A(\gamma) = ((1-\gamma)C + \gamma C_{t_\gamma}) \exp\left(\frac{\sum_{i=1}^{t_\gamma} \frac{\ln(C_i/C_{t_\gamma})}{\lambda_i} - Y}{\sum_{i=1}^N (1/\lambda_i)} \right). \tag{32}$$

(c_{iii}) *Let*

$$\gamma < \gamma_* \text{ and } \gamma \in (\gamma_-, \gamma_+). \tag{33}$$

Then, $t_\gamma = k_D$. *The equilibrium strategies and the value of the game are given as follows:*

$$x_i^D(\gamma) = \begin{cases} \frac{1/\lambda_i}{\sum_{j=1}^{t_\gamma} (1/\lambda_j)}, & i \leqslant t_\gamma, \\ 0, & i > t_\gamma, \end{cases} \tag{34}$$

$$x_i^R(\gamma) = \begin{cases} 0, & i \leqslant t_\gamma, \\ \frac{1/\lambda_i}{\sum_{j=t_\gamma+1}^N (1/\lambda_j)}, & t > t_\gamma, \end{cases} \tag{35}$$

$$y_i(\gamma) = \begin{cases} \frac{1}{\lambda_i} \ln\left(\frac{\gamma C_i \sum_{j=1}^N (1/\lambda_j)}{v_A(\gamma) \sum_{j=1}^{t_\gamma} (1/\lambda_j)} \right), & t \leqslant t_\gamma, \\ \frac{1}{\lambda_i} \ln\left(\frac{(1-\gamma)C \sum_{j=1}^N (1/\lambda_j)}{v_A(\gamma) \sum_{j=t_\gamma+1}^N (1/\lambda_j)} \right), & i > t_\gamma, \end{cases} \tag{36}$$

$$v_A(\gamma) = \sum_{m=1}^N (1/\lambda_m) \times e^{\frac{\sum_{j=1}^{t_\gamma} \frac{\ln\left(\frac{\gamma C_j}{\sum_{m=1}^{t_\gamma} \frac{1}{\lambda_m}}\right)}{\lambda_j} + \sum_{j=t_\gamma+1}^N \frac{\ln\left(\frac{(1-\gamma)C}{\sum_{m=t_\gamma+1}^N \frac{1}{\lambda_m}}\right)}{\lambda_j} - Y}{\sum_{j=1}^N (1/\lambda_j)}}. \tag{37}$$

In the second step, the adversary selects a γ to maximize its payoff, i.e., $\gamma^* = \arg\max_\gamma v_A(\gamma)$.

In particular, the theorem shows that the adversary's equilibrium strategy has node sharing structure, i.e., some nodes are identified with a maximal damage attack while some nodes are identified with a reconnaissance mission with overlapping intention of at most one node. Fig. 2 illustrates the dependence of subcases c_i, c_{ii} and c_{iii} on γ for the first step of the decision making scheme of the adversary.

If γ is large, namely, $\gamma > \gamma_*$, then the adversary's strategies do not depend on γ, and he applies the same strategy as if there were no reconnaissance threat at all.

If $\gamma \in (\gamma_-, \gamma_+)$ then the adversary's equilibrium strategies do not overlap. The switching node as well as the adversary's strategies do not depend on γ; meanwhile the protector's strategy depends on γ continuously.

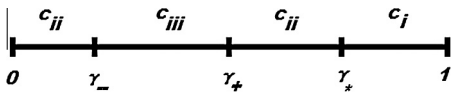

Fig. 2. Dependence of subcases c_i, c_{ii} and c_{iii} on γ.

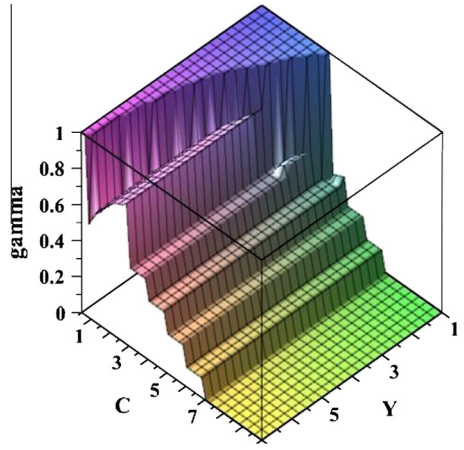

Fig. 3. Equilibrium probability γ for the scenario with flexible resource allocation strategies.

