Deception-Based Game Theoretical Approach to Mitigate DoS Attacks

Hayreddin Çeker[1(✉)], Jun Zhuang[1], Shambhu Upadhyaya[1], Quang Duy La[2], and Boon-Hee Soong[3]

[1] University at Buffalo, Buffalo, NY 14260, USA
{hayreddi,jzhuang,shambhu}@buffalo.edu
[2] Singapore University of Technology and Design, Singapore 487372, Singapore
quang_la@sutd.edu.sg
[3] Nanyang Technological University, Singapore 639798, Singapore
ebhsoong@ntu.edu.sg

Abstract. Denial of Service (DoS) attacks prevent legitimate users from accessing resources by compromising availability of a system. Despite advanced prevention mechanisms, DoS attacks continue to exist, and there is no widely-accepted solution. We propose a deception-based protection mechanism that involves game theory to model the interaction between the defender and the attacker. The defender's challenge is to determine the optimal network configuration to prevent attackers from staging a DoS attack while providing service to legitimate users. In this setting, the defender can employ camouflage by either disguising a normal system as a honeypot, or by disguising a honeypot as a normal system. We use *signaling game* with perfect Bayesian equilibrium (PBE) to explore the strategies and point out the important implications for this type of dynamic games with incomplete information. Our analysis provides insights into the balance between resource and investment, and also shows that defenders can achieve high level of security against DoS attacks with cost-effective solutions through the proposed deception strategy.

Keywords: Game theory · Deception · DoS attacks · Honeypot · Perfect Bayesian equilibrium · Security · Signaling game

1 Introduction

A denial of service (DoS) attack is an attempt to prevent legitimate users from accessing resources. An attacker may target an entire network to cause temporary or permanent unavailability, reduce intended users' bandwidth, or interrupt access to a particular service or a system. The distributed DoS (DDoS) attacks even make it more difficult to prevent and harder to recover. These attacks have already become a major threat to the stability of the Internet [7]. In the survey paper on DDoS attacks, Lau et al. [17] observe that as time has passed, the distributed techniques (e.g., Trinoo, TFN, Stacheldraht, Shaft, and TFN2K) have

Q. Zhu et al. (Eds.): GameSec 2016, LNCS 9996, pp. 18–38, 2016.
DOI: 10.1007/978-3-319-47413-7_2

become more advanced and complicated. Many observers have stated that there is currently no successful defense against a fully distributed DoS attack.

In addition, attackers have the advantage of time and stealth over defenders, since an attacker can obtain information about a defender by pretending to be a legitimate user. Thus, in order to counter this imbalance, *deception* can be utilized to lead an attacker to take actions in the defender's favor by sending fake signals. This way, deception can be used to increase the relative cost of attack, which in turn will delay the attacker because of the uncertainty. In the meantime, the defender can work on solutions to defer and counter the potential attacks. In this setting, although, both the defender and the attacker may spend extra resources to understand the real intention of each other, from the defender's view point, this approach provides a means to mitigate DoS attacks.

Furthermore, the need for protection against DoS attacks extends beyond employing routine intrusion detection system into the domain of survivability. Survivability focuses on the provisioning of essential services in a timely manner without relying on the guarantee that precautionary measures will always succeed against failures, accidents as well as coordinated attacks. It is not an easy task to capture unprecedented DoS attacks while monitoring the entire traffic and providing service to legitimate users. Some resources are to be allocated for attacker detection and advanced tracking tools are to be utilized to protect against patient, strategic and well organized attackers. At the end, it turns out to be an optimization problem from the defender's side about how to allocate the limited resources in a way that the cost will be minimum while the deterrence will be maximum. Similarly, the attacker will try to cause as much damage as possible with limited resources.

In this paper, we propose a game-theoretical approach to model the interaction between the defender and the attacker by deploying honeypots as a means to attract the attacker and retrieve information about the attacker's real intention. A honeypot, unlike a normal system, is a computer system to trap the attacker [3]. Honeypots produce a rich source of information by elaborating the attacker intention and methods used when attackers attempt to compromise a seemingly real server.

In addition to deploying honeypots, we employ deception in our dynamic game in which players (i.e., defender and attacker) take turns choosing their actions. In the scenario under study, the defender moves first by deciding whether to camouflage or not, after which the attacker responds with attack, observe or retreat actions. It is a game of incomplete information because of the attacker's uncertainty of system type. We determine the perfect Bayesian equilibria (PBE) at which both players do not have incentives to deviate from the actions taken.

The contribution of this paper is two-fold: (1) A new defense framework which proactively uses deception as a means to assist in developing effective responses against unconventional, coordinated and complex attacks emanating from adversaries. (2) Determination of the Bayesian equilibrium solutions for this model and analyze the corresponding strategies of the players using a new quantification method for the cost variables.

