Proactive Defense Against Physical Denial of Service Attacks Using Poisson Signaling Games

Jeffrey Pawlick(✉) and Quanyan Zhu

Department of Electrical and Computer Engineering, New York University Tandon School of Engineering, 6 MetroTech Center, Brooklyn, NY 11201, USA
{jpawlick,quanyan.zhu}@nyu.edu

Abstract. While the Internet of things (IoT) promises to improve areas such as energy efficiency, health care, and transportation, it is highly vulnerable to cyberattacks. In particular, distributed denial-of-service (DDoS) attacks overload the bandwidth of a server. But many IoT devices form part of cyber-physical systems (CPS). Therefore, they can be used to launch "physical" denial-of-service attacks (PDoS) in which IoT devices overflow the "physical bandwidth" of a CPS. In this paper, we quantify the population-based risk to a group of IoT devices targeted by malware for a PDoS attack. In order to model the recruitment of bots, we develop a "Poisson signaling game," a signaling game with an unknown number of receivers, which have varying abilities to detect deception. Then we use a version of this game to analyze two mechanisms (legal and economic) to deter botnet recruitment. Equilibrium results indicate that (1) defenders can bound botnet activity, and (2) legislating a minimum level of security has only a limited effect, while incentivizing active defense can decrease botnet activity arbitrarily. This work provides a quantitative foundation for proactive PDoS defense.

1 Introduction to the IoT and PDoS Attacks

The Internet of things (IoT) is a "dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'things' have identities, physical attributes, and virtual personalities" [2]. The IoT is (1) decentralized, (2) heterogeneous, and (3) connected to the physical world. It is *decentralized* because nodes have "self-configuring capabilities," some amount of local intelligence, and incentives which are not aligned with the other nodes. The IoT is *heterogeneous* because diverse "things" constantly enter and leave the IoT, facilitated by "standard and interoperable communication protocols." Finally, IoT devices are *connected*

Q. Zhu—This work is partially supported by an NSF IGERT grant through the Center for Interdisciplinary Studies in Security and Privacy (CRISSP) at New York University, by the grant CNS-1544782, EFRI-1441140, and SES-1541164 from National Science Foundation (NSF) and DE-NE0008571 from the Department of Energy.

S. Rass et al. (Eds.): GameSec 2017, LNCS 10575, pp. 336–356, 2017.
DOI: 10.1007/978-3-319-68711-7_18

Fig. 1. Conceptual diagram of a PDoS attack. (1) Attack sponsor hires botnet herder. (2) Botnet herder uses server to manage recruitment. (3) Malware scans for vulnerable IoT devices and begins cascading infection. (4) Botnet herder uses devices (*e.g.,* HVAC controllers) to deplete bandwidth of a cyber-physical service (*e.g.,* electrical power).

to the physical world, *i.e.*, they are part of cyber-physical systems (CPS). For instance, they may influence behavior, control the flow of traffic, and optimize home lighting.

1.1 Difficulties in Securing the Internet of Things

While the IoT promises gains in efficiency, customization, and communication ability, it also raises new challenges. One of these challenges is security. The social aspect of IoT devices makes them vulnerable to attack through social engineering. Moreover, the dynamic and heterogeneous attributes of the IoT create a large attack surface. Once compromised, these "things" serve as vectors for attack. The most notable example has been the Mirai botnet attack on Dyn in 2016. Approximately 100,000 bots—largely belonging to the (IoT)—attacked the domain name server (DNS) for Twitter, Reddit, Github, and the New York Times [15]. A massive flow of traffic overwhelmed the bandwidth of the DNS.

1.2 Denial of Cyber-Physical Service Attacks

Since IoT devices are part of CPS, they also require physical "bandwidth." As an example, consider the navigation app Waze [1]. Waze uses real-time traffic information to find optimal navigation routes. Due to its large number of users, the app also influences traffic. If too many users are directed to one road, they can consume the physical bandwidth of that road and cause unexpected congestion. An attacker with insider access to Waze could use this mechanism to manipulate transportation networks.

Another example can be found in healthcare. Smart lighting systems (which deploy, *e.g.*, *time-of-flight* sensors) detect falls of room occupants [22]. These systems alert emergency responders about a medical situation in an assisted living center or the home of someone who is aging. But an attacker could potentially trigger many of these alerts at the same time, depleting the response bandwidth of emergency personnel.

Such a threat could be called a denial of *cyber-physical* service attack. To distinguish it from a cyber-layer DDoS, we also use the acronym *PDoS* (*Physical* Denial of Service). Figure 1 gives a conceptual diagram of a PDoS attack. In the rest of the paper, we will consider one specific instance of a PDoS attack, although our analysis is not limited to this example. We consider the infection and manipulation of a population of IoT-based heating, ventilation, and air conditioning (HVAC) controllers in order to cause a sudden load shock to the power grid. Attackers either disable demand response switches used for reducing peak load [6], or they unexpectedly activate inactive loads. This imposes risks ranging from frequency droop to load shedding and cascading failures.

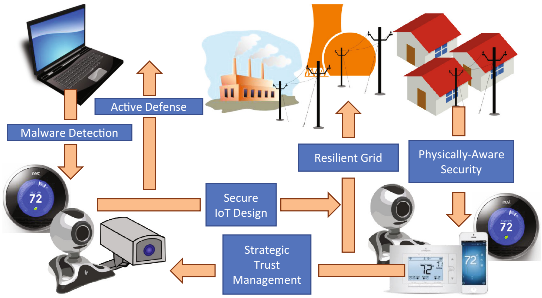

Fig. 2. PDoS defense can be designed at multiple layers. Malware detection and active defense can combat initial infection, secure IoT design and strategic trust can reduce the spread of the malware, and CPS can be resilient and physically-aware. We focus on detection and active defense.

1.3 Modeling the PDoS Recruitment Stage

Defenses against PDoS can be designed at multiple layers (Fig. 2). The scope of this paper is limited to defense at the stage of botnet recruitment, in which the attacker scans a wide range of IP addresses, searching for devices with weak security settings. Mirai, for example, does this by attempting logins with a dictionary of factory-default usernames and passwords (*e.g.* `root/admin`, `admin/admin`, `root/123456`) [12]. Devices in our mechanism identify these suspicious login attempts and use active defense to learn about the attacker or report his activity.

In order to quantify the risk of malware infection, we combine two game-theoretic models known as signaling games [7,14] and Poisson games [18]. Signaling games model interactions between two parties, one of which possesses information unknown to the other party. While signaling games consider only two players, we extend this model by allowing the number of target IoT devices to be a random variable (r.v.) that follows a Poisson distribution. This captures the fact that the malware scans a large number of targets. Moreover, we allow the targets to have heterogeneous abilities to detect malicious login attempts.

1.4 Contributions and Related Work

We make the following principle contributions:

1. We describe an IoT attack called a *denial of cyber-physical service* (*PDoS*).
2. We develop a general model called *Poisson signaling games* (*PSG*) which quantifies one-to-many signaling interactions.
3. We find the pure strategy equilibria of a version of the PSG model for PDoS.
4. We analyze legal and economic mechanisms to deter botnet recruitment, and find that (1) defenders can bound botnet activity, and (2) legislating a minimum level of security has only a limited effect, while incentivizing active defense, in principle, can decrease botnet activity arbitrarily.

Signaling games are often used to model deception and trust in cybersecurity [16,19,21]. Poisson games have also been used to model malware epidemics in large populations [11]. Wu *et al.* use game theory to design defense mechanisms against DDoS attacks [24]. But the defense mechanisms mitigate the actual the flood of traffic against a target system, while we focus on botnet recruitment. Bensoussan *et al.* use a susceptible-infected-susceptible (SIS) model to study the growth of a botnet [5]. But IoT devices in our model maintain beliefs about the reliability of incoming messages. In this way, our paper considers the need to trust legitimate messages. Finally, *load altering attacks* [4,17] to the power grid are an example of PDoS attacks. But PDoS attacks can also deal with other resources.