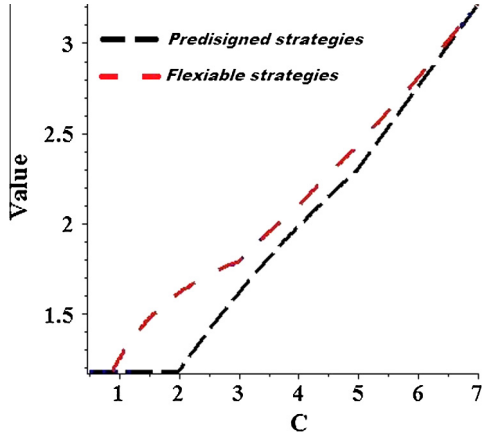

Fig. 4. The value of the game with flexible and predesigned resource allocation strategies for $Y = 7$.

If $\gamma \notin (\gamma_-, \gamma_+)$, $\gamma < \gamma_*$, then the adversary's equilibrium strategies share a node depending on γ, and the adversary's equilibrium strategies are continuous in γ; meanwhile the protector's strategy is a piecewise constant function of γ. It is interesting that this version of the game with flexible effort allocation also retains the phenomenon of possible cheating, combining it with straightforward behavior, which allows for an increase in the payoff to the adversary. Figs. 3 and 4 illustrate this phenomenon for $N = 9$ nodes, and $\boldsymbol{C} = (7, 6, 5, 4, 3, 1, 0.7, 0.5, 0.2)$, $\lambda = (1, 0.9, 0.8, 0.7, 0.6, 0.5, 0.4, 0.3, 0.2)$.

4. Conclusions

In this paper we have considered the incorporation in a network protection strategy of an adversary who as a decision-maker can choose the motivation of an attack: either to inflict maximal damage or to perform reconnaissance. This turns the adversary into a maxmaxmin decision-maker. This approach allows us to incorporate into the protection strategy the possibility that the adversary may try to deceive the protector, and also to observe an essential difference in designing the intrusion strategy by the adversary and the protection strategy by the protector. Figs. 1 and 3 illustrate that the adversary might make a sudden decision on the intrusion strategy he is going to apply, which is reflected by piece-wise continuous structure of the optimal probability of choosing the attack's type. Also, allowing flexible resource allocation strategies instead of predesigned ones yields an increasing number of such sudden decisions. In other words, the adversary's strategy might be sensitive to the network's parameters. Thus, the adversary might be inclined to make tactical decisions in attack's planning assuming sudden switches between attack types. Fig. 4 illustrates that for small or large value of the reconnaissance intrusion the selection of the attack's type is robust, while for intermediate such values the attack's type is not predetermined, and its selection is performed by a random mechanism. To meet with this uncertainty the protector has, in advance, to incorporate into its protection's strategy the possibility of such randomness in the adversary's behavior. Thus, the protector has to respond by planning the protection strategy to account for the tactical decision making approach of the adversary. So, the protector has to take such a strategic decision making approach as a basic principle for designing the protection strategy. A goal of our future research is to extend our approach to more sophisticated dynamic intrusion and protection scenarios involving the possibility of combining attack types based on the currently achieved result of the attack.

Appendix A. Proof of Theorem 1

Strategies $(\boldsymbol{x}, \boldsymbol{y})$ are equilibrium if and only if they are the best response for each other, i.e., $\boldsymbol{x} = \mathrm{BR}_A(\boldsymbol{y}) = \arg\max_{\boldsymbol{x}} v_A^D(\boldsymbol{x}, \boldsymbol{y})$ and $\boldsymbol{y} = \mathrm{BR}_P(\boldsymbol{x}) = \arg\min_{\boldsymbol{y}} v_A^D(\boldsymbol{x}, \boldsymbol{y})$. Then, since v_A^D is linear on $\boldsymbol{x}$ and convex on $\boldsymbol{y}$, strategies $(\boldsymbol{x}, \boldsymbol{y})$ are equilibrium if and only if there are v (the maximal coefficient of all x_i) and ω (a Lagrange multiplier) such that

