A Reinforcement Protection Game in the Internet of Things

Andrey Garnaev[1,2(✉)] and Wade Trappe[2]

[1] Saint Petersburg State University, St. Petersburg, Russia
garnaev@yahoo.com
[2] WINLAB, Rutgers University, North Brunswick, USA
trappe@winlab.rutgers.edu

Abstract. The vast scale of the Internet of Things (IoT), combined with its heterogeneous nature involving many different types of devices and machines, could lead the IoT to be vulnerable to a variety of security threats and malicious attacks. Addressing the broad array of threats requires that different security mechanisms are deployed at appropriate locations within the broader IoT communication network. In this paper, we examine this problem by applying a resource allocation approach involving a game-theoretical framework to model: (a) an attack aimed to maximize total damage to the network, and (b) an attack aimed to compromise at least one of the devices. To evaluate the probability of a successful attack we apply a contest success function, and found the associated equilibrium strategies in closed form. Additionally, we note an interesting relationship between equilibrium strategies in security reinforcement games and OFDM transmission games under hostile jamming. A criteria is designed that allows one to determine whether an IoT controller's resources is sufficient to protect all of the IoT devices it manages.

Keywords: IoT · Security · Compromised devices · Nash equilibrium

1 Introduction

The Internet of Things (IoT) is an emerging technology consisting of countless devices that were not traditionally associated with the Internet (such as TVs, thermostats, lighting appliances, coffeemakers, etc.), but are now being attached to the broader Internet. As these devices are deployed alongside next generation network protocols, they will be remotely accessible, allowing them to be monitored, updated, and reprogrammed. Unfortunately, with this increased connectivity comes the increased likelihood that they will be the target of malicious attacks.

Due to the large scale and heterogeneous nature of the devices involved (especially as many will have varying security capabilities), the IoT could end up more vulnerable to variety of security threats (such as cyber attacks or radio interference attacks [24]) than the Internet we have been familiar with. The recent the

G. Fortino et al. (Eds.): InterIoT 2017/SaSeIoT 2017, LNICST 242, pp. 85–95, 2018.
https://doi.org/10.1007/978-3-319-93797-7_11

WannaCry virus attack [11] and demonstration of a thermostat ransomware hack [22], where the thermostat was set to 99°, and control would only be returned if the target paid Bitcoin to the cyber attackers, illustrated that such cyber attack will have unprecedented speed and scale, and might be especially dangerous as they can influence the physical world around us.

The large scale and heterogeneity of security capabilities makes developing and deploying anti-adversary strategies more challenging than in traditional networks [3]. One of the tools that has been used extensively in the literature to model different adversarial attacks on the IoT, as well as in the other networks, is game theory [13]. This is motivated by the fact that in such a security problem, there are at least two agents (e.g., the IoT controller and the adversary) that are present, and each of them has its own objective. For such a multi-agent problem, game theory supplies the foundations for developing and understanding the form that solutions should take [13]. As examples, we refer the readers to [17] for a Colonel Blotto game formalism, that arrives at a lower bound on SINR as a criteria for successful communication, and an evolutionary algorithm is devised that involves a centralized anti-jamming approach for an OFDM-based IoT system, where the IoT controller faces an adversarial attack aimed at maximizing the number of devices that cannot communicate with each other. In [15], signaling games were used to model honeypot-based deception mechanism to ensure security. In [16], a model motivated by low throughput networks was presented that models an attack where the adversary wants to maximize the number of compromised nodes while avoiding detection. In [18], a bi-matrix game was employed to model a choice of the subset of prosumers to share data if one of the prosumers can be compromised. In [19], an anomaly detection technique for low-resource IoT devices based on Nash equilibrium was suggested.

In this paper, motivated by the recent (and extremely rapid world-wide spread) WannaCry virus attack, in which many IoT devices were compromised throughout the world, we look at IoT security from a different angle. Namely: *how should the IoT controller allocate its protection reinforcement efforts in a heterogeneous network to minimize possible damage?* Here we quantify the damage involved by either the total number of compromised devices or the possibility that just one device will be compromised. The last scenario is important since, if a device inside of a corporate network is compromised, it makes it much easier for thieves to gain access to workstations and servers, and thus it is desirable to minimize the likelihood of a single device being compromised. To model the problem, we apply a resource allocation approach, which has been used extensively to model different network/communication security problems. As examples, we refer the readers to [21] for design multiband transmission protocol under jamming, to [6] for modeling one-time spectrum coexistence in dynamic spectrum access, to [23] for fair and efficient resource allocation in cloud computing, to [5,7–9] for bandwidth scanning strategy and to [2] for network protection.