We also show that deception is an optimal/best response action in some cases where the attacker chooses not to attack a real server because of the confusion caused in the signaling game. Furthermore, we include comprehensive graphics to reflect the possible scenarios that may occur between an attacker and a defender.

The paper continues with the background information and related work on the use of game theory in DoS attacks in Sect. 2. We give the details on the formulation of our model, and specify the assumptions made and notations used in this paper in Sect. 3. In Sect. 4, in case of an attack, the methods for quantifying the damage to a defender and the benefit to an attacker are discussed. Then, we continue with the analysis of PBE and document pooling and separating equilibria in Sect. 5. Section 6 presents the equilibria solutions under various circumstances and find out important implications about the interaction between a defender and an attacker. Section 7 compares our model with real-life systems, and finally Sect. 8 summarizes our findings and gives an insight into how our methodology could be improved further.

Occasionally, the feminine subject she is used to refer to the defender and he to the attacker in the rest of the paper.

2 Background

In this section, we briefly review the basic elements of the game theoretical approach, and relate them to our proposed solution.

2.1 Deception via Honeypots

Game theory has been used in the cyber-security domain ranging from wireless sensor networks [14,28] to DoS attacks [1,18] and information warfare [13] in general. Specifically for DoS attacks, after an attack plan is made by an attacker, even though launching a DoS attack against a victim/defender is always preferred regardless of system type (because of, say, its low cost), the attacker might prefer not to attack if he cannot confirm if a system is of a normal type or a honeypot [6,19].

Defenders can employ deception to increase the effectiveness of their defense system and also to overcome a persistent adversary equipped with sophisticated attack strategies and stealth.

Deception has been used in the military [8,24] and homeland security [29] to protect information critical systems. When attackers cannot determine the type of a system due to deception employed by the defender, they might want to postpone the attack or retreat conditionally. Additional resources might be required to perceive the true system type. In other words, deception hampers the attackers' motivation by increasing the cost. In this paper, we explore the strategies for the defender to estimate the expectations of an attacker and behave accordingly in order to halt him from becoming excessively aggressive and launching DoS attacks. Although we illustrate the solution for DoS attacks, the framework can be used for addressing broader category of attacks in general.

In the context of DoS attacks, a defender can deceive an attacker by deploying several honeypots in her system, and behave as if the attack was successful. However, an intelligent attacker can run simple scripts to understand the real type of the system. For example, an attacker can measure simple I/O time delays or examine unusual and random system calls on the defender server. Similarly, temptingly obvious file names (e.g., "passwords"), and the addition of data in memory as discussed in [10] can disclose the system type obviously [6]. On the other hand, Rowe et al. [24] propose using *fake honeypots* (normal systems that behave as honeypots) to make the job of detecting system type more complicated for the attacker. It is also a form of deception in which the system is camouflaged or disguised to appear as some other types [5].

Similarly, Pibil et al. [21] investigate how a honeypot should be designed and positioned in a network in such a way that it does not disclose valuable information but attracts the attacker for target selection. Also, La et al. [16] analyze a honeypot-enabled network that comprises of IoTs to defend the system against deceptive attacks. In this setting, the attacker might avoid attacking, assuming that the system could be actually a honeypot. As this defensive strategy becomes common knowledge between players, the attacker needs to expend additional resources to determine a system's true type.

Accordingly, a defender can use deception to halt the attacker from executing his contingency plan until she is better prepared, or to effectively recover the system to a secure state that patches all the vulnerabilities exploited by the attacker in the current recovery cycle. The concept of deception is formulated in greater detail in [23,30] as a multi-period game. In this paper, we use a formulation method similar to Zhuang et al. [31] for single period games.

2.2 DoS Attacks from a Game-Theoretical Perspective

The studies that analyze DoS attacks from the game theoretical perspective mostly applied game theory on wireless sensor networks (WSN) considering an intrusion detector as defender and malicious nodes among the sensors as attackers [18,28]. Malicious nodes are those sensors that do not forward incoming packets properly.

Agah and Das [1] formulate the prevention of passive DoS attacks in wireless sensor networks as a repeated game between an intrusion detector and nodes of a sensor network, where some of these nodes act maliciously. In order to prevent DoS, they model the interaction between a normal and a malicious node in forwarding incoming packets, as a non-cooperative N player game.

Lye et al. [18] deal with interactions between an attacker and an administrator of a web server. The game scenario begins with the attacker's attempts to hack the homepage, and the Nash equilibria are computed accordingly. By verifying the usefulness of the approach with network managers, they conclude that the approach can be applied on heterogeneous networks with proper modeling. As for Hamilton et al. [13], they take the security issues from a very general perspective and discuss the role of game theory in information warfare. The paper focuses mostly on areas relevant to tactical analysis and DoS attacks.