In Sect. 2, we review signaling games and Poisson games. In Sect. 3, we combine them to create Poisson signaling games (PSG). In Sect. 4, we apply PSG to quantify the population risk due to PDoS attacks. Section 5 obtains the perfect Bayesian Nash equilibria of the model. Some of these equilibria are harmful for power companies and IoT users. Therefore, we design proactive mechanisms to improve the equilibria in Sect. 6. We underline the key contributions in Sect. 7.

2 Signaling Games and Poisson Games

This section reviews two game-theoretic models: signaling games and Poisson games. In Sect. 3, we combine them to create PSG. PSG can be used to model many one-to-many signaling interactions in addition to PDoS.

2.1 Signaling Games with Evidence

Signaling games are a class of dynamic, two-player, information-asymmetric games between a sender S and a receiver R (*c.f.* [7,14]). Signaling games *with evidence* extend the typical definition by giving receivers some exogenous ability to detect deception[1] [20]. They are characterized by the tuple

$$\Phi_{\mathbf{SG}} = \left(X, M, E, A, q^S, \delta, u^S, u^R\right).$$

[1] This is based on the idea that deceptive senders have a harder time communicating some messages than truthful senders. In interpersonal deception, for instance, lying requires high cognitive load, which may manifest itself in external gestures [23].

First, S posses some private information unknown to R. This private information is called a *type*. The type could represent, *e.g.*, a preference, a technological capability, or a malicious intent. Let the finite set X denote the set of possible types, and let $x \in X$ denote one particular type. Each type occurs with a probability $q^S(x)$, where $q^S : X \to [0,1]$ such that (s.t.) $\sum_{x \in X} q^S(x) = 1$ and $\forall x \in X$, $q^S(x) \geq 0$.

Based on his private information, S communicates a *message* to the receiver. The message could be, *e.g.*, a pull request, the presentation of a certificate, or the execution of an action which partly reveals the type. Let the finite set M denote the set of possible messages, and let $m \in M$ denote one particular type. In general, S can use a strategy in which he chooses various m with different probabilities. We will introduce notation for these *mixed strategies* later.

In typical signaling games (*e.g.* Lewis signaling games [7,14] and signaling games discussed by Crawford and Sobel [7]), R only knows about x through m. But this suggests that deception is undetectable. Instead, signaling games with evidence include a *detector*[2] which emits evidence $e \in E$ about the sender's type [20]. Let $\delta : E \to [0,1]$ s.t. for all $x \in X$ and $m \in M$, we have $\sum_{e \in E} \delta(e \,|\, x, m) = 1$ and $\delta(e \,|\, x, m) \geq 0$. Then $\delta(e \,|\, x, m)$ gives the probability with which the detector emits evidence e given type x and message m. This probability is fixed, not a decision variable. Finally A be a finite set of *actions*. Based on m and e, R chooses some $a \in A$. For instance, R may choose to accept or reject a request represented by the message. These can also be chosen using a mixed-strategy.

In general, x, m, and a can impact the utility of S and R. Therefore, let $u^S : M \times A \to \mathbb{R}^{|X|}$ be a vector-valued function such that $u^S(m,a) = \left[u^S_x(m,a)\right]_{x \in X}$. This is a column vector with entries $u^S_x(m,a)$. These entries give the utility that S of each receiver of type $x \in X$ obtains for sending a message m when the receiver plays action a. Next, define the utility function for R by $u^R : X \times M \times A \to \mathbb{R}$, such that $u^R(x,m,a)$ gives the utility that R receives when a sender of type x transmits message m and R plays action a.

2.2 Poisson Games

Poisson games were introduced by Roger Myerson in 1998 [18]. This class of games models interactions between an unknown number of players, each of which belongs to one type in a finite set of types. Modeling the population uncertainty using a Poisson r.v. is convenient because merging or splitting Poisson r.v. results in r.v. which also follow Poisson distributions.

Section 3 will combine signaling games with Poisson games by considering a sender which issues a command to a pool of an unknown number of receivers, which all respond at once. Therefore, let us call the players of the Poisson game

[2] This could literally be a hardware or software detector, such as email filters which attempt to tag phishing emails. But it could also be an abstract notion meant to signify the innate ability of a person to recognize deception.

"receivers," although this is not the nomenclature used in the original game. Poisson games are characterized by the tuple

$$\Phi^{\mathbf{PG}} = \left(\lambda, Y, q^R, A, \tilde{u}^R\right).$$

First, the population parameter $\lambda > 0$ gives the mean and variance of the Poisson distribution. For example, λ may represent the expected number of mobile phone users within range of a base station. Let the finite set Y denote the possible types of each receiver, and let $y \in Y$ denote one of these types. Each receiver has type y with probability $q^R(y)$, where $\sum_{y \in Y} q^R(y) = 1$ and $\forall y \in Y$, $q^R(y) > 0$.

Because of the decomposition property of the Poisson r.v., the number of receivers of each type $y \in Y$ also follows a Poisson distribution. Based on her type, each receiver chooses an action a in the finite set A. We have deliberately used the same notation as the action for the signaling game, because these two actions will coincide in the combined model.

Utility functions in Poisson games are defined as follows. For $a \in A$, let $c_a \in \mathbb{Z}_+$ (the set of non-negative integers) denote the count of receivers which play action a. Then let c be a column vector which contains entries c_a for each $a \in A$. Then c falls within the set $\mathbb{Z}(A)$, the set of all possible integer counts of the number of players which take each action.

Poisson games assume that all receivers of the same type receive the same utility. Therefore, let $\tilde{u}^R : A \times \mathbb{Z}(C) \to \mathbb{R}^{|Y|}$ be a vector-valued function such that $\tilde{u}^R(a, c) = \left[\tilde{u}^R_y(a, c)\right]_{y \in Y}$. The entries $\tilde{u}^R_y(a, c)$ give the utility that receivers of each type $y \in Y$ obtain for playing an action a while the vector of the total count of receivers that play each action is given by c. Note that this is different from the utility function of receivers in the signaling game. Given the strategies of the receivers, c is also distributed according to a Poisson r.v.

3 Poisson Signaling Games

Figure 3 depicts Poisson signaling games (PSG). PSG are characterized by combining $\Phi_{\mathbf{SG}}$ and $\Phi^{\mathbf{PG}}$ to obtain the tuple

$$\Phi^{\mathbf{PG}}_{\mathbf{SG}} = \left(X, Y, M, E, A, \lambda, q, \delta, U^S, U^R\right).$$

3.1 Types, Actions, and Evidence, and Utility

As with signaling games and Poisson games, X denotes the set of types of S, and Y denotes the set of types of R. M, E, and A denote the set of messages, evidence, and actions, respectively. The Poisson parameter is λ.

The remaining elements of $\Phi^{\mathbf{PG}}_{\mathbf{SG}}$ are slightly modified from the signaling game or Poisson game. First, $q : X \times Y \to [0, 1]^2$ is a vector-valued function such that $q(x, y)$ gives the probabilities $q^S(x)$, $x \in X$, and $q^R(y)$, $y \in Y$, of each type of sender and receiver, respectively.

As in the signaling game, δ characterizes the quality of the deception detector. But receivers differ in their ability to detect deception. Various email clients, for example, may have different abilities to identify phishing attempts. Therefore, in PSG, we define the mapping by $\delta : E \to [0,1]^{|Y|}$, s.t. the vector $\delta\left(e \,|\, x, m\right) = \left[\delta_y\left(e \,|\, x, m\right)\right]_{y \in Y}$ gives the probabilities $\delta_y(e \,|\, x, m)$ with which each receiver type y observes evidence e given sender type x and message m. This allows each receiver type to observe evidence with different likelihoods[3].