The organization of this paper is as follows: in Sect. 2, two game-theoretical models for security reinforcement are formulated. In Sect. 3, for the first model dealing with minimizing the total damage (number of devices) to the network,

equilibrium strategies are found. In Sect. 4, for the second model dealing with maximizing probability for the network not to be compromised, equilibrium strategies are designed. Finally, in Sect. 5, discussion of the obtained results is offered, and, in Appendix, the proofs of the obtained results are given.

2 Model

In the paper, we consider an IoT system consisting of a set of IoT devices located in a (protected) zone, connected to each other for the purpose of communicating and sharing data. We will abstract the notion of the network and not specify any particular topology, but instead consider just a subset D of the protected zone. This set consists of a finite number (say, n) of devices, i.e., $D = \{1, \ldots, n\}$. The devices are under attack by an adversary attempting to intrude on the protected zone in order to perform a damaging action (e.g. to steal data). To perform intrusion, the adversary also has some resources, for example this might be a number of compromised devices attacking the network. The total adversary's resources are X. To reinforce the network's protection, the IoT controller also has some resources (e.g., it can be related to the amount of time devoted to remote scanning and attestation of a device). The total IoT controller's resources is Y. Let y_t be the reinforcement effort the IoT controller applies to protect device t, and x_t be the resource applied by the adversary to infect/intrude into the device t. Thus, the set of feasible strategies to the adversary is $\Pi_A = \{\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n_+ : \sum_{t \in D} x_t = X\}$. Similarly, the set of feasible strategies for the IoT controller is $\Pi_C = \{\boldsymbol{y} = (y_1, \ldots, y_n) \in \mathbb{R}^n_+ : \sum_{t \in D} y_t = Y\}$. Let $P_t(x, y)$ be the probability of a successful intrusion into a device t of the network, when the protection effort x_t and intrusion effort y_t are employed. In this paper, we assume that this probability is proportional to the fraction of effort put into the attack, that is

$$P_t(\boldsymbol{x}, \boldsymbol{y}) = \alpha_t x_t / (d_t + \alpha_t x_t + \beta_t y_t), \tag{1}$$

where d_t is an initial level of the device's security, α_t and β_t are coefficients associated with the protection sensitivity to attack and protection efforts. The provability (1) is given by the ratio form contest success function commonly used in the attack-defense literature [4,12,14,20].

To avoid bulkiness in formulas we introduce the notation: $\alpha_t := \alpha_t / d_t$ and $\beta_t := \beta_t / d_t$. In the new notation, (1), reflects the probability of a successful attack on the device t, and becomes

$$P_t(\boldsymbol{x}, \boldsymbol{y}) = \alpha_t x_t / (1 + \alpha_t x_t + \beta_t y_t). \tag{2}$$

Then, the probability that no device has been compromised, is

$$Q(\boldsymbol{x}, \boldsymbol{y}) = \prod_{t \in D} (1 - P_t(\boldsymbol{x}, \boldsymbol{y})). \tag{3}$$

We now consider the two different goals for the IoT controller.

The goal of the IoT controller is to minimize total damage to the network. Let R_t be the value of device t, which reflects the reward to the adversary for successful intrusion of the network at node t. Then, the expected total damage is given as follows:

$$v_A(\boldsymbol{x}, \boldsymbol{y}) = \sum_{t \in D} R_t P_t(\boldsymbol{x}, \boldsymbol{y}). \tag{4}$$

In particular, for $R \equiv 1$, v_A is the expected number of devices that might be compromised by the adversary's attack. The v_A can be considered as a payoff to the adversary, which he aims to maximize. For the IoT controller, on the other hand, it is a cost function to be minimized. We assume that the agents have complete information about the parameters of the networks, i.e., α, β and R as well as on the total resources X and Y they have in their disposition. This scenario is described by a zero-sum game, and we look for an equilibrium [13]. Recall that, for a pair of strategies $(\boldsymbol{x}_*, \boldsymbol{y}_*)$ is an equilibrium in a zero-sum game if and only if the following inequalities hold for each $(\boldsymbol{x}, \boldsymbol{y})$:

$$v_A(\boldsymbol{x}, \boldsymbol{y}_*) \le v_A(\boldsymbol{x}_*, \boldsymbol{y}_*) \le v_A(\boldsymbol{x}_*, \boldsymbol{y}), \tag{5}$$

where $v_A(\boldsymbol{x}_*, \boldsymbol{y}_*)$ is called the value of the game. Even if there are several equilibria, each of them returns the same value of the game, i.e., the value of the game uniquely defined by (5).