Some of the studies that involve game theory about DoS attacks are discussed in a survey by Shen et al. [25]. Here the authors categorize them under non-cooperative, cooperative and repeated game models. However, the use of *signaling game* in DoS attacks is not mentioned under those categories as it is a new area that we explore throughout this paper. Nevertheless, a theoretical analysis of DDoS attacks is proposed using signaling game in [12]. They show the effectiveness and feasibility of a defense strategy based on port and network address hopping compared to packet filtering alone and do not employ any deception. The study is very specific to certain conditions and lacks a comprehensive analysis of possible scenarios that may occur between an attacker and a defender.

The work closest to ours is that of Carroll and Grosu [6] who also use signaling game to investigate the interactions between an attacker and a defender of a computer network. Honeypots are added to the network to enable deception, and they show that camouflage can be an equilibrium strategy for the defender. We extend this study to a broader aspect that includes DoS attacks and we not only find out inequalities that must hold during the game with certain parameters but also propose a parameter valuation mechanism to quantify benefits and damages using existing security evaluations.

Although not directly related to DoS attacks, the authors in [26] study the interactions between a malicious node and a regular node by using PBE to characterize the beliefs the nodes have for each other. Since the best response strategies depend on the current beliefs, the authors apply signaling game to model the process of detecting the malicious nodes in the network.

Despite these studies end up with equilibrium points that represent how a defender and an attacker would act under some conditions, the formulations of the game require all parameters to be known in advance. Also, concrete modeling of DoS attacks requires involving various parameters and valuations of the players to explore equilibria. In this paper, we propose a quantification method with parametric functions under uncertain conditions (incomplete information). This way, the number of all possible scenarios increases and the interactions between players can be reflected in a more comprehensive manner.

3 Model Formulation

We start with a model of incomplete information in which only the defender has private information. In particular, the defender is of a particular type *normal* or *honeypot*. This private information is known by the defender herself but not by the attacker. Although the defender's type is not directly observable by the attacker, the prior probability of her type is assumed to be common knowledge to the attacker. We will let nature make the initial (zero-stage) move, randomly drawing the defender's type from the prior probability distribution.

A defender protects her network by deploying honeypots, which are traps to detect unauthorized access. The defender can disguise normal systems as honeypots and honeypots as normal systems. After the network is created, an

attacker then attempts to compromise systems. The attacker can successfully compromise normal systems, but not honeypots. If the attacker attempts to compromise a honeypot, the defender observes the actions and can later improve her defenses. We model this interaction between defender and attacker as a signaling game as described next.

3.1 Assumptions

Although DoS (especially distributed DoS) attacks are launched by a mass (army) of computers, we do restrict our attention to the case of a single centralized attacker where he can submit multiple requests to a server in parallel to cause unavailability (the main purpose of DoS attacks) or temporarily unreachable server error. Thus, we do not address the case of decentralized attackers (such as multiple hacker groups, countries or companies).

During the game, the attacker can update his knowledge about the defender type after observing the signal sent by the defender. However, we do not include any other types of observations (such as spying or probing attacks) for simplicity. Finally, we assume that the players are fully rational, and want to maximize their utilities.

3.2 Signaling Game with Perfect Bayesian Equilibrium

A signaling game is a dynamic game with two players: attacker and defender in our case. The defender has a certain type which is set by nature. The defender observes her own type to take an action during the game, while the attacker does not know the type of the defender. Based on the knowledge of her own type, the defender chooses to send a signal from a set of possible options. Then, the attacker observes the signal sent by the defender and chooses an action from a set of possible actions. At the end, each player gets the payoff based on the defender's type, the signal sent and the action chosen in response.

In our game, the nature decides the defender type to be either normal (N) or honeypot (H). Based on the type, the defender makes truthful disclosure or sends the deception signal. For example, when the defender sends 'H' signal (the apostrophe indicates the message is a signal) for N type, she informs the attacker as if the system is slowing down and the attack is successful. The attacker receives the signal 'H' or 'N' and decides whether to attack (A), observe (O) or retreat (R). Both players will choose the option which yields the maximum utility considering all possibilities.

However, in game theory, sometimes Nash equilibrium results in some implausible equilibria, such as incredible threats from the players. To deal with this type of threats, the concept of PBE which is a strategy profile that consists of sequentially rational decisions is utilized in a game with incomplete information. PBE can be used to refine the solution by excluding theoretically feasible but not probable situations [11].

3.3 Notation and Problem Formulation

We define the notations as follows:

- A and D: Attacker (signal receiver) and defender (signal sender), respectively.
- θ_D is the nature's decision of defender type.
- α^N and α^H are the probabilities of signaling 'N' which originates from a normal type and a honeypot defender, respectively.
- μ refers to the attacker's belief for the probability of receiving the signal 'N' from a normal type defender. Accordingly, $(1-\mu)$ represents the probability when the signal is 'N' but the defender type is honeypot.
- γ and $(1-\gamma)$ denote to the attacker's belief for how likely the signal of 'H' might have originated from a normal type defender or a honeypot.
- c_a and c_o are attacker's cost of attacking and observing respectively where $c_a, c_o \geqslant 0$ (we do not incur any charges for retreating in this model).
- b_a and b_o correspond to benefit of attacking and observing where $b_a \geqslant c_a, b_o \geqslant c_o$.
- c_c, c_s, c_h and c_w are defender's costs of compromise, signaling, honeypot and being watched, respectively, where $c_c, c_s, c_h, c_w \geqslant 0$.
- b_{cs} and b_w are customer satisfaction on normal system and benefit of observing the attacker on a honeypot, respectively.
- R_d is the service rate of the defender, and R_a, R_o are the attacking and observing rates of the attacker.
- C is the quantification factor for scaling the rates.