$$C_i e^{-\lambda_i y_i} \begin{cases} = v, & x_i > 0, \\ \leqslant v, & x_i = 0, \end{cases} \tag{A.1}$$

$$C_i x_i \lambda_i e^{-\lambda_i y_i} \begin{cases} = \omega, & y_i > 0, \\ \leqslant \omega, & y_i = 0. \end{cases} \tag{A.2}$$

Then, (A.1) implies $v > 0$. Since there is at least one i such that $x_i > 0$, then (A.2) yields $\omega > 0$. Also, by (A.2), if $x_i = 0$ then $y_i = 0$. Then, by (1) and (A.1), there exists a k such that

$$C_{k+1} < v \leqslant C_k \text{ with } C_{N+1} = 0, \tag{A.3}$$

and

$$y_i = \begin{cases} \ln(C_i/v)/\lambda_i, & i \leqslant k, \\ 0, & i > k+1. \end{cases} \tag{A.4}$$

Summing up (A.4) we obtain that

$$Y = \sum_{i=1}^{k} y_i = \sum_{i=1}^{k} \frac{\ln(C_i/v)}{\lambda_i}. \tag{A.5}$$

Thus,

$$\ln(v) = \left(\sum_{i=1}^{k} (\ln(C_i)/\lambda_i) - Y \right) \Big/ \left(\sum_{i=1}^{k} (1/\lambda_i) \right). \tag{A.6}$$

Substituting (A.6) into (A.3) implies the switching node k is defined by:

$$\ln(C_{k+1}) < \frac{\sum_{i=1}^{k} (\ln(C_i)/\lambda_i) - Y}{\sum_{i=1}^{k} (1/\lambda_i)} \leqslant \ln(C_k).$$

This condition is equivalent to (3) with φ_k given by (4). Thus, $k \equiv k_D$, and (5) follows.

Since v_A^D is linear on $\boldsymbol{x}$, then (A.1) implies that v is the value of the game. Thus, (A.6) yields (2) with

$$\bar{v}^D = v. \tag{A.7}$$

First note that, by (1), (A.1), (A.3) and (A.4), $x_i = 0$ for $i \geqslant k_D + 1$.

To find the equilibrium strategy $\boldsymbol{x}$ we have to consider separately two cases: (a) $\bar{v}^D \neq C_{k_D}$, and (b) $\bar{v}^D = C_{k_D}$.

(a) Let $\bar{v}^D \neq C_{k_D}$. Then, by (A.4),

$$y_i \begin{cases} > 0, & i \leqslant k_D, \\ = 0, & i \geqslant k_D + 1. \end{cases}$$

Then, by (A.2) and (A.4), we have that

$$x_i = \begin{cases} \omega/(\lambda_i v), & i \leqslant k_D, \\ 0, & i \geqslant k_D + 1. \end{cases}$$

Since $\boldsymbol{x}$ is a probability vector, (6) follows.

(b) Let $\bar{v}^D = C_{k_D}$. Then by (A.4)

$$y_i \begin{cases} > 0, & i \leqslant k_D - 1, \\ = 0, & i \geqslant k_D. \end{cases}$$

For $\boldsymbol{x}$ we still have $x_i > 0$ for $i \leqslant k_D - 1$, and we also have that $x_{k_D} \geqslant 0$. Then, since $v = C_{k_D}$, by (A.2) and (A.4), we have that

$$x_i = \begin{cases} \omega/(\lambda_i C_{k_D}), & i \leqslant k_D - 1, \\ x_{k_D}, & i = k_D, \\ 0, & i \geqslant k_D + 1, \end{cases} \tag{A.8}$$

for any

$$0 \leqslant x_{k_D} \leqslant \omega/(\lambda_{k_D} C_{k_D}). \tag{A.9}$$

Since $\boldsymbol{x}$ is a probability vector, $x_{k_D} = 1 - \sum_{i=1}^{k_D - 1} x_i$. Then, by (A.8), the inequalities (A.9) are equivalent to

$$C_{k_D} \Big/ \left(\sum_{i=1}^{k_D} (1/\lambda_i) \right) \leqslant \omega \leqslant C_{k_D} \Big/ \left(\sum_{i=1}^{k_D - 1} (1/\lambda_i) \right),$$

and (7) follows.