The goal of the IoT controller is to maximize the probability that no device will be compromised. In this case, the payoff to the IoT controller is $Q(\boldsymbol{x}, \boldsymbol{y})$, while for the adversary this is its cost function. Again, this is a zero sum game and we look for the equilibrium strategies.

3 The Minimizing Total Damage Game

In this section, we find the equilibrium strategies for the game involving minimizing the total damage.

Theorem 1. *(a) In the minimizing total damage game, each equilibria has to have the form* $(\boldsymbol{x}, \boldsymbol{y}) = (\boldsymbol{x}_{\omega,\nu}, \boldsymbol{y}_{\omega,\nu})$ *where* ω *and* ν *are positive parameters and*

$$x_{\omega,\tau,t} = \begin{cases} R_t \alpha_t \beta_t \tau / (\omega \left(\tau \alpha_t + \beta_t\right)^2), & t \in I^{11}_{\omega,\tau}, \\ \left(\sqrt{R_t \alpha_t / \omega} - 1\right) / \alpha_t, & t \in I^{10}_{\omega,\tau}, \\ 0, & t \in I^{00}_{\omega,\tau}, \end{cases} \tag{6}$$

$$y_{\omega,\tau,t} = \begin{cases} R_t \alpha_t \beta_t / (\omega \left(\alpha_t \tau + \beta_t\right)^2) - 1/\beta_t, & t \in I^{11}_{\omega,\tau}, \\ 0, & t \notin I^{11}_{\omega,\tau}, \end{cases} \tag{7}$$

where

$$I^{00}_{\omega,\tau} := \{t : R_t \alpha_t / \omega \le 1\}, \; I^{10}_{\omega,\tau} := \left\{t : 1 < \sqrt{R_t \alpha_t / \omega} \le 1 + (\alpha_t / \beta_t)\tau\right\},$$
$$I^{11}_{\omega,\tau} := \left\{t : 1 + (\alpha_t \beta_t)\tau < \sqrt{R_t \alpha_t / \omega}\right\}. \tag{8}$$

(b) Functions $S_x(\omega,\tau) := \sum_{t\in D} x_{\omega,\tau,t}$ *and* $S_y(\omega,\tau) := \sum_{t\in D} y_{\omega,\tau,t}$ *have the following properties:*

(b-a) For a fixed $\tau > 0$, $S_y(\omega,\tau)$ *is continuous on* ω *and decreasing from infinity for* $\omega \downarrow 0$ *to zero for* $\omega \geq \max_t \alpha_t/(1+\alpha_t\tau/\beta_t)^2$.

(b-b) For a fixed $\omega > 0$, $S_y(\omega,\tau)$ *is continuous on* τ *and decreasing from* $S_y(\omega,0) = \sum_{t\in D}(1/\beta_t)\lfloor R_t\alpha_t/\omega - 1\rfloor_+$ *for* $\tau = 0$ *to zero for large* τ.

(b-c) For a fixed τ *there is a unique* $\Omega(\tau)$ *such that*

$$S_y(\Omega(\tau),\tau) = Y. \tag{9}$$

Moreover, due to the monotonicity properties given in (a), the $\Omega(\tau)$ *can be found by bisection method.*

(b-d) $\Omega(\tau)$ *is a continuous and decreasing function from* Ω_0 *for* $\tau = 0$ *to zero, while* τ *tends to infinity, where* Ω_0 *is the unique positive root of the equation:* $\sum_{t\ D}(1/\beta_t)\lfloor R_t\alpha_t/\Omega_0 - 1\rfloor_+ = Y$.