Table 1. Actions and posterior probabilities

$\alpha^N = \Pr(\text{'N'} \mid \text{type N})$	$(1-\alpha^N) = \Pr(\text{'H'} \mid \text{type N})$
$\alpha^H = \Pr(\text{'N'} \mid \text{type H})$	$(1-\alpha^H) = \Pr(\text{'H'} \mid \text{type H})$
$\mu = \Pr(\text{type N} \mid \text{'N'})$	$(1-\mu) = \Pr(\text{type H} \mid \text{'N'})$
$\gamma = \Pr(\text{type N} \mid \text{'H'})$	$(1-\gamma) = \Pr(\text{type H} \mid \text{'H'})$

3.4 Sequence of Actions in an Extensive Form

Figure 1 illustrates the sequence of deception actions of the signaling game in an extensive form. The nature decides the system type as normal (N) with probability θ_D (top part of the figure) or honeypot (H) with probability $1-\theta_D$ (bottom shaded part of the figure) and only defender knows it. The defender can choose to disclose her real type by sending message N (top-left branch) or H (bottom-right branch). On the other hand, she can choose to deceive the attacker by signaling 'H' in normal type (top-right branch) or 'N' in honeypot (bottom-left branch). The attacker receives the signal as 'N' or 'H' from the defender, updates his posterior probability and takes an action accordingly.

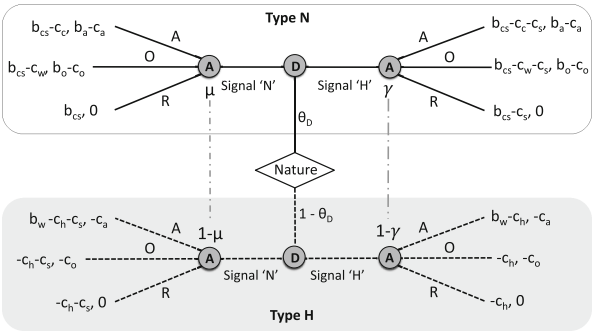


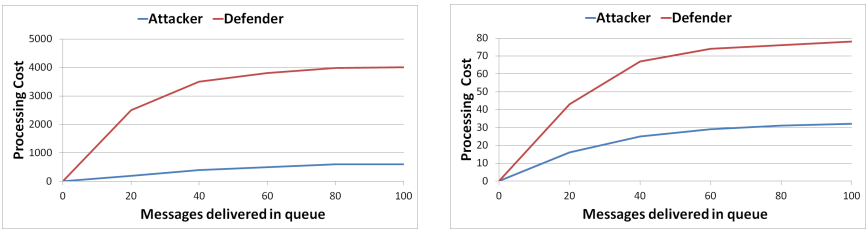
Fig. 1. Signaling game in extensive form

4 Quantification of Damage

We consider a game scenario in which the attacker is uncertain about the defender's asset valuation and the cost. In this section, we first quantify the cost of a DoS attack to the defender and to the attacker, then solve the perfect Bayesian equilibrium (PBE) using sequential rationality.

Basagiannis et al. [4] propose a probabilistic model to quantify the cost of a DoS attack to the defender and to the attacker using Meadows' framework [20]. Although the model makes the cost calculation by including a security protocol, the costs for both parties generically reflect the level of resource expenditure (memory, capacity, bandwidth) for the related actions. As the security level increases, the cost of providing security on the defender's side and the cost of breaking security on the attacker's side increase too. In [4], there is an analysis of how defender/attacker costs change with respect to security level. We refer to the high and low security level cases in Fig. 2a and b respectively. The security level referred in [4] is determined by the complexity of a puzzle that the attacker tries to solve by intercepting messages. In comparison of the processing costs at high security level with low security level, the relative costs to the defender and to the attacker can be approximated by the values specified in the figures for the quantification of equilibrium points. For example, the processing costs at high security level for 100 messages can be used to determine the cost of compromise (c_c) and cost of attacking (c_a), e.g., $c_c = 4000$ units and $c_a = 600$ units. Similarly considering the relative costs, the rewards at low level security can be used to quantify the costs when the defender chooses to disclose her own type and the attacker chooses to observe.