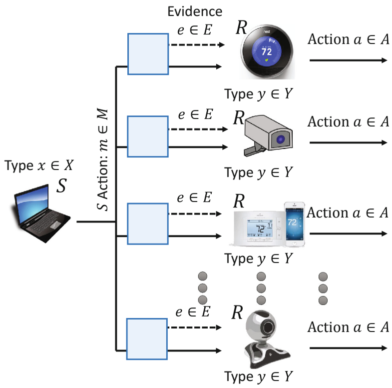

Fig. 3. PSG model the third stage of a PDoS attack. A sender of type x chooses an action m which is observed by an unknown number of receivers. The receivers have multiple types $y \in Y$. Each type may observe different evidence $e \in E$. Based on m and e, each type of receiver chooses an action a.

The utility functions U^S and U^R are also adjusted for PSG. Let $U^S : M \times \mathbb{Z}(A) \to \mathbb{R}^{|X|}$ be a vector-valued function s.t. the vector $U^S\left(m, c\right) = \left[U^S_x\left(m, c\right)\right]_{x \in X}$ gives the utility of senders of each type x for sending message m if the count of receivers which choose each action is given by c. Similarly, let $U^R : X \times M \times A \times \mathbb{Z}(A) \to \mathbb{R}^{|Y|}$ be a vector-valued function s.t. $U^R\left(x, m, a, c\right) = \left[U^R_y\left(x, m, a, c\right)\right]_{y \in Y}$ gives the utility of receivers of each type $y \in Y$. As earlier, x is the type of the sender, and m is the message. But note that a denotes the action of *this particular receiver*, while c denotes the count of overall receivers which choose each action.

3.2 Mixed-Strategies and Expected Utility

Next, we define the nomenclature for mixed-strategies and expected utility functions. For senders of each type $x \in X$, let $\sigma^S_x : M \to [0,1]$ be a mixed strategy

[3] In fact, although all receivers with the same type y have the same likelihood $\delta_y(e \,|\, x, m)$ of observing evidence e given sender type x and message m, our formulation allows the receivers to observe different actual realizations e of the evidence.

such that $\sigma_x^S(m)$ gives the probability with which he plays each message $m \in M$. For each $x \in X$, let Σ_x^S denote the set of possible σ_x^S. We have

$$\Sigma_x^R = \left\{ \bar{\sigma} \mid \sum_{m \in M} \bar{\sigma}(m) = 1 \text{ and } \forall m \in M,\, \bar{\sigma}(m) \geq 0 \right\}.$$

For receivers of each type $y \in Y$, let $\sigma_y^R : A \to [0,1]$ denote a mixed strategy such that $\sigma_y^R(a \mid m, e)$ gives the probability with which she plays action a after observing message m and action e. For each $y \in Y$, the function σ_y^R belongs to the set

$$\Sigma_y^R = \left\{ \bar{\sigma} \mid \sum_{a \in A} \bar{\sigma}(a) = 1 \text{ and } \forall a \in A,\, \bar{\sigma}(a) \geq 0 \right\}.$$

In order to choose her actions, R forms a belief about the sender type x. Let $\mu_y^R(x \mid m, e)$ denote the likelihood with which each R of type y who observes message m and evidence e believes that S has type x. In equilibrium, we will require this belief to be consistent with the strategy of S.

Now we define the expected utilities that S and each R receive for playing mixed strategies. Denote the expected utility of a sender of type $x \in X$ by $\bar{U}_x^S : \Sigma_x^S \times \Sigma^R \to \mathbb{R}$. Notice that all receiver strategies must be taken into account. This expected utility is given by

$$\bar{U}_x^S(\sigma_x^S, \sigma^R) = \sum_{m \in M} \sum_{c \in \mathbb{Z}(A)} \sigma_x^S(m)\, \mathbb{P}\left\{c \mid \sigma^R, x, m\right\} U_x^S(m, c).$$

Here, $\mathbb{P}\{c \mid \sigma^R, x, m\}$ is the probability with which the vector c gives the count of receivers that play each action. Myerson shows that, due to the aggregation and decomposition properties of the Poisson r.v., the entries of c are also Poisson r.v. [18]. Therefore, $\mathbb{P}\{c \mid \sigma^R, x, m\}$ is given by

$$\mathbb{P}\left\{c \mid \sigma^R, x, m\right\} = \prod_{a \in A} e^{\lambda_a} \frac{\lambda_a^{c_a}}{c_a!},\ \lambda_a = \lambda \sum_{y \in Y} \sum_{e \in E} q^R(y)\, \delta_y(e \mid x, m)\, \sigma_y^R(a \mid m, e). \tag{1}$$

Next, denote the expected utility of each receiver of type $y \in Y$ by $\bar{U}_y^R : \Sigma_y^R \times \Sigma^R \to \mathbb{R}$. Here, $\bar{U}_y^R(\theta, \sigma^R \mid m, e, \mu_y^R)$ gives the expected utility when this particular receiver plays mixed strategy $\theta \in \Sigma_y^R$ and the population of all types of receivers plays the mixed-strategy vector σ^R. The expected utility is given by

$$\bar{U}_y^R(\theta, \sigma^R \mid m, e, \mu_y^R) = \sum_{x \in X} \sum_{a \in A} \sum_{c \in \mathbb{Z}(A)} \mu_y^R(x \mid m, e)\, \theta(a \mid m, e)\, \mathbb{P}\left\{c \mid \sigma^R, x, m\right\} U_y^R(x, m, a, c), \tag{2}$$

where again $\mathbb{P}\{c \mid \sigma^R, x, m\}$ is given by Eq. (1).

3.3 Perfect Bayesian Nash Equilibrium

First, since PSG are dynamic, we use an equilibrium concept which involves *perfection*. Strategies at each information set of the game must be optimal for the remaining subgame [8]. Second, since PSG involve incomplete information, we use a *Bayesian* concept. Third, since each receiver chooses her action without knowing the actions of the other receivers, the Poisson stage of the game involves a *fixed point*. All receivers choose strategies which best respond to the optimal strategies of the other receivers. Perfect Bayesian Nash equilibrium (PBNE) is the appropriate concept for games with these criteria [8].

Consider the two chronological stages of PSG. The second stage takes place among the receivers. This stage is played with a given m, e, and μ^R determined by the sender (and detector) in the first stage of the game. When m, e, and μ^R are fixed, the interaction between all receivers becomes a standard Poisson game. Define $BR_y^R : \Sigma^R \to \mathcal{P}(\Sigma_y^R)$ (where $\mathcal{P}(\mathbb{S})$ denotes the power set of $\mathbb{S}$) such that the best response of a receiver of type y to a strategy profile σ^R of the other receivers is given by the strategy or set of strategies

$$BR_y^R \left(\sigma^R \,|\, m, e, \mu_y^R \right) \triangleq \underset{\theta \in \Sigma_y^R}{\arg\max}\, \bar{U}_y^R \left(\theta, \sigma^R \,|\, m, e, \mu_y^R \right). \tag{3}$$

The first stage takes place between the sender and the set of receivers. If we fix the set of receiver strategies σ^R, then the problem of a sender of type $x \in X$ is to choose σ_x^S to maximize his expected utility given σ^R. The last criteria is that the receiver beliefs μ^R must be consistent with the sender strategies according to Bayes' Law. Definition 1 applies PBNE to PSG.