(b-e) $\Omega(\tau) \sim \Omega_\infty/\tau^2$ *for* τ *tending to infinity, where* Ω_∞ *is the unique positive root of the equation:* $\sum_{t\in D}\lfloor R_t\beta_t/(\alpha_t\Omega_\infty) - 1/\beta_t\rfloor_+ = Y$.

(c) The value of the parameters, ω *and* τ*, can be found based on the condition that the resource budgets have to be fully utilized by both agents, i.e., as a solution of equations* $S_x(\omega,\tau) = X$ *and* $S_y(\omega,\tau) = Y$ *in two steps:*

(c-a) For each τ*, find* $\omega = \Omega(\tau)$ *as the unique root of (9) by bisection method.*

(c-b) Since $S_x(\Omega(0),0) = 0$ *and* $S_x(\Omega(\tau),\tau)$ *tends to infinity for* τ *tending to infinity,* τ *can be found as the root of the equation* $S_x(\Omega(\tau),\tau) = X$ *by bisection method.*

Here, we can observe that the IoT controller, due to the restricted resources, generally applies reinforcement partly, namely to a subset of devices I^{11} which were not originally protected in a reliable manner, relying on initial level of security for the others devices. While the adversary, besides attacking initially less protected devices will, if he has enough resources, also exhibit a tendency to take a chance among a subset I^{10} of the originally reliable protected devices. A similar phenomena was also observed in the OFDM jamming problem, where in general SNR regime the jammer can generally jam fewer subcarriers than the user employs for transmission [1,10].

The theorem, beyond giving an algorithm to design equilibrium strategies, also implies a criteria needed to establish whether the IoT controller's resources are sufficient to reinforce all the devices.

Theorem 2. *In the game to minimize damage, the IoT controller can reinforce all of the devices if the following condition holds:*

$$\tau < X \min_{t\in D} \frac{R_t\alpha_t}{(\tau\alpha_t/\beta_t+1)^2} \Big/ \sum_{t\in D} \frac{R_s\alpha(s)/\beta_s}{(\tau\alpha_s/\beta_s+1)^2}, \tag{10}$$

where

$$\tau = X/(Y + \sum_{t\in D} 1/\beta_t). \tag{11}$$

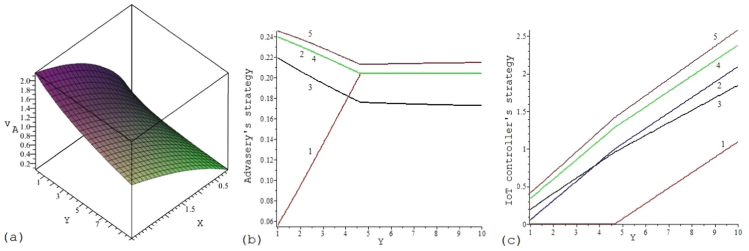

Fig. 1. (a) The payoff to an adversary aimed at maximizing the total damage, as functions of X and Y; (b) the strategy of the adversary and (c) the strategy of the IoT controller as functions of Y for $X = 1$.

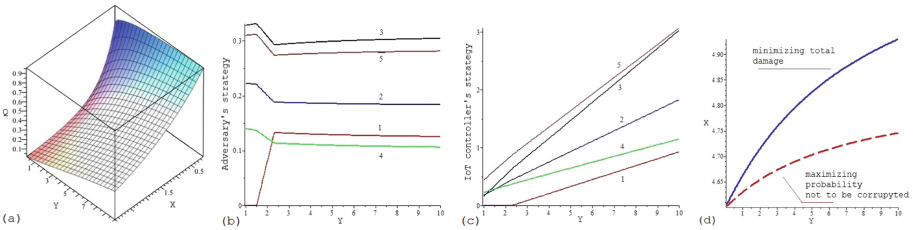

Fig. 2. (a) The payoff for the IoT controller that is aimed at maximizing the probability that the network is not compromised, as a function of X and Y; (b) the strategy of the adversary and (c) the strategy of the IoT controller as functions of Y for $X = 1$; and (d) the switching lines in the plane (X, Y) for the zones where the IoT controller's resources are enough to reinforce all of the devices.

Then, the equilibrium strategies are given by the first lines (6) and (7) with

$$\omega = \frac{\tau}{X} \sum_{t \in D} \frac{R_s \alpha_s / \beta_s}{(\tau \alpha_s / \beta_s + 1)^2}. \tag{12}$$

4 Maximizing Probability Not to Be Compromised

In this Section, we consider the game where the IoT controller wants to maximize the probability that none of the devices are compromised.