Moving forward with that analogy, the cost variables introduced in the extensive form of the game turn out to be: $c_c = 4000$ units, $c_a = 600$ units, $c_w = 80$ units and $c_o = 30$ units. We fit these values to estimate the service rate of the defender so that our analysis can explore the degradation as a result of the attacker's strategies. We use the formula derived in [15] to measure the



(a) High security level (b) Low security level

Fig. 2. Processing costs in high & low security levels [4]

satisfaction rate of customers (R) with respect to effective service rate:

$$U(R) = 0.16 + 0.8\,ln(R - 3) \tag{1}$$

Equation (1) quantifies the satisfaction of customers who visit the defender's resources (e.g., website) when she serves at a rate of R. The rate R can be disrupted by an attack as the attacker's aim is to cause unavailability for intended customers. Using this equation helps us reflect the degradation when there is an attack against the defender.

In [15], the maximum satisfaction is rated out of 5, we accept that value as normal case for which $R_d = 427.11$. We assume that the decrease in service rate will reduce the satisfaction of the customers, and eventually it will turn out to be a negative cost for the defender. This way, the satisfaction rate can be referred as the difference between the service rate of the defender and the degradation caused by the attacker. However, since the costs referred in [4] are of large magnitudes, to be able to properly measure the satisfaction rate, we scale it with a quantification factor, C.

We refer to the cost of defender as the degradation in the satisfaction, which corresponds to the difference between the satisfaction in normal case, $C \cdot U(R_d)$ and attack case, $C \cdot U(R_d - R_a)$ or observe case, $C \cdot U(R_d - R_o)$. It can be summarized as follows:

$$\begin{aligned} C \cdot U(R_d) - C \cdot U(R_d - R_a) &= C \cdot 0.8 \cdot ln(\frac{R-3}{R - R_a - 3}) = c_c \\ C \cdot U(R_d) - C \cdot U(R_d - R_o) &= C \cdot 0.8 \cdot ln(\frac{R-3}{R - R_o - 3}) = c_w \end{aligned} \tag{2}$$

Also, we assume that the cost of attacker is proportional to the rate that they send traffic to cause DoS attack: $\frac{R_a}{R_o} = \frac{c_a}{c_o} = \frac{600}{30} = 20$.

Solving these equations, we end up with $R_a = 389.31$ and $R_o = 19.46$. Having real values for the players' rates helps us estimate the constants in the cost table and make reasonable assumptions accordingly. Substituting the numeric values, we set $C = 1600$ and $c_s = 50$.

As a result, we represent the players' utilities for every action more accurately. Figure 3 updates the notation used in extensive form as a function of service/attack rate so that cost and benefit for each strategy are reflected to both players in a precise manner. New constant values such as v_a, v_1 and v_2 are introduced to reflect the conditional variables that arise based on the strategies taken by the players, e.g., the original service rate $(v_1 \cdot R_d)$ reduces to $v_2 \cdot R_d$ when signaling 'H' in normal type.

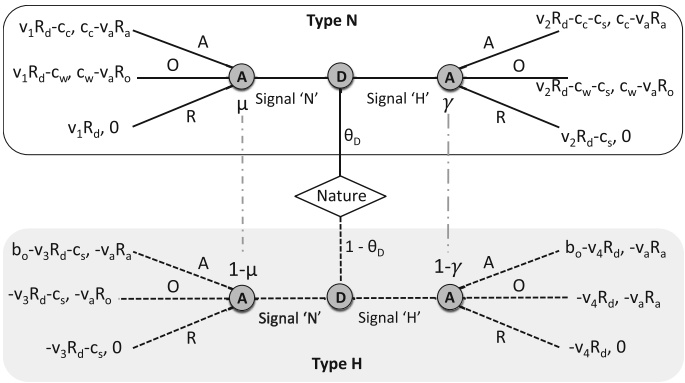


Fig. 3. Updated signaling game

5 Analysis of Perfect Bayesian Equilibrium

In a game with incomplete information, players might update their beliefs through observations about types of the opponent. This belief updating process must satisfy Bayes' rule in which posterior probability is determined by the priori and the likelihood of each type.

5.1 Separating Equilibria

In this section, we provide the steps to find out if there is a *separating equilibrium* where defenders' signals are different. We first examine the game depicted in Fig. 4 where both defender types are truthful, i.e., normal type's signal is 'N' and honeypot's signal is 'H'.