Definition 1. *(PBNE) Strategy and belief profile* $(\sigma^{S*}, \sigma^{R*}, \mu^R)$ *is a PBNE of a PSG if all of the following hold [8]:*

$$\forall x \in X,\ \sigma_x^{S*} \in \underset{\sigma_x^S \in \Sigma_x^S}{\arg\max}\, \bar{U}_x^S(\sigma_x^S, \sigma^{R*}), \tag{4}$$

$$\forall y \in Y, \forall m \in M, \forall e \in E,\ \sigma_y^{R*} \in BR_y^R \left(\sigma^{R*} \,|\, m, e, \mu_y^R \right), \tag{5}$$

$$\forall y \in Y, \forall m \in M, \forall e \in E,\ \mu_y^R \left(d \,|\, m, e \right) \in \frac{\delta_y \left(e \,|\, d, m \right) \sigma_d^S \left(m \right) q^S \left(d \right)}{\sum\limits_{\tilde{x} \in X} \delta_y \left(e \,|\, \tilde{x}, m \right) \sigma_{\tilde{x}}^S \left(m \right) q^S \left(\tilde{x} \right)}, \tag{6}$$

if $\sum\limits_{\tilde{x} \in X} \delta_y \left(e \,|\, \tilde{x}, m \right) \sigma_{\tilde{x}}^S \left(m \right) q^S \left(\tilde{x} \right) > 0$, *and* $\mu_y^R \left(d \,|\, m, e \right) \in [0, 1]$, *otherwise. We also always have* $\mu_y^R \left(l \,|\, m, e \right) = 1 - \mu_y^R \left(d \,|\, m, e \right)$.

Equation (4) requires the sender to choose an optimal strategy given the strategies of the receivers. Based on the message and evidence that each receiver observes, Eq. (5) requires each receiver to respond optimally to the profile of the strategies of the other receivers. Equation (6) uses Bayes' law (when possible) to obtain the posterior beliefs μ^R using the prior probabilities q^S, the sender strategies σ^S, and the characteristics δ_y, $y \in Y$ of the detectors [20].

4 Application of PSG to PDoS

Section 3 defined PSG in general, without specifying the members of the type, message, evidence, or action sets. In this section, we apply PSG to the recruitment stage of PDoS attacks. Table 1 summarizes the nomenclature.

S refers to the agent which attempts a login attempt, while R refers to the device. Let the set of sender types be given by $X = \{l, d\}$, where l represents a legitimate login attempt, while d represents a malicious attempt. Malicious S attempt to login to many devices through a wide IP scan. This number is drawn from a Poisson r.v. with parameter λ. Legitimate S only attempt to login to one device at a time. Let the receiver types be $Y = \{k, o, v\}$. Type k represents weak receivers which have no ability to detect deception and do not use active defense. Type o represents strong receivers which can detect deception, but do not use active defense. Finally, type v represents active receivers which can both detect deception and use active defense.

Table 1. Application of PSG to PDoS recruitment

Set	Elements
Type $x \in X$ of S	l : legitimate, d : malicious
Type $y \in Y$ of R	k : no detection; o : detection; v : detection & active defense
Message $m \in M$ of S	$m = \{m^1, m^2, \ldots\}$, a set of $\lvert m \rvert$ password strings
Evidence $e \in E$	b : suspicious, n : not suspicious
Action $a \in A$ of R	t : trust, g : lockout, f : active defense

4.1 Messages, Evidence Thresholds, and Actions

Messages consist of sets of consecutive unsuccessful login attempts. They are denoted by $m = \{m^1, m^2, \ldots\}$, where each $m^1, m^2, \ldots$ is a string entered as an attempted password[4]. For instance, botnets similar to Mirai choose a list of default passwords such as [12]

$$m = \{\texttt{admin}, \texttt{888888}, \texttt{123456}, \texttt{default}, \texttt{support}\}.$$

Of course, devices can lockout after a certain number of unsuccessful login attempts. Microsoft Server 2012 recommends choosing a threshold at 5 to 9 [3]. Denote the lower end of this range by $\tau_L = 5$. Let us allow all attempts with $\lvert m \rvert < \tau_L$. In other words, if a user successfully logs in before τ_L, then the PSG does not take place. (See Fig. 5).

The PSG takes place for $\lvert m \rvert \geq \tau_L$. Let $\tau_H = 9$ denote the upper end of the Microsoft range. After τ_L, S may persist with up to τ_H login attempts, or he may not persist. Let p denote persist, and w denote not persist. Our goal is to force malicious S to play w with high probability.

[4] A second string can also be considered for the username.

For R of types o and v, if S persists and does not successfully log in with $|m| \leq \tau_H$ login attempts, then $e = b$. This signifies a suspicious login attempt. If S persists and does successfully login with $|m| \leq \tau_H$ attempts, then $e = n$, *i.e.*, the attempt is not suspicious[5].

If a user persists, then the device R must choose an action a. Let $a = t$ denote trusting the user, *i.e.*, allowing login attempts to continue. Let $a = g$ denote locking the device to future login attempts. Finally, let $a = f$ denote using an active defense such as reporting the suspicious login attempt to an Internet service provider (ISP), recording the attempts in order to gather information about the possible attacker, or attempting to block the offending IP address.

4.2 Characteristics of PDoS Utility Functions

The nature of PDoS attacks implies several features of the utility functions U^S and U^R. These are listed in Table 2. Characteristic 1 (C1) states that if S does not persist, both players receive zero utility. C2 says that R also receives zero utility if S persists and R locks down future logins. Next, C3 states that receivers of all types receive positive utility for trusting a benign login attempt, but negative utility for trusting a malicious login attempt. We have assumed that only type v receivers use active defense; this is captured by C4. Finally, C5 says that type v receivers obtain positive utility for using active defense against a malicious login attempt, but negative utility for using active defense against a legitimate login attempt. Clearly, C1-C5 are all natural characteristics of PDoS recruitment.

Table 2. Characteristics of PDoS utility functions

#	Notation
C1	$\forall x \in X,\ y \in Y,\ a \in A,\ c \in \mathbb{Z}(A)$, $U_x^S(w, c) = U_y^R(x, w, a, c) = 0.$
C2	$\forall x \in X,\ y \in Y,\ c \in \mathbb{Z}(A)$, $U_y^R(x, p, g, c) = 0.$
C3	$\forall y \in Y,\ c \in \mathbb{Z}(A)$, $U_y^R(d, p, t, c) < 0 < U_y^R(l, p, t, c).$
C4	$\forall x \in X,\ c \in \mathbb{Z}(A)$, $U_k^R(x, p, f, c) = U_o^R(x, p, f, c) = -\infty.$
C5	$\forall c \in \mathbb{Z}(A)$, $U_v^R(l, p, f, c) < 0 < U_v^R(d, p, f, c).$

[5] For strong and active receivers, $\delta_y(b \,|\, d, p) > \delta_y(b \,|\, l, p)$, $y \in \{o, v\}$. That is, these receivers are more likely to observe suspicious evidence if they are interacting with a malicious sender than if they are interacting with a legitimate sender. Mathematically, $\delta_k(b \,|\, d, p) = \delta_k(b \,|\, l, p)$ signifies that type k receivers do not implement a detector.

4.3 Modeling the Physical Impact of PDoS Attacks

The quantities c_t, c_g, and c_f denote, respectively, the number of devices that trust, lock down, and use active defense. Define the function $Z : \mathbb{Z}(A) \rightarrow \mathbb{R}$ such that $Z(c)$ denotes the load shock that malicious S cause based on the count c. $Z(c)$ is clearly non-decreasing in c_t, because each device that trusts the malicious sender becomes infected and can impose some load shock to the power grid.