Theorem 3. *In the maximizing probability not to be compromised game, there is a unique equilibrium given by* $(\boldsymbol{x}_{\omega,\tau,t}, \boldsymbol{y}_{\omega,\tau,t})$ *where*

$$x_{\omega,\tau,t} = \begin{cases} \dfrac{\alpha_i \tau}{(\alpha_t \tau + \beta_t)\omega}, & t \in I^{11}_{\omega,\tau}, \\ \dfrac{1}{\omega} - \dfrac{1}{\alpha_t}, & t \in I^{10}_{\omega,\tau}, \\ 0, & t \in I^{00}_{\omega,\tau} \end{cases} \quad y_{\omega,\tau,t} = \begin{cases} \dfrac{\alpha_t}{(\alpha_t \tau + \beta_t)\omega} - \dfrac{1}{\beta_t}, & t \in I^{11}_{\omega,\tau}, \\ 0, & t \notin I^{11}_{\omega,\tau} \end{cases} \tag{13}$$

with $I^{00}_{\omega,\tau} := \{t : \alpha_t \leq \omega\}$, $I^{10}_{\omega,\tau} := \{t : \alpha_t\beta_t/(\alpha_t\tau + \beta_t) \leq \omega < \alpha_t\}$ *and* $I^{11}_{\omega,\nu} := \{t : \omega < \alpha_t\beta_t/(\alpha_t\tau + \beta_t)\}$.
Astonishingly, these strategies coincide with OFDM transmission strategies when facing jamming [10]. This coincidence with OFDM transmission strategies implies that the value of parameters can be uniquely defined by superposition of bisection methods from the condition that the strategy must employ all of the resources, as was done in Theorem 1. Here, as in Theorem 1, as parameters we use the Lagrange multiplier ω*, while as the other parameter* τ *we use ratio of Lagrange multipliers that arise to solve the corresponding best response equations. This allows, similar to Theorem 2, to show that if the following condition holds then the IoT controller's resources are enough to reinforce all of the devices:*

$$\tau < X \min_{t\in D}(\alpha_t\beta_t)/(\tau\alpha_t + \beta_t)/\sum_{t\in D} \alpha(s)/(\tau\alpha_s + \beta_s) \text{ where } \tau \text{ is given by (11).} \tag{14}$$

5 Discussions

As an example, let us consider a network consisting of $n = 5$ devices and $\alpha = (1, 2, 2.1, 2.8, 3.2)$, $\beta = (1.5, 2, 1.2, 5, 2)$, and $R = (1, 1, 1, 1, 1)$. Since $R \equiv 1$, the payoff v_A, i.e., the expected total damage, reflects the expected number of compromised devices. Figure 1(a) illustrates that the total damage is decreasing with respect to an increase in Y, and it is increasing with respect to an increase on X. Figure 2(a) illustrates that the probability for the network to not be compromised is increasing with an increase in Y and it is decreasing with an increase in X. Figures 1 and 2 illustrate that the adversary's strategy for compromising at least one device is more distributed among the devices than for the case where the objective is to maximize the total damage.

Note that, by (11), the left-side of condition (10) tends to zero for Y tending to infinity, while its right-side tends to $\min_{t\in D} R_t\alpha_t/\sum_{s\in D} R_s\alpha_s/\beta_s > 0$. Thus, for each fixed X there is a Y such that the resource is enough to reinforce all of the devices. By (14), a similar conclusion holds for maximizing the probability that the network is not compromised. Figure 2(d) illustrates, in the plane (X, Y), the switching line between the zone where the IoT controller has enough resources to reinforce all of the devices and the zone where the resources only allows one to maintain partial reinforcement. In particular, this confirms that, in the game to maximize the probability for the network to not be compromised, the IoT controller must employ a strategy to reinforce all of the devices under a smaller resource budget than in the game to minimize total damage.