Appendix B. Proof of Theorem 3

By (10), if $a_{21} C < a_{11}$, then strategy $\bar{\boldsymbol{x}}^D$ dominates strategy $\bar{\boldsymbol{x}}^R$, and if $a_{12} C > a_{22}$ then strategy $\bar{\boldsymbol{x}}^R$ dominates strategy $\bar{\boldsymbol{x}}^D$ for the adversary, and (a) and (b) follow. For (c), by (10), there are no saddle points in pure strategies. Thus, there is the unique mixed equilibrium (for 2×2 zero sum game it is an equalizing one), and the result follows.

Appendix C. Proof of Lemma 1

It is clear that $\frac{\bar{v}^D(\gamma)}{(1-\gamma)C}$ is an increasing function from zero for $\gamma \downarrow 0$ to infinity for $\gamma \uparrow 1$, and the result follows.

Appendix D. Proof of Lemma 2

(a) Since ψ_t is increasing from 0 for $t = 1$ to infinity for $t = N + 1$ and C_t is decreasing from $C_1 > 0$ for $t = 1$ to 0 for $t = N + 1$, there exists a unique t such that

$$\frac{\gamma C_t}{(1-\gamma)C} \geqslant \psi_t \tag{D.1}$$

and

$$\frac{\gamma C_{t+1}}{(1-\gamma)C} < \psi_{t+1}. \tag{D.2}$$

For such t one of the following inequalities must hold:either

$$\frac{\gamma C_t}{(1-\gamma)C} \leqslant \psi_{t+1} \tag{D.3}$$

or

$$\frac{\gamma C_t}{(1-\gamma)C} > \psi_{t+1}. \tag{D.4}$$

Then, (D.1) and (D.3) imply (18). Also, (D.2) and (D.4) yield (19) with $t_\gamma = t$.

(b) Recall that by definition of k_D we have that

$$\sum_{j=1}^{k_D} \frac{1}{\lambda_j} \ln \left(\frac{\gamma C_i}{\bar{v}^D(\gamma)} \right) = Y \tag{D.5}$$

and

$$\gamma C_{k_D+1} < \bar{v}^D(\gamma) \leqslant \gamma C_{k_D}. \tag{D.6}$$

Then, by (17) and (D.6),

$$\frac{\gamma C_{k_D+1}}{(1-\gamma)C} < \frac{\gamma \bar{v}^D(\gamma)}{(1-\gamma)C} < \psi_{k_D+1}. \tag{D.7}$$

So, only the following two subcases can hold:

$$\frac{\gamma C_{k_D+1}}{(1-\gamma)C} < \frac{\bar{v}^D(\gamma)}{(1-\gamma)C} < \psi_{k_D+1} \leqslant \frac{\gamma C_{k_D}}{(1-\gamma)C} \tag{D.8}$$

and

$$\frac{\gamma C_{k_D+1}}{(1-\gamma)C} < \frac{\bar{v}^D(\gamma)}{(1-\gamma)C} \leqslant \frac{\gamma C_{k_D}}{(1-\gamma)C} < \psi_{k_D+1}. \tag{D.9}$$

If (D.8) holds, then, by (19), $k_D = t_\gamma$. Meanwhile, since ψ_i is increasing, by (18), (D.9) implies that $t_\gamma < k_D$.

(c) follows from (b).

(d) follows from (19) with $t_\gamma = k_D$.

Appendix E. Proof of Theorem 4

(a) and (b) are obvious.