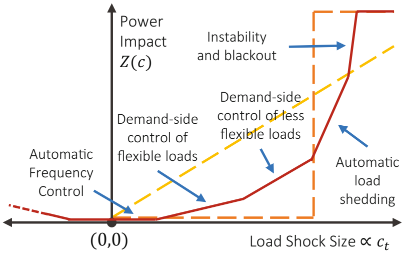

Fig. 4. Conceptual relationship between load shock size and damage to the power grid. Small shocks are mitigated through automatic frequency control or demand-side control of flexible loads. Large shocks can force load shedding or blackouts. (Color figure online)

The red (solid) curve in Fig. 4 conceptually represents the mapping from load shock size to damage caused to the power grid based on the mechanisms available for regulation. Small disturbances are regulated using automatic frequency control. Larger disturbances can significantly decrease frequency and should be mitigated. Grid operators have recently offered customers *load control switches*, which automatically deactivate appliances in response to a threshold frequency decrease [10]. But the size of this voluntary demand-side control is limited. Eventually, operators impose involuntary load shedding (*i.e.*, rolling blackouts). This causes higher inconvenience. In the worst case, transient instability leads to cascading failures and blackout [9].

The yellow and orange dashed curves in Fig. 4 provide two approximations to $Z(c)$. The yellow curve, $\tilde{Z}_{\text{lin}}(c)$, is linear in c^t. We have $\tilde{Z}_{\text{lin}}(c) = \omega_d^t\, c^t$, where ω_d^t is a positive real number. The orange curve, $\tilde{Z}_{\text{step}}(c)$, varies according to a step function, *i.e.*, $Z(c) = \Omega_d^t \mathbf{1}_{\{c_t > \tau_t\}}$, where Ω_d^t is a positive real number and $\mathbf{1}_{\{\bullet\}}$ is the indicator function. In this paper, we derive solutions for the linear approximation. Under this approximation, the utility of malicious S is given by

$$U_d^S\,(m, c) = \tilde{Z}_{\text{lin}}(c) + \omega_d^g\, c_g + \omega_d^f\, c_f = \omega_d^t\, c_t + \omega_d^g\, c_g + \omega_d^f\, c_f.$$

where $\omega_d^g < 0$ and $\omega_d^f < 0$ represent the utility to malicious S for each device that locks down or uses active defense, respectively.

Using $\tilde{Z}_{\text{lin}}(c)$, the decomposition property of the Poisson r.v. simplifies $\bar{U}_x^S(\sigma_x^S, \sigma^R)$. We show in Appendix A that the sender's expected utility depends on the expected values of each of the Poisson r.v. that represent the number of receivers who choose each action c_a, $a \in A$. The result is that

$$\bar{U}_x^S(\sigma_x^S, \sigma^R) = \lambda \sigma_x^S(p) \sum_{y \in Y} \sum_{e \in E} \sum_{a \in A} q^R(y)\, \delta_y(e \,|\, x, p)\, \sigma_y^R(a \,|\, p, e) \overset{a}{\underset{x}{\omega}}. \tag{7}$$

Next, assume that the utility of each receiver does not depend directly on the actions of the other receivers. (In fact, the receivers are still endogenously coupled through the action of S.) Abusing notation slightly, we drop c (the count of receiver actions) in $U_y^R(x, m, a, c)$ and σ^R (the strategies of the other receivers) in $\bar{U}_y^R(\theta, \sigma^R \,|\, m, e, \mu_y^R)$. Equation (2) is now

$$\bar{U}_y^R\left(\theta \,|\, m, e, \mu_y^R\right) = \sum_{x \in X} \sum_{a \in \{t,f\}} \mu_y^R(x \,|\, m, e)\, \theta(a \,|\, m, e)\, \mathcal{U}_y^R(x, m, a).$$

5 Equilibrium Analysis

In this section, we obtain the equilibrium results by parameter region. In order to simplify analysis, without loss of generality, let the utility functions be the same for all receiver types (except when $a = f$), *i.e.*, $\forall x \in X$, $U_k^R(x, p, t) = U_o^R(x, p, t) = U_v^R(x, p, t)$. Also without loss of generality, let the quality of the detectors for types $y \in \{o, v\}$ be the same: $\forall e \in E, x \in X$, $\delta_o(e \,|\, x, p) = \delta_v(e \,|\, x, p)$.

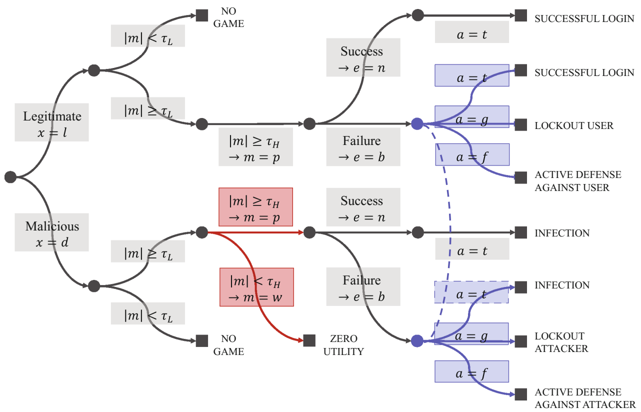

Fig. 5. Model of a PSG under Lemma 1. Only one of many R is depicted. After the types x and y, of S and R, respectively, are drawn, S chooses whether to persist beyond τ_L attempts. Then R chooses to trust, lockout, or use active defense against S based on whether S is successful. Lemma 1 determines all equilibrium strategies except $\sigma_d^{S*}(\bullet)$, $\sigma_o^{R*}(\bullet \,|\, p, b)$, and $\sigma_v^{R*}(\bullet \,|\, p, b)$, marked by the blue and red items. (Color figure online)

5.1 PSG Parameter Regime

We now obtain equilibria for a natural regime of the PSG parameters. First, assume that legitimate senders always persist: $\sigma_l^S(p) = 1$. This is natural for our application, because IoT HVAC users will always attempt to login. Second, assume that R of all types trust login attempts which appear to be legitimate (*i.e.*, give evidence $e = n$). This is satisfied for

$$q^S(d) < \frac{U_k^R(l,p,t)}{U_k^R(l,p,t) - U_k^R(d,p,t)}. \tag{8}$$

Third, we consider the likely behavior of R of type o when a login attempt is suspicious. Assume that she will lock down rather than trust the login. This occurs under the parameter regime

$$q^S(d) > \frac{\tilde{U}_o^R(l,p,t)}{\tilde{U}_o^R(l,p,t) - \tilde{U}_o^R(d,p,t)}, \tag{9}$$

using the shorthand notation

$$\tilde{U}_o^R(l,p,t) = U_o^R(l,p,t)\,\delta_0(b\,|\,l,p), \quad \tilde{U}_o^R(d,p,t) = U_o^R(d,p,t)\,\delta_0(b\,|\,d,p).$$

The fourth assumption addresses the action of R of type v when a login attempt is suspicious. The optimal action depends on her belief $\mu_o^R(d\,|\,p,b)$ that S is malicious. The belief, in turn, depends on the mixed-strategy probability with which malicious S persist. We assume that there is some $\sigma_d^S(p)$ for which R should lock down $(a = g)$. This is satisfied if there exists a real number $\phi \in [0,1]$ such that, given[6] $\sigma_d^S(p) = \phi$,

$$\bar{U}_v^R(t\,|\,p,b,\mu_v^R) > 0, \quad \bar{U}_v^R(f\,|\,p,b,\mu_v^R) > 0. \tag{10}$$

This simplifies analysis, but can be removed if necessary.

Lemma 1 summarizes the equilibrium results under these assumptions. Legitimate S persist, and R of type o lock down under suspicious login attempts. All receiver types trust login attempts which appear legitimate. R of type k, since she cannot differentiate between login attempts, trusts all of them. The proof follows from the optimality conditions in Eqs. (4–6) and the assumptions in Eqs. (8–10).