Appendix

Proof of Theorem 1. (a) By (5), (x, y) is an equilibrium if and only if x and y are the best response strategies to each other, i.e., they are the solution of the best response equations: $x = \mathrm{BR}_A(y) = \arg\max_{x\in\Pi_A} v_A(x, y)$ and $y =$

$\mathrm{BR}_C(x) = \arg\min_{y \in \Pi_C} v_A(x,y)$. Since $v_A(\boldsymbol{x},\boldsymbol{y})$ is concave on $\boldsymbol{x}$ and convex on $\boldsymbol{y}$, a pair of strategies $(\boldsymbol{x},\boldsymbol{y})$ is the solution of the best response equations if and only if there are ω and ν (Lagrange multipliers) such that the following conditions hold:

$$\frac{R_t\alpha_t(1+\beta_t y_t)}{(1+\alpha_t x_t+\beta_t y_t)^2}\begin{cases}=\omega, & x_t>0,\\ \le\omega, & x_t=0,\end{cases} \quad \frac{R_t\alpha_t\beta_t x_t}{(1+\alpha_t x_t+\beta_t y_t)^2}\begin{cases}=\nu, & y_t>0,\\ \le\nu, & y_t=0.\end{cases} \tag{15}$$

By (15), $\nu>0$ and $\omega>0$. Also, by the second relation of (15), if $x_t=0$ then $y_t=0$, since otherwise $\nu=0$. Thus, we have to consider separately only three cases: (a-i) $x_t=0$, $y_t=0$, (a-ii) $x_t>0$, $y_t=0$ and (a-iii) $x_t>0$, $y_t>0$.

(a-i) Let $x_t=0$, $y_t=0$. Then, (15) is equivalent to $t \in I^{00}_{\omega,\nu} := \{t : R_t\alpha_t/\omega \le 1\}$.

(a-ii) Let $x_t>0$, $y_t=0$. Then, (15) is equivalent to

$$R_t\alpha_t/((1+\alpha_t x_t)^2)=\omega, \tag{16}$$

$$R_t\alpha_t\beta_t x_t/(1+\alpha_t x_t)^2 \le \nu. \tag{17}$$

Solving (16) implies that

$$x_t = \left(\sqrt{R_t\alpha_t/\omega}-1\right)/\alpha_t. \tag{18}$$

Then, since $x_t>0$, (18) implies that

$$\omega < R_t\alpha_t. \tag{19}$$

By (16), (17) is equivalent to

$$\beta_t x_t \le \nu/\omega. \tag{20}$$

Substituting x_t given by (18) into (20) implies $\sqrt{R_t\alpha_t/\omega} \le 1+(\alpha_t/\beta_t)(\nu/\omega)$. This, jointly with (19), gives that $t \in I^{10}_{\omega,\nu} := \{t : 1 < \sqrt{R_t\alpha_t/\omega} \le 1+(\alpha_t/\beta_t)(\nu/\omega)\}$.

(a-iii) Let $x_t>0$, $y_t>0$. Then, (15) is equivalent to

$$R_t\alpha_t(1+\beta_t y_t)/((1+\alpha_t x_t+\beta_t y_t)^2)=\omega, \tag{21}$$

$$R_t\alpha_t\beta_t x_t/((1+\alpha_t x_t+\beta_t y_t)^2)=\nu. \tag{22}$$

Dividing (21) by (22) implies

$$1+\beta_t y_t = (\omega/\nu)\beta_t x_t. \tag{23}$$

Substituting (23) into (22) yields $x_t = R_t\alpha_t\beta_t/\left(\nu\left(\alpha_t+\beta_t\omega/\nu\right)^2\right)$. Clearly, such x_t is positive. Substituting this x_t into (23) implies that $y_t = R_t\alpha_t\beta_t/(\omega\left(\alpha_t\nu/\omega+\beta_t\right)^2) - 1/\beta_t$. Then, the condition that such y_t is positive is equivalent that $t \in I^{11}_{\omega,\nu} := \left\{t : 1+(\alpha_t/\beta_t)(\nu/\omega) < \sqrt{R_t\alpha_t/\omega}\right\}$.

Finally, let us introduce an auxiliary notation $\tau := \nu/\omega$. In this notation x, y, I^{00}, I^{10} and I^{11} have the form given by (6), (7) and (8), and (a) follows.

(b-a) and b-(b) follow in a straightforward manner from (7) and (8) and the fact that $S_y(\omega, \tau) = 0$ if and only if the set $I^{11}_{\omega,\tau}$ is empty. (b-c) and (b-d) follow from (b-a) and (b-b).