(c) For a fixed $\gamma \in (0,1)$, $((\boldsymbol{x}^D(\gamma), \boldsymbol{x}^R(\gamma)), \boldsymbol{y}(\gamma))$ is an equilibrium if and only if there are v^D, v^R (the maximal coefficients of all x_i in maximal damage and reconnaissance components of the adversary's payoff) and ω (a Lagrange multiplier) such that the following relations hold:

$$\gamma C_i e^{-\lambda_i y_i} \begin{cases} = v^D, & x_i^D > 0, \\ \leqslant v^D, & x_i^D = 0, \end{cases} \tag{E.1}$$

$$(1-\gamma) C e^{-\lambda_i y_i} \begin{cases} = v^R, & x_i^R > 0, \\ \leqslant v^R, & x_i^R = 0 \end{cases} \tag{E.2}$$

and

$$\left(\gamma C_i x_i^D + (1-\gamma) C x_i^R \right) \lambda_i e^{-\lambda_i y_i} \begin{cases} = \omega, & y_i > 0, \\ \leqslant \omega, & y_i = 0. \end{cases} \tag{E.3}$$

To find an equilibrium we consider separately two subcases that can arise:

(A) There exists an i such that $y_i = 0$, (E.4)

(B) $y_i > 0$ for all i. (E.5)

(A) Let (E.4) hold. We will find a necessary and sufficient condition for existence of such an equilibrium strategy of the adversary. First note that (E.2) yields

$$x_j^R \begin{cases} \geqslant 0, & y_j = 0, \\ = 0, & y_j > 0, \end{cases} \tag{E.6}$$

and, (E.1) and (E.3) imply

$$x_j^D \begin{cases} > 0, & y_j > 0, \\ = 0, & y_j = 0. \end{cases} \tag{E.7}$$

Thus, (E.1) and (E.3), following the proof of Theorem 1, imply that

$$\boldsymbol{x}^D(\gamma)=\bar{\boldsymbol{x}}^D,\quad \boldsymbol{y}(\gamma)=\bar{\boldsymbol{y}}^D, \tag{E.8}$$

and

$$\gamma C_{k_D+1}<v^D\leqslant\gamma C_{k_D}, \tag{E.9}$$

where v^D equals to $\bar{v}^D$ from (2) with substitution of C_i by γC_i. Thus, $v^D=\bar{v}^D(\gamma)$ given by (15). By (E.1), (E.3) and (E.8) we have that

$$\omega=\frac{\bar{v}^D(\gamma)}{\sum_{j=1}^{k_D}(1/\lambda_j)}. \tag{E.10}$$

Also, by (E.1), (E.3), (E.8) and (E.10), $\boldsymbol{x}^R$ has to be any probability vector such that

$$x^R=0 \text{ for } i\leqslant k_D \tag{E.11}$$

and

$$\begin{aligned} x_i^R&\leqslant\frac{\omega/\lambda_i}{(1-\gamma)C}=\frac{\bar{v}^D(\gamma)}{(1-\gamma)C}\frac{1/\lambda_i}{\sum_{j=1}^{k_D}(1/\lambda_j)}\\ &=\frac{\bar{v}^D(\gamma)}{(1-\gamma)C\psi_{k_D+1}}\frac{1/\lambda_i}{\sum_{j=k_D+1}^{N}(1/\lambda_j)} \text{ for } i>k_D. \end{aligned} \tag{E.12}$$

Such a probability vector $\boldsymbol{x}^R$ exists if and only if (14) holds. In particular, $\boldsymbol{x}^R$ is given by (25) is a probability vector, and (c_i) follows.

(B) Let (E.5) hold. We will find necessary and sufficient conditions for such an equilibrium strategy, $\boldsymbol{y}$, to exist. First note that, by (1), there exists at most one t such that $x_t^R>0$ and $x_t^D>0$, since if such a t exists, then (E.1) and (E.2) yield that

$$\frac{\gamma C_t}{(1-\gamma)C}=\frac{v^D}{v^R}. \tag{E.13}$$

Also, (E.1) and (E.2) imply that

$$\frac{\gamma C_i}{(1-\gamma)C}\geqslant\frac{v^D}{v^R} \text{ if } x_i^D>0, x_i^R=0 \tag{E.14}$$

and

$$\frac{\gamma C_i}{(1-\gamma)C}\leqslant\frac{v^D}{v^R} \text{ if } x_i^D=0, x_i^R>0. \tag{E.15}$$