Lemma 1 *(Constant PBNE Strategies)***.** *If* $\sigma_d^S(p) = 1$ *and Eqs. (8–10) hold, then the following equilibrium strategies are implied:*

$$\sigma_l^{S*}(p) = 1, \ \sigma_o^{R*}(g\,|\,p,b) = 1, \ \sigma_k^{R*}(t\,|\,p,b) = 1,$$
$$\sigma_o^{R*}(t\,|\,p,n) = \sigma_v^{R*}(t\,|\,p,n) = \sigma_k^{R*}(t\,|\,p,n) = 1.$$

Figure 5 depicts the results of Lemma 1. The remaining equilibrium strategies to be obtained are denoted by the red items for S and the blue items for R. These strategies are $\sigma_o^{R*}(\bullet\,|\,p,b)$, $\sigma_v^{R*}(\bullet\,|\,p,b)$, and $\sigma_d^{S*}(p)$. Intuitively, $\sigma_d^{S*}(p)$ depends on whether R of type o and type v will lock down and/or use active defense to oppose suspicious login attempts.

[6] We abuse notation slightly to write $\bar{U}_v^R(a\,|\,m,e,\mu_y^R)$ for the expected utility that R of type v obtains by playing action a.

5.2 Equilibrium Strategies

The remaining equilibrium strategies fall into four parameter regions. In order to delineate these regions, we define two quantities.

Let $TD_v^R(U_v^R, \delta_v)$ denote a threshold which determines the optimal action of R of type v if $\sigma_d^S(p) = 1$. If $q^S(d) > TD_v^R(U_v^R, \delta_v)$, then the receiver uses active defense with some probability. Equation (3) can be used to show that

$$TD_v^R\left(U_v^R, \delta_v\right) = \frac{\tilde{U}_v^R\left(l, p, f\right)}{\tilde{U}_v^R\left(l, p, f\right) - \tilde{U}_v^R\left(d, p, f\right)},$$

where we have used the shorthand notation:

$$\tilde{U}_v^R\left(l, p, f\right) := U_v^R\left(l, p, f\right)\delta_v\left(b \,|\, l, p\right), \;\; \tilde{U}_v^R\left(d, p, f\right) := U_v^R\left(d, p, f\right)\delta_v\left(b \,|\, d, p\right).$$

Next, let $BP_d^S\left(\omega_d, q^R, \delta\right)$ denote the benefit which S of type d receives for choosing $m = p$, *i.e.*, for persisting. We have

$$BP_d^S\left(\omega_d, q^R, \delta\right) := \sum_{y\in Y}\sum_{e\in E}\sum_{a\in A} q^R\left(y\right)\delta_y\left(e \,|\, d, p\right)\sigma_y^R\left(a \,|\, p, e\right)\omega_d^a.$$

If this benefit is negative, then S will not persist. Let $BP_d^S\left(\omega_d, q^R, \delta \,|\, a_k, a_o, a_v\right)$ denote the benefit of persisting when receivers use the pure strategies:

$$\sigma_k^R\left(a_k \,|\, p, b\right) = \sigma_o^R\left(a_o \,|\, p, b\right) = \sigma_v^R\left(a_v \,|\, p, b\right) = 1.$$

We now have Theorem 1, which predicts the risk of malware infection in the remaining parameter regions. The proof is in Appendix B.

Theorem 1 *(PBNE within Regions).* *If $\sigma_d^S(p) = 1$ and Eqs. (8–10) hold, then $\sigma_o^{R*}(\bullet \,|\, p, b)$, $\sigma_v^{R*}(\bullet \,|\, p, b)$, and $\sigma_d^{S*}(p)$ vary within the four regions listed in Table 3.*

In the *status quo* equilibrium, strong and active receivers lock down under suspicious login attempts. But this is not enough to deter malicious senders from persisting. We call this the status quo because it represents current scenarios in which botnets infect vulnerable devices but incur little damage from being locked out of secure devices. This is a poor equilibrium, because $\sigma_d^{S*}(p) = 1$.

In the *active deterrence* equilibrium, lockouts are not sufficient to deter malicious S from fully persisting. But since $q^S(d) > TD_v^R$, R of type v use active defense. This is enough to deter malicious $S : \sigma_d^{S*}(p) < 1$. In this equilibrium, R of type o always locks down: $\sigma_o^{R*}\left(g \,|\, p, b\right) = 1$. R of type v uses active defense with probability

$$\sigma_v^{R*}\left(f \,|\, p, b\right) = \frac{\omega_d^t\, q^R\left(k\right) + \omega_d^g\left(q^R\left(o\right) + q^R\left(v\right)\right)}{\left(\omega_d^g - \omega_d^f\right) q^R\left(v\right)\delta_v\left(v \,|\, d, p\right)}, \tag{11}$$

and otherwise locks down: $\sigma_v^{R*}(g \mid p,b) = 1 - \sigma_v^{R*}(f \mid p,b)$. Deceptive S persist with reduced probability

$$\sigma_d^{S*}(p) = \frac{1}{q^S(d)} \left(\frac{\tilde{U}_v^R(l,p,f)}{\tilde{U}_v^R(l,p,f) - \tilde{U}_v^R(d,p,f)} \right). \tag{12}$$

In the *resistant attacker* equilibrium, $q^S(d) > TD_v^R$. Therefore, R of type v use active defense. But $BP_d^S(\bullet \mid t,g,f) > 0$, which means that the active defense is not enough to deter malicious senders. This is a "hopeless" situation for defenders, since all available means are not able to deter malicious senders. We still have $\sigma_d^{S*}(p) = 1$.

In the *vulnerable attacker* equilibrium, there is no active defense. But R of type o and type v lock down under suspicious login attempts, and this is enough to deter malicious S, because $BP_d^S(\bullet \mid t,g,g) < 0$. R of types o and v lock down with probability

$$\sigma_o^{R*}(g \mid p,b) = \sigma_v^{R*}(g \mid p,b) = \frac{\omega_d^t}{\left(q^R(0) + q^R(v)\right)\delta_o(b \mid d,p)\left(\omega_d^t - \omega_d^g\right)}, \tag{13}$$

and trust with probability $\sigma_o^{R*}(t \mid p,b) = \sigma_v^{R*}(t \mid p,b) = 1 - \sigma_o^{R*}(g \mid p,b)$. Deceptive S persist with reduced probability

$$\sigma_d^{S*}(p) = \frac{1}{q^S(d)} \left(\frac{\tilde{U}_o^R(l,p,t)}{\tilde{U}_o^R(l,p,t) - \tilde{U}_o^R(d,p,t)} \right). \tag{14}$$

The *status quo* and *resistant attacker* equilibria are poor results because infection of devices is not deterred at all. The focus of Sect. 6 will be to shift the PBNE to the other equilibrium regions, in which infection of devices is deterred to some degree.

Table 3. Equilibrium regions of the PSG for PDoS

<table>
<tr><th></th><th>$q^S(d) < TD_v^R(\bullet)$</th><th>$q^S(d) > TD_v^R(\bullet)$</th></tr>
<tr><td>$BP_d^S(\bullet \mid t,g,g) < 0$,
$BP_d^S(\bullet \mid t,g,f) < 0$</td><td colspan="2">Vulnerable Attacker
$\sigma^{S*}(p) < 1$
$0 < \sigma_o^{R*}(t \mid p,b), \sigma_o^{R*}(g \mid p,b) < 1$
$0 < \sigma_v^{R*}(t \mid p,b), \sigma_v^{R*}(g \mid p,b) < 1$</td></tr>
<tr><td>$BP_d^S(\bullet \mid t,g,g) > 0$,
$BP_d^S(\bullet \mid t,g,f) < 0$</td><td rowspan="2">Status Quo
$\sigma^{S*}(p) = 1$
$\sigma_o^{R*}(g \mid p,b) = 1$
$\sigma_v^{R*}(g \mid p,b) = 1$</td><td>Active Deterrence
$\sigma^{S*}(p) < 1$
$\sigma_o^{R*}(g \mid p,b) = 1$
$0 < \sigma_v^{R*}(g \mid p,b)$,
$\sigma_v^{R*}(f \mid p,b) < 1$</td></tr>
<tr><td>$BP_d^S(\bullet \mid t,g,g) > 0$,
$BP_d^S(\bullet \mid t,g,f) > 0$</td><td>Resistant Attacker
$\sigma^{S*}(p) = 1$
$\sigma_o^{R*}(g \mid p,b) = 1$
$\sigma_v^{R*}(f \mid p,b) = 1$</td></tr>
</table>

6 Mechanism Design

The equilibrium results are delineated by the quantities q^S, $TD_v^R(U_v^R, \delta_v)$ and $BP_d^S(\omega_d, q^R, \delta)$. These quantities are functions of the parameters q^S, q^R, δ_o, δ_v, ω_d, and U_v^R. Mechanism design manipulates these parameters in order to obtain a desired equilibrium. We discuss two possible mechanisms.