(b-e) By (7) and (8), $S_y(\omega, \tau) = Y$ is equivalent to

$$\sum_{t\in D} \left\lfloor R_t\alpha_t\beta_t/((\omega/\tau^2)\,(\alpha_t + \beta_t/\tau)^2) - 1/\beta_t \right\rfloor_+ = Y. \tag{24}$$

Then, substituting $\omega = \Omega(\tau)$ into (24) and taking τ to infinity we obtain that (24) is asymptotically equivalent to $\sum_{t\in D} \lfloor \beta_t/((\Omega(\tau)/\tau^2)\alpha_t) - 1/\beta_t \rfloor_+ = Y$. This implies (b-e), and (b) follows.

(c) By (8), $I^{10}_{\omega,0}$ is empty. Thus, by (6) and (b-d), $S_x(\Omega(0), 0) = S_x(\Omega_0, 0) = 0$. By (7) and (6), $I^{11}_{\Omega(\tau),\tau}$ is not empty for any τ. By (6) and (b-e), for large τ

$$x_{\Omega(\tau),\tau,t} \sim R_t\alpha_t\beta_t\tau^3/(\Omega_\infty(\alpha_t\tau + \beta_t)^2) \sim R_t\beta_t\tau/(\alpha_t\Omega_\infty) \text{ with } t \in I^{11}_{\Omega(\tau),\tau}.$$

Thus, $\lim_{\tau\uparrow\infty} S_x(\Omega(\tau), \tau) = \infty$, and the result follows. ■

Proof of Theorem 2. Since $I^{11}_{\omega,\tau} = \{1, \ldots, n\}$, x and y are given by the first lines in (6) and (7). Summing up these $x_{\omega,\tau,t}$ divided by τ on t, summing up these $y_{\omega,\tau,t}$ on t, and taking into account that $\boldsymbol{x}_{\omega,\tau} \in \Pi_A$ and $\boldsymbol{y}_{\omega,\tau} \in \Pi_C$ imply (11). Then, by (11), summing up these $x_{\omega,\tau,t}$ implies (12). Finally, (12) and the fact that $I^{11}_{\omega,\tau} = \{1, \ldots, n\}$ yields (10). ■

Proof of Theorem 3. It is clear that the problem of maximizing (minimizing) $Q(\boldsymbol{x}, \boldsymbol{y})$ is equivalent to the problem of maximizing (minimizing) $\ln(Q(\boldsymbol{x}, \boldsymbol{y}))$. Using this simple observation implies that a pair of strategies $(\boldsymbol{x}, \boldsymbol{y})$ is the solution of the best response equations if and only if there are ω and ν (Lagrange multipliers) such that the following conditions hold:

$$\frac{\alpha_t}{1 + \alpha_t x_t + \beta_t y_t} \begin{cases} = \omega, & x_t > 0, \\ \leq \omega, & x_t = 0, \end{cases} \quad \frac{\alpha_t\beta_t x_t}{(1 + \beta_t y_t)(1 + \alpha_t x_t + \beta_t y_t)} \begin{cases} = \nu, & y_t > 0, \\ \leq \nu, & y_t = 0. \end{cases}$$

Astonishingly, these conditions coincide with the conditions for designing a transmission strategy under hostile jamming in OFDM communication [10]. Then, introducing a new variable $\tau = \nu/\omega$, in variables τ and ω the result follows. ■

References

1. Ara, M., Reboredo, H., Ghanem, S.A.M., Rodrigues, M.R.D.: A zero-sum power allocation game in the parallel Gaussian wiretap channel with an unfriendly jammer. In: IEEE International Conference on Communication Systems (ICCS) (2012)
2. Baston, V.J., Garnaev, A.Y.: A search game with a protector. Naval Res. Logistics **47**, 85–96 (2000)