Thus, for equilibrium strategies $\boldsymbol{x}^D$ and $\boldsymbol{x}^R$ the following conditions have to hold:

$$x_i^D\begin{cases}>0, & i\leqslant t,\\ =0, & i>t\end{cases} \text{ and } x_i^R\begin{cases}=0, & i\leqslant t-1,\\ >0, & i>t-1\end{cases} \tag{E.16}$$

or

$$x_i^D\begin{cases}>0, & i\leqslant t,\\ =0, & i>t,\end{cases} \text{ and } x_i^R\begin{cases}=0, & i\leqslant t,\\ >0, & i>t.\end{cases} \tag{E.17}$$

We consider separately these two cases: (B_i) (E.16) holds, and (B_{ii}) (E.17) holds.

(B_i) Let (E.16) hold. Then by (E.1), (E.2) and (E.3) and the fact that $\boldsymbol{x}^D$ and $\boldsymbol{x}^R$ are probability vectors we have that

$$\begin{aligned} x_i^D&=\begin{cases}\omega/(v^D\lambda_i), & i\leqslant t-1,\\ 1-\sum_{j=1}^{t-1}(\omega/(v^D\lambda_j)), & i=t,\\ 0, & i\geqslant t+1,\end{cases}\\ x_i^R&=\begin{cases}0, & i\leqslant t-1,\\ 1-\sum_{j=t+1}^{N}(\omega/(v^R\lambda_j)), & i=t,\\ \omega/(v^R\lambda_i), & i\geqslant t+1\end{cases} \end{aligned} \tag{E.18}$$

and

$$y_i=\begin{cases}\ln\left(\gamma C_i/v^D\right)/\lambda_i, & i\leqslant t,\\ \ln\left((1-\gamma)C/v^R\right)/\lambda_i, & i\geqslant t+1.\end{cases} \tag{E.19}$$

Also, by (E.1) and (E.18) we have that

$$v^D<\gamma C_t. \tag{E.20}$$

Substituting (E.18) and (E.19) for $i=t$ into (E.3) implies that

$$\omega=\frac{v^D+v^R}{\sum_{j=1}^{N}(1/\lambda_j)}. \tag{E.21}$$

Using (E.13) and (E.19) we can find that

$$\begin{aligned} \omega&=\frac{1+\gamma C_t/((1-\gamma)C)}{\sum_{j=1}^{N}(1/\lambda_j)}v^R\\ &=\frac{1+(1-\gamma)C/(\gamma C_t)}{\sum_{j=1}^{N}(1/\lambda_j)}v^D. \end{aligned} \tag{E.22}$$

For positive v^D, v^R, and ω, the vectors $\boldsymbol{x}^D$ and $\boldsymbol{x}^R$ given by (E.18) are probability vectors if and only if

$$\sum_{j=1}^{t-1}\frac{1}{\lambda_j}\leqslant\frac{v^D}{\omega} \text{ and } \sum_{j=t+1}^{N}\frac{1}{\lambda_j}\leqslant\frac{v^R}{\omega}.$$

By (E.22), the last two inequalities are equivalent to (18) Thus, $t=t_\gamma$. By Lemma 2, $t_\gamma<k_D$, and it follows that condition (28) of case (c_{ii}) holds.

Substituting (E.13) into (E.19) and summing up these y_i imply that for the equilibrium $\boldsymbol{y}$ the following condition has to hold:

$$\begin{aligned} &\sum_{i=1}^{t_\gamma}\frac{1}{\lambda_i}\ln\left(\frac{\gamma C_i}{\omega\sum_{j=1}^{N}(1/\lambda_j)}\left(1+\frac{(1-\gamma)C}{\gamma C_{t_\gamma}}\right)\right)\\ &+\sum_{i=t_\gamma+1}^{N}\frac{1}{\lambda_i}\ln\left(\frac{(1-\gamma)C}{\omega\sum_{j=1}^{N}(1/\lambda_j)}\left(1+\frac{\gamma C_{t_\gamma}}{(1-\gamma)C}\right)\right)=Y. \end{aligned} \tag{E.23}$$

The left-side of Eqn. (E.23) is defined for $\omega\in(0,(\gamma C_{t_\gamma}+(1-\gamma)C)/\sum_{j=1}^{N}(1/\lambda_j)]$ and it is decreasing in ω from infinity for $\omega\downarrow 0$ to φ_{t_γ} for $\omega=(\gamma C_{t_\gamma}+(1-\gamma)C)/\sum_{j=1}^{N}(1/\lambda_j)$ with φ_m given by (3). Since $t_\gamma<k_D$, $\boldsymbol{y}$ is a positive vector, and (c_{ii}) follows.