6.1 Legislating Basic Security

Malware which infects IoT devices is successful because many IoT devices are poorly secured. Therefore, one mechanism design idea is to legally require better authentication methods, in order to decrease $q^R(k)$ and increase $q^R(o)$.

The left-hand sides of Figs. 6, 7 and 8 depict the results. Figure 6(a) shows that decreasing $q^R(k)$ and increasing $q^R(o)$ moves the game from the *status quo* equilibrium to the *vulnerable attacker* equilibrium. But Fig. 7(a) shows that this only causes a fixed decrease in $\sigma_d^{S*}(p)$, regardless of the amount of decrease in $q^R(k)$. The reason, as shown in Fig. 8(a), is that as $q^R(o)$ increases, it is incentive-compatible for receivers to lock down with progressively lower probability $\sigma_y^{R*}(g \mid p, b)$, $y \in \{o, v\}$. Rather than forcing malicious S to not persist,

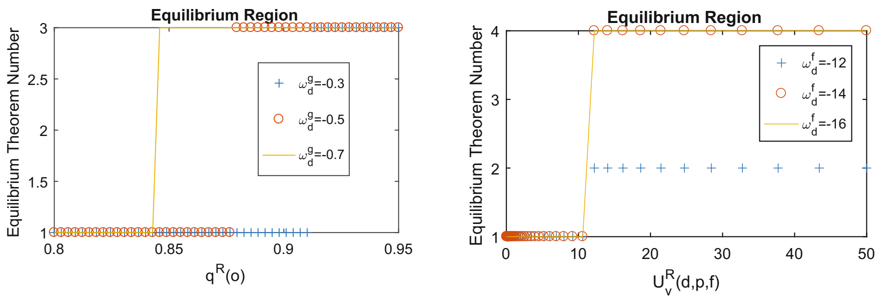

Fig. 6. Equilibrium transitions for (a) legal and (b) active defense mechanisms. The equilibrium numbers signify: 1-*status quo*, 2-*resistant attacker*, 3-*vulnerable attacker*, 4-*active deterrence*.

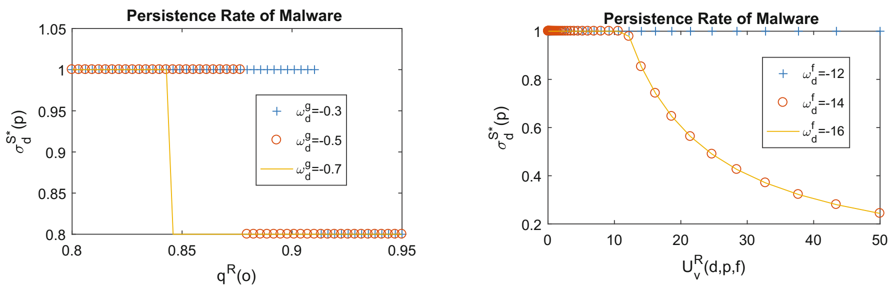

Fig. 7. Malware persistence rate for (a) legal and (b) active defense mechanisms.

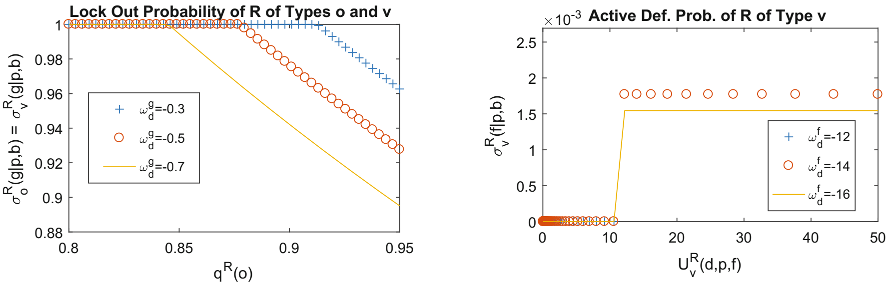

Fig. 8. Probabilities of opposing malicious S. Plot (a): probability that R lock down with the legal mechanism. Plot (b): probability that R use active defense.

increasing $q^R(o)$ only decreases the incentive for receivers to lock down under suspicious login attempts.

6.2 Incentivizing Active Defense

One reason for the proliferation of IoT malware is that most devices which are secure (*i.e.*, R of type $y = o$) do not take any actions against malicious login attempts except to lock down (*i.e.*, to play $a = g$). But there is almost no cost to malware scanners for making a large number of login attempts under which devices simply lock down. There is a lack of economic pressure which would force $\sigma_d^{S*}(p) < 1$, unless $q^R(0) \approx 1$.

This is the motivation for using active defense such as reporting the activity to an ISP or recording the attempts in order to gather information about the attacker. The right hand sides of Figs. 6, 7 and 8 show the effects of providing an incentive $U_v^R(d, p, f)$ for active defense. This incentive moves the game from the *status quo* equilibrium to either the *resistant attacker* equilibrium or the *vulnerable attacker* equilibrium, depending on whether $BP_d^S(\bullet \,|\, t, g, f)$ is positive (Fig. 6(b)). In the *vulnerable attacker* equilibrium, the persistence rate of malicious S is decreased (Fig. 7(b)). Finally, Fig. 8(b) shows that only a small amount of active defense $\sigma_v^{R*}(f \,|\, p, b)$ is necessary, particularly for high values of[7] ω_d^f.

7 Discussion of Results

The first result is that *the defender can bound the activity level of the botnet*. Recall that the *vulnerable attacker* and *active deterrence* equilibria force $\sigma_d^{S*}(p) < 1$. That is, they decrease the persistence rate of the malware scanner. But another interpretation is possible. In Eqs. (14) and (12), the product $\sigma_d^{S*}(p)\, q^S(d)$ is bounded. This product can be understood as the *total activity* of botnet scanners: a combination of prior probability of malicious senders and

[7] In Fig. 8(b), $\sigma_v^{R*}(f \,|\, p, b) = 1$ for $\omega_d^f = -12$.

the effort that malicious senders exert[8]. Bensoussan *et al.* note that the operators of the Confiker botnet of 2008–2009 were forced to limit its activity [5,13]. High activity levels would have attracted too much attention. The authors of [5] confirm this result analytically, using a dynamic game based on an SIS infection model. Interestingly, our result agrees with [5], but using a different framework.

Secondly, we *compare the effects of legal and economic mechanisms to deter recruitment for PDoS*. Figures 6(a)–8(a) showed that $\sigma_d^{S*}(p)$ can only be reduced by a fixed factor by mandating security for more and more devices. In this example, we found that strategic behavior worked against legal requirements. By comparison, Figs. 6(b)–8(b) showed that $\sigma_d^{S*}(p)$ can be driven arbitrarily low by providing an economic incentive $U_v^R(d, p, f)$ to use active defense.