3. Fragkiadakis, A.G., Tragos, E.Z., Askoxylakis, I.G.: Survey on security threats and detection techniques in cognitive radio networks. IEEE Commun. Surv. Tutorials **15**, 428–445 (2013)
4. Garnaev, A., Baykal-Gursoy, M., Poor, H.V.: Security games with unknown adversarial strategies. IEEE Trans. Cybern. **46**, 2291–2299 (2016)
5. Garnaev, A., Trappe, W.: Stationary equilibrium strategies for bandwidth scanning. In: Jonsson, M., Vinel, A., Bellalta, B., Marina, N., Dimitrova, D., Fiems, D. (eds.) MACOM 2013. LNCS, vol. 8310, pp. 168–183. Springer, Cham (2013). https://doi.org/10.1007/978-3-319-03871-1_15
6. Garnaev, A., Trappe, W.: One-time spectrum coexistence in dynamic spectrum access when the secondary user may be malicious. IEEE Trans. Inf. Forensics Secur. **10**, 1064–1075 (2015)
7. Garnaev, A., Trappe, W.: A bandwidth monitoring strategy under uncertainty of the adversary's activity. IEEE Trans. Inf. Forensics Secur. **11**, 837–849 (2016)
8. Garnaev, A., Trappe, W.: Bandwidth scanning when facing interference attacks aimed at reducing spectrum opportunities. IEEE Trans. Inf. Forensics Secur. **12**, 1916–1930 (2017)
9. Garnaev, A., Trappe, W., Kung, C.-T.: Optimizing scanning strategies: selecting scanning bandwidth in adversarial RF environments. In: 8th International Conference on Cognitive Radio Oriented Wireless Networks (CROWNCOM), pp. 148–153 (2013)
10. Garnaev, A., Trappe, W., Petropulu, A.: Equilibrium strategies for an OFDM network that might be under a jamming attack. In: 51st Annual Conference on Information Systems and Sciences (CISS), pp. 1–6 (2017)
11. Gerstein, D.M.: The WannaCry virus, a lesson in global unpreparedness. The National Interest, 17 May 2017. http://nationalinterest.org/feature/the-wannacry-virus-lesson-global-unpreparedness-20719
12. Guan, P., Zhuang, J.: Modeling resources allocation in attacker-defender games with "warm up" CSF. Risk Anal. **36**, 776–791 (2016)
13. Han, Z., Niyato, D., Saad, W., Basar, T., Hjrungnes, A.: Game Theory in Wireless and Communication Networks: Theory, Models, and Applications. Cambridge University Press, New York (2012)
14. Hausken, K., Levitin, G.: Review of systems defense and attack models. Int. J. Performability Eng. **8**, 355–366 (2012)
15. La, Q.D., Quek, T.Q.S., Lee, J., Jin, S., Zhu, H.: Deceptive attack and defense game in honeypot-enabled networks for the Internet of Things. IEEE Internet Things J. **3**, 1025–1035 (2016)
16. Margelis, G., Piechocki, R., Tryfonas, T., Thomas, P.: Smart attacks on the integrity of the Internet of Things: avoiding detection by employing game theory. In: IEEE Global Communications Conference (GLOBECOM) (2016)
17. Namvar, N., Saad, W., Bahadori, N., Kelleys, B.: Jamming in the Internet of Things: a game-theoretic perspective. In: IEEE Global Communications Conference (GLOBECOM) (2016)
18. Rontidis, G., Panaousis, E., Laszka, A., Dagiuklas, T., Malacaria, P., Alpcan, T.: A game-theoretic approach for minimizing security risks in the Internet-of-Things. In: IEEE International Conference on Communication Workshop (ICCW), pp. 2639–2644 (2015)
19. Sedjelmaci, H., Senouci, S.-M., Bahri, M.A.: A lightweight anomaly detection technique for low-resource IOT devices: a game-theoretic methodology. In: IEEE International Conference on Communication (ICC), pp. 1–6 (2016)

20. Skaperdas, S.: Contest success functions. Econ. Theory **7**, 283–290 (1996)
21. Song, T., Stark, W.E., Li, T., Tugnait, J.K.: Optimal multiband transmission under hostile jamming. IEEE Trans. Commun. **64**, 4013–4027 (2016)
22. Storm, D.: Hackers demonstrated first ransomware for IoT thermostats at DEF CON. ComputerWorld, 8 August 2016. http://www.computerworld.com/article/3105001/security/hackers-demonstrated-first-ransomware-for-iot-thermostats-at-def-con.html
23. Xu, X., Yu, H.: A game theory approach to fair and efficient resource allocation in cloud computing. Math. Prob. Eng. **2014**, 1–14 (2014)
24. Zhou, L., Chao, H.-C.: Multimedia traffic security architecture for the Internet of Things. IEEE Netw. **25**, 35–40 (2011)