Based on the scenario, when the attacker receives the signal 'N' (on the left side), he updates the posterior probability, μ:

$$\mu = \frac{\theta_D \cdot \alpha^N}{\theta_D \cdot \alpha^N + (1 - \theta_D) \cdot \alpha^H} = \frac{\theta_D \cdot 1}{\theta_D \cdot 1 + (1 - \theta_D) \cdot 0} = 1$$

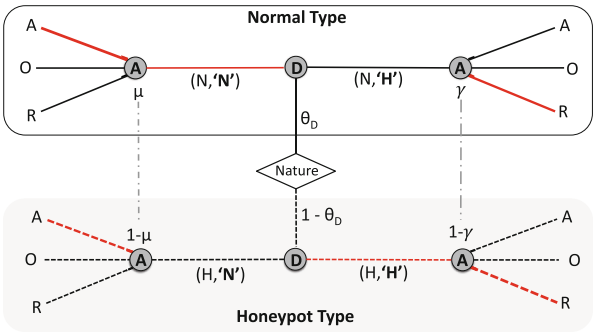


Fig. 4. Perfect Bayesian equilibrium of ('N','H') - (A,R)

With this strategy, the attacker assigns full probability to the normal type defender because only the normal type defender can send signal 'N' in this separating equilibrium setting. Using this posterior probability, the attacker chooses a response among the three options (A, O, R) on the top-left side that yields the highest payoff (by the sequential rationality). In this case, the attacker decides to attack if $c_c - v_a \cdot R_a \geq 0 \Rightarrow R_a \leq \frac{c_c}{v_a}$, and similarly he decides to retreat if $R_a > \frac{c_c}{v_a}$.

We omit comparison of attack (A) with observe (O) option since $c_c > c_w$ by Eq. 2. When the attacker chooses to attack, we mark the corresponding branches for both defender types on the top and bottom left side. Similarly, if the attacker receives 'H', he believes that the signal comes from a honeypot by the posteriori calculation:

$$\gamma = \frac{\theta_D \cdot (1-\alpha^N)}{\theta_D \cdot (1-\alpha^N) + (1-\theta_D) \cdot (1-\alpha^H)} = \frac{\theta_D \cdot 0}{\theta_D \cdot 0 + (1-\theta_D) \cdot 1} = 0$$

In this case, the attacker chooses to retreat (R) with 0 payoff among the three options because A and O have negative values in Fig. 3. Accordingly, the branches are shaded (top and bottom right) for both defender types in Fig. 4.

Once the actions are taken for both players, PBE seeks for any deviations from the players' decisions. In other words, if a player has incentive to change the decision among the shaded branches, we say that PBE does not exist for such a case. We first consider the scenario in which the attacher decides to attack against receiving signal 'N' (shaded branches). The normal type defender compares the utility of signaling 'N' ($v_1 \cdot R_d - c_c$) with signaling 'H' ($v_2 \cdot R_d - c_s$). She does not deviate from the decision as long as:

$$v_1 \cdot R_d - c_c \geq v_2 \cdot R_d - c_s \Rightarrow R_d \geq \frac{c_c - c_s}{(v_1 - v_2)}$$

Similarly, the honeypot type compares the shaded branches and does not deviate if and only if:

$$-v_4 \cdot R_d \geq b_o - v_3 \cdot R_d - cs \Rightarrow R_d \geq \frac{b_o - c_s}{v_3 - v_4}$$

Consequently, this separating equilibrium strategy (the defender plays ('N','H') and the attacker plays (A,R) represents a PBE of this incomplete information game, if and only if:

$$R_d \geq \frac{c_c - c_s}{(v_1 - v_2)}, R_d \geq \frac{b_o - c_s}{v_3 - v_4}, R_a \leq \frac{c_c}{v_a}$$

Now we consider the scenario in which the attacher decides to retreat against receiving signal 'N'. In a similar way, both defender types seek for incentives to deviate from current strategy by comparing the utility of signaling 'N' with that of 'H'. After substituting the payoffs, we conclude that she does not deviate if:

$$R_d \leq \frac{c_s}{(v_2 - v_1)}, R_d \leq \frac{c_s}{v_4 - v_3}, R_a \geq \frac{c_c}{v_a}.$$

For illustration purposes, we show the exhaustive analysis of the strategy in which the defenders signal ('N','H') and the attacker responds by (A,R). All separating equilibria (including the above solution) that satisfy PBE and the corresponding conditions are listed in Table 2.

Table 2. Perfect Bayesian equilibrium for separating equilibria

	(s_1, s_2), (a_1, a_2)	Conditions	μ, γ
E1	('N','H') - (A,R)	$R_d \geq \frac{c_c - c_s}{(v_1 - v_2)}, R_d \geq \frac{b_o - c_s}{v_3 - v_4}, R_a \leq \frac{c_c}{v_a}$	1, 0
E2	('N','H') - (R,R)	$R_d \leq \frac{c_s}{(v_2 - v_1)}, R_d \leq \frac{c_s}{v_4 - v_3}, R_a > \frac{c_c}{v_a}$	1, 0
E3	('H','N') - (A,R)	$R_d > \frac{c_c + c_s}{(v_2 - v_1)}, R_d > \frac{b_o + c_s}{v_4 - v_3}, R_a \leq \frac{c_c}{v_a}$	0, 1
E4	('H','N') - (R,R)	$R_d > \frac{c_s}{(v_2 - v_1)}, R_d > \frac{c_s}{v_4 - v_3}, R_a > \frac{c_c}{v_a}$	0, 1

s_1 and s_2 represent the signals sent by normal type and honeypot defenders. a_1 and a_2 represent attacker's responses against normal type and honeypot defenders.