Future work can evaluate technical aspects of mechanism design such as improving malware detection quality. This would involve a non-trivial trade-off between a high true-positive rate and a low false-positive rate. Note that the model of Poisson signaling games is not restricted PDoS attacks. PSG apply to any scenario in which one sender communicates a possibly malicious or misleading message to an unknown number of receivers. In the IoT, the model could capture the communication of a roadside location-based service to a set of autonomous vehicles, or spoofing of a GPS signal used by multiple ships with automatic navigation control, for example. Online, the model could apply to deceptive opinion spam in product reviews. In interpersonal interactions, PSG could apply to advertising or political messaging.

A Simplification of Sender Expected Utility

Each each component of c is distributed according to a Poisson r.v. The components are independent, so $\mathbb{P}\{c \,|\, \sigma^R, x, m\} = \prod_{a\in A} \mathbb{P}\{c_a \,|\, \sigma^R, x, m\}$. Recall that S receives zero utility when he plays $m = w$. So we can choose $m = p$:

$$\bar{U}_x^S(\sigma_x^S, \sigma^R) = \sigma_x^S(p) \sum_{c\in\mathbb{Z}(A)} \prod_{a\in A} \mathbb{P}\left\{c_a \,|\, \sigma^R, x, p\right\} \left(\overset{t}{\underset{x}{\omega}} c_t + \overset{g}{\underset{x}{\omega}} c_g + \overset{f}{\underset{x}{\omega}} c_f \right).$$

Some of the probability terms can be summed over their support. We are left with

$$\bar{U}_x^S(\sigma_x^S, \sigma^R) = \sigma_x^S(p) \sum_{a\in A} \overset{a}{\underset{x}{\omega}} \sum_{c_a\in\mathbb{Z}_+} c_a \mathbb{P}\left\{c_a \,|\, \sigma^R, x, p\right\}. \tag{15}$$

The last summation is the expected value of c_a, which is λ_a. This yields Eq. (7).

[8] A natural interpretation in an evolutionary game framework would be that $\sigma_d^{S*}(p) = 1$, and $q^S(d)$ decreases when the total activity is bounded. In other words, malicious senders continue recruiting, but some malicious senders drop out since not all of them are supported in equilibrium.

B Proof of Theorem 1

The proofs for the *status quo* and *resistant attacker* equilibria are similar to the proof for Lemma 1. The *vulnerable attacker* equilibrium is a partially-separating PBNE. Strategies $\sigma_o^{R*}(g\,|\,p,b)$ and $\sigma_v^{R*}(g\,|\,p,b)$ which satisfy Eq. (13) make malicious senders exactly indifferent between $m=p$ and $m=w$. Thus, they can play the mixed-strategy in Eq. (14), which makes strong and active receivers exactly indifferent between $a=g$ and $a=t$. The proof of the *vulnerable attacker* equilibrium follows a similar logic.

References

1. Free community-based mapping, traffic and navigation app. Waze Mobile. https://www.waze.com/
2. Visions and challenges for realising the internet of things. Technical report, CERP IoT Cluster, European Commission (2010)
3. Account lockout threshold. Microsoft TechNet (2014). https://technet.microsoft.com/en-us/library/hh994574(v=ws.11).aspx
4. Amini, S., Mohsenian-Rad, H., Pasqualetti, F.: Dynamic load altering attacks in smart grid. In: Innovative Smart Grid Technologies Conference, pp. 1–5. IEEE (2015)
5. Bensoussan, A., Kantarcioglu, M., Hoe, S.R.C.: A game-theoretical approach for finding optimal strategies in a botnet defense model. In: Alpcan, T., Buttyán, L., Baras, J.S. (eds.) GameSec 2010. LNCS, vol. 6442, pp. 135–148. Springer, Heidelberg (2010). doi:10.1007/978-3-642-17197-0_9
6. Byers, T.: Demand response and the IoT: using data to maximize customer benefit. Comverge Blog (2017). http://www.comverge.com/blog/february-2017/demand-response-and-iot-using-data-to-maximize-cus/
7. Crawford, V.P., Sobel, J.: Strategic information transmission. Econom. J. Econom. Soc. **50**(6), 1431–1451 (1982)
8. Fudenberg, D., Tirole, J.: Game Theory, vol. 393. MIT Press, Cambridge (1991)
9. Glover, J.D., Sarma, M.S., Overbye, T.: Power System Analysis & Design, SI Version. Cengage Learning, Boston (2012)
10. Hammerstrom, D.J.: Part II. Grid friendly appliance project. In: GridWise Testbed Demonstration Projects. Pacific Northwest National Laboratory (2007)
11. Hayel, Y., Zhu, Q.: Epidemic protection over heterogeneous networks using evolutionary poisson games. IEEE Trans. Inf. Forensics Secur. **12**(8), 1786–1800 (2017)
12. Herzberg, B., Bekerman, D., Zeifman, I.: Breaking down mirai: An IoT DDoS botnet analysis. Incapsula Blog, Bots and DDoS, Security (2016). https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html
13. Higgins, K.J.: Conficker botnet 'dead in the water', researcher says, 2010. Dark Reading. http://www.darkreading.com/attacks-breaches/conficker-botnet-dead-in-the-water-researcher-says/d/d-id/1133327?
14. Lewis, D.: Convention: A Philosophical Study. Wiley, New York (2008)
15. Meyer, R.: How a Bunch of Hacked DVR Machines Took Down Twitter and Reddit. The Atlantic, Darya Ganj (2016)
16. Mohammadi, A., Manshaei, M.H., Moghaddam, M.M., Zhu, Q.: A game-theoretic analysis of deception over social networks using fake avatars. In: Zhu, Q., Alpcan, T., Panaousis, E., Tambe, M., Casey, W. (eds.) GameSec 2016. LNCS, vol. 9996, pp. 382–394. Springer, Cham (2016). doi:10.1007/978-3-319-47413-7_22

17. Mohsenian-Rad, A.-H., Leon-Garcia, A.: Distributed internet-based load altering attacks against smart power grids. IEEE Trans. Smart Grid **2**(4), 667–674 (2011)
18. Myerson, R.B.: Population uncertainty and poisson games. Int. J. Game Theor. **27**(3), 375–392 (1998)
19. Pawlick, J., Farhang, S., Zhu, Q.: Flip the cloud: cyber-physical signaling games in the presence of advanced persistent threats. In: Khouzani, M.H.R., Panaousis, E., Theodorakopoulos, G. (eds.) GameSec 2015. LNCS, vol. 9406, pp. 289–308. Springer, Cham (2015). doi:10.1007/978-3-319-25594-1_16
20. Pawlick, J., Zhu, Q.: Deception by design: evidence-based signaling games for network defense. In: Workshop on the Economics of Information Security and Privacy, Delft, The Netherlands (2015)
21. Pawlick, J., Zhu, Q.: Strategic trust in cloud-enabled cyber-physical systems with an application to glucose control. IEEE Trans. Inf. Forensics and Secur. (2017, to appear)
22. Radke, R.J., Woodstock, T-K., Imam, M.H., Sanderson, A.C., Mishra, S.: Advanced sensing and control in the smart conference room at the center for lighting enabled systems and applications. In: SID Symposium Digest of Technical Papers, vol. 47, pp. 193–196. Wiley Online Library (2016)
23. Vrij, A., Mann, S.A., Fisher, R.P., Leal, S., Milne, R., Bull, R.: Increasing cognitive load to facilitate lie detection: the benefit of recalling an event in reverse order. Law Hum. Behav. **32**(3), 253–265 (2008)
24. Wu, Q., Shiva, S., Roy, S., Ellis, C., Datla, C.: On modeling and simulation of game theory-based defense mechanisms against DoS and DDoS attacks. In: Proceedings of Spring Simulation Multiconference, p. 159. Society for Computer Simulation International (2010)