(B_{ii}) Let (E.17) hold. Then, by (E.14) and (E.15), we have that

$$\frac{\gamma C_{t+1}}{(1-\gamma)C}<\frac{v^D}{v^R}<\frac{\gamma C_t}{(1-\gamma)C}. \tag{E.24}$$

Also, (E.1), (E.2) and the fact that $\boldsymbol{x}^D$ and $\boldsymbol{x}^R$ are probability vectors imply that

$$\begin{aligned} x_i^D&=\begin{cases}\frac{\omega}{\lambda_i v^D}, & i\leqslant t,\\ 0, & i>t\end{cases}\\ x_i^R&=\begin{cases}0, & i\leqslant t,\\ \frac{\omega}{\lambda_i v^R}, & i>t\end{cases} \end{aligned} \tag{E.25}$$

with

$$\frac{v^D}{\omega}=\sum_{i=1}^{t}\frac{1}{\lambda_i} \text{ and } \frac{v^R}{\omega}=\sum_{i=t+1}^{N}\frac{1}{\lambda_i}. \tag{E.26}$$

Substituting (E.26) into (E.24) implies that t is given by the condition

$$\frac{\gamma C_{t+1}}{(1-\gamma)C}<\frac{\sum_{i=1}^{t}(1/\lambda_i)}{\sum_{i=t+1}^{N}(1/\lambda_i)}<\frac{\gamma C_t}{(1-\gamma)C}. \tag{E.27}$$

Since $\frac{\sum_{i=1}^{t}(1/\lambda_i)}{\sum_{i=t+1}^{N}(1/\lambda_i)}=\psi_{t+1}$, (E.27) is equivalent to (19). Thus, $t=t_\gamma$. Moreover, by Lemma 2, $t_\gamma=k_D$, and condition (33) of case (c_{iii}) holds.

The strategy $\boldsymbol{y}$ has to be given by (E.19). Substituting (E.26) into (E.19) yields that ω has to satisfy the following equation:

$$\sum_{i=1}^{t_\gamma} \frac{1}{\lambda_i} \ln\left(\frac{\gamma C_i}{\omega \sum_{j=1}^{t_\gamma}(1/\lambda_j)}\right) + \sum_{i=t_\gamma+1}^{N} \frac{1}{\lambda_i} \ln\left(\frac{(1-\gamma)C}{\omega \sum_{j=t_\gamma+1}^{N}(1/\lambda_j)}\right) = Y. \tag{E.28}$$

The last equation has a root $\omega \in \left(0, \frac{\sum_{j=t_\gamma+1}^{N}(1/\lambda_j)}{(1-\gamma)C}\right)$ if and only if the following condition holds:

$$\sum_{i=1}^{t_\gamma} \frac{1}{\lambda_i} \ln\left(\frac{\gamma C_i}{(1-\gamma)C\psi_{t_\gamma+1}}\right) < Y.$$

Since $t_\gamma = k_D$, by (17), this inequality holds, and (c_{iii}) follows.

References

Agah, A., Das, S. K., Basu, K., & Asadi, M. (2007). Intrusion detection in sensor networks: A non-cooperative game approach. In *IEEE international symposium on network computing and applications*.

Baston, V. J., & Garnaev, A. Y. (2000). A search game with a protector. *Naval Research Logistics, 47*, 85–96.

Baykal-Gursoy, M., Duan, Z., Poor, H. V., & Garnaev, A. (2014). Infrastructure security games. *European Journal of Operational Research, 239*, 469–478.