5.2 Pooling Equilibria

In this section, we provide the steps to find out potential PBEs where both defender types send the same signal. We examine the scenario shaded on the left half of Fig. 5 when both defender types send the signal 'N'. The attacker updates the posterior probability, μ in a similar way for which $\alpha^N = 1$ and $\alpha^H = 1$ based on the definition in Table 1.

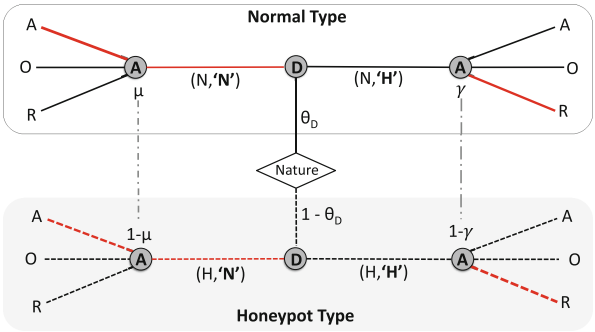


Fig. 5. Perfect Bayesian equilibrium of ('N','N') - (A,R)

$$\mu = \frac{\theta_D \cdot \alpha^N}{\theta_D \cdot \alpha^N + (1-\theta_D) \cdot \alpha^H} = \frac{\theta_D \cdot 1}{\theta_D \cdot 1 + (1-\theta_D) \cdot 1} = \theta_D$$

With this strategy, the attacker cannot distinguish between the defender types, hence the announcements from the defenders are uninformative. In contrast to strategies in separating equilibria, the attacker cannot assign a full probability to a certain type, and must consider the nature's probability (priori) θ_D as a result of the updated μ value. In this scenario, the posteriori coincides with the prior probability which is a common case in pooling equilibria [9].

After μ is updated, the attacker chooses between the actions. He chooses A, if these conditions hold from Fig. 3:

$$\theta_D(c_c - v_a \cdot R_a) + (1-\theta_D)(-v_a \cdot R_a) \geq \theta_D(c_w - v_a \cdot R_o) + (1-\theta_D)(-v_a \cdot R_o)$$

$$\theta_D(c_c - v_a \cdot R_a) + (1-\theta_D)(-v_a \cdot R_a) \geq 0$$

which holds for

$$\theta_D \geq \frac{v_a \cdot (R_a - R_o)}{c_c - c_w} \text{ and } \theta_D \geq \frac{R_a \cdot v_a}{c_c}$$

On the other hand, the attacker decides to observe (O) if:

$$\theta_D < \frac{v_a \cdot (R_a - R_o)}{c_c - c_w} \theta_D \geq \frac{R_o \cdot v_a}{c_w}$$

and finally he decides to retreat (R) if:

$$\theta_D < \frac{R_a \cdot v_a}{c_c} \text{ and } \theta_D < \frac{R_o \cdot v_a}{c_w}$$

Despite the probability of signaling **'H'** is 0 for both defenders, the attacker must still update γ to finish the game:

$$\gamma = \frac{\theta_D \cdot (1-\alpha^N)}{\theta_D \cdot (1-\alpha^N) + (1-\theta_D) \cdot (1-\alpha^H)} = \frac{\theta_D \cdot 0}{\theta_D \cdot 0 + (1-\theta_D) \cdot 0} = \frac{0}{0}$$

which is a special case where γ can have an arbitrary value ($\gamma \in [0, 1]$) because the player is at a state which should not be reached in equilibrium [2]. To handle such cases, we first set restrictions on the range of γ based on the attacker's decisions, then check whether there is a deviation in any of the defenders. For example, let us assume that the attacker chooses to retreat when he receives the signal **'H'** on the right half of Fig. 5. Then, this equations must hold for the retreat option to be optimal:

$$\gamma \cdot 0 + (1-\gamma) \cdot 0 > \gamma(c_c - v_a \cdot R_a) + (1-\gamma)(-v_a \cdot R_a) \Rightarrow \gamma < \frac{v_a \cdot R_a}{c_c}$$

$$\gamma \cdot 0 + (1-\gamma) \cdot 0 > \gamma(c_w - v_a \cdot R_o) + (1-\gamma)(-v_a \cdot R_o) \Rightarrow \gamma < \frac{v_a \cdot R_o}{c_w}$$

After setting the restrictions and assuming that the attacker has chosen to attack against normal type defender (A in the first computation), we check if there is deviation by the defender types by comparing the marked selections in Fig. 5. Then, we can conclude that the PBE can be sustained with this scenario, if these conditions hold:

$$v_1 \cdot R_d - c_c \geq v_2 \cdot R_d - c_s \Rightarrow R_d \geq \frac{c_c - c_s}{v_1 - v_2}$$

$$b_o - v_3 \cdot R_d - c_s \geq -v_4 \cdot R_d \Rightarrow R_d \leq \frac{b_o - c_s}{v_3 - v_4}$$

The remaining pooling equilibrium scenarios that satisfy PBE in the exhaustive analysis are all listed in Table 3 with respective conditions.