Fudenberg, D., & Tirole, J. (1991). *Game theory*. Boston, MA: MIT Press.

Garnaev, A., Baykal-Gursoy, M., & Poor, H. V. (2014). Incorporating attack-type uncertainty into network protection. *IEEE Transactions on Information Forensics and Security, 9*, 1278–1287.

Garnaev, A., & Trappe, W. (2014). Bandwidth scanning involving a Bayesian approach to adapting the belief of an adversary's presence. In *2014 IEEE conference on communications and network security (CNS)* (pp. 35–43).

Garnaev, A., & Trappe, W. (2015). One-time spectrum coexistence in dynamic spectrum access when the secondary user may be malicious. *IEEE Transactions on Information Forensics and Security, 10*, 1064–1075.

Garnaev, A., Trappe, W., & Kung, C.-T. (2012). Dependence of optimal monitoring strategy on the application to be protected. In *2012 IEEE global communications conference (GLOBECOM)* (pp. 1054–1059).

Garnaev, A., Trappe, W., & Kung, C.-T. (2013). Optimizing scanning strategies: Selecting scanning bandwidth in adversarial RF environments. In *Proceedings of the 8th international conference on cognitive radio oriented wireless networks (CROWNCOM)* (pp. 148–153).

Guikema, S. (2009). Game theory models of intelligent actors in reliability analysis: An overview of the state of the art. In V. Bier & M. Azaiez (Eds.), *Game theoretic risk analysis of security threats* (pp. 13–32). Springer.

Hausken, K., & Levitin, G. (2012). Review of systems defense and attack models. *International Journal of Performability Engineering, 8*, 355–366.

Iida, K., Hohzaki, R., & Sato, K. (1994). Hide-and-search game with the risk criterion. *Journal of Operations Research Society of Japan, 37*, 287–296.

Konak, A., Kulturel-Konak, S., & Snyder, L. (2015). A game-theoretic genetic algorithm for the reliable server assignment problem under attacks. *Computers & Industrial Engineering, 85*, 73–85.

Kumar, S., & Liu, J. (2014). Impact of terrorism on international stock markets. *Journal of Applied Business and Economics, 14*, 42–60.

Levitin, G., Hausken, K., Taboada, H., & Coit, D. (2012). Data survivability vs. security in information systems. *Reliability Engineering & System Safety, 100*, 19–27.

Lewis, T. (2009). *Network science: Theory and applications*. John Wiley and Sons, Inc.

Li, F., & Wu, J. (2008). Hit and run: A Bayesian game between malicious and regular nodes in MANETs. In *5th Annual IEEE communications society conference on sensor, mesh and ad hoc communications and networks (SECON)* (pp. 432–440).

Liu, Y., Comaniciu, C., & Mani, H. (2006). A Bayesian game approach for intrusion detection in wireless ad hoc networks. In *First international conference on performance evaluation methodologies and tools (Valuetools)*.

Magnuson, S. (2014). Power companies struggle to maintain defenses against cyber-attacks. National Defense, NDIA's Business and Technology Magazine, March.

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

Mueller, J., & Stewart, M. (2011). Does the United States spend too much on homeland security? *Slate*. September 7.

NRC (2008). *Department of homeland security bioterrorism risk assessment: A call for change*. Washington, DC: National Academies Press. http://www.nap.edu/catalog.php?record_id=12206.

Rainie, L., Anderson, J., & Connolly, J. (2014). Cyber attacks likely to increase. Pew Research Center, October 29.

Ren, X., Mo, Y., & Shi, L. (2014). Optimal DoS attacks on Bayesian quickest change detection. In *53rd IEEE conference on decision and control (CDC)* (pp. 3765–3770).

Sakaguchi, M. (1973). Two-sided search games. *Journal of the Operations Research Society of Japan, 16*, 207–225.

Stone, L. (2007). Theory of optimal search. MAS.

Tambe, M., Jiang, A., An, B., & Jain, M. (2012). Computational game theory for security: Progress and challenges. In *AAAI spring symposium on applied computational game theory*.

Zengerle, P. (2014). NSA chief warns Chinese cyber attacks could shut U.S. infrastructure. The reuters, November 21.