6 Results

Using the valuations of players (e.g., cost variables, service rate), we explore the Nash equilibria by finding out steady states where neither player has incentives to deviate from the actions taken. We take all possibilities into account for both defender types (normal and honeypot) and one attacker including the nature's decision, our results in Fig. 6 show that the equilibrium can be at 4 different settings based on the valuation of the players. In particular, when normal defender's service rate is very high compared to the attacker (the square □ and triangle ▽ area), the defender does not anticipate the use of deception because the overhead caused by signaling is more than the damage the attacker may cause. In response, when the attacker's rate is comparable to defender's service rate (triangle ▽ area), he wants to attack in normal type and retreat in honeypot; whereas if the defender's service rate is extremely high (the square □), then the attacker chooses to retreat with certainty. That is, the attacker's utility which takes into account the prior belief (θ_D), the signal (s) and the posterior probability (μ), makes it infeasible to attack. However, in the former case (triangle ▽ area), since the attack rate is relatively close to the defender's

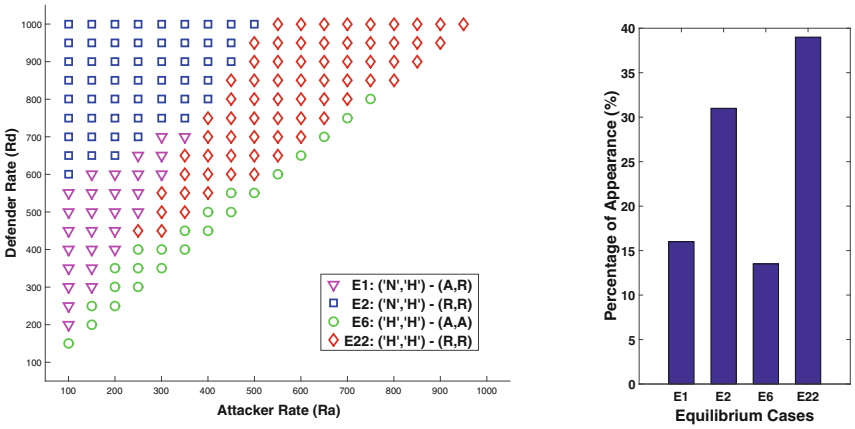
service rate, the attacker finds initiatives to attack in the case where he receives the signal 'N'. In other words, the potential damage he may cause (if the target is normal) is larger than the cost incurred on the attacker (in case he fails to attack a normal server).

In pooling equilibria where defenders with different types all choose the same signal to be sent (the diamond ◊ and circle ◯ area), we see that if the attacker's rate is very close to the defender's service rate (circle ◯ area), the attacker chooses to attack with certainty. If the attack succeeds, the damage to the defender is huge and a permanent unavailability can occur on the server side. However, even if the attacker's rate is high enough in some cases (the diamond ◊), the attacker may prefer retreating because of the likelihood that the defender's

Table 3. Perfect Bayesian equilibrium for pooling equilibria

	(s_1, s_2) - (a_1, a_2)	Conditions	Prior & Posterior*
E5	('N','N') - (A,A)	$\frac{c_s}{v_2 - v_1} \geq R_d \geq \frac{c_s}{v_4 - v_3}$	$\theta_D \geq \frac{v_a \cdot (R_a - R_o)}{c_c - c_w}$, $\theta_D \geq \frac{R_a \cdot v_a}{c_c}$, $\gamma \geq \frac{v_a \cdot (R_a - R_o)}{c_c - c_w}$, $\gamma \geq \frac{v_a \cdot R_a}{c_c}$
E6	('H','H') - (A,A)	$\frac{c_s}{v_4 - v_3} > R_d > \frac{c_s}{v_2 - v_1}$	
E7	('N','N') - (A,O)	$\frac{c_s + c_w - c_c}{v_2 - v_1} \geq R_d \geq \frac{c_s - b_o}{v_4 - v_3}$	$\theta_D \geq \frac{v_a \cdot (R_a - R_o)}{c_c - c_w}$, $\theta_D \geq \frac{R_a \cdot v_a}{c_c}$, $\gamma < \frac{v_a \cdot (R_a - R_o)}{c_c - c_w}$, $\gamma \geq \frac{v_a \cdot R_o}{c_w}$
E8	('H','H') - (A,O)	$\frac{c_s - b_o}{v_4 - v_3} > R_d > \frac{c_s + c_w - c_c}{v_2 - v_1}$	
E9	('N','N') - (A,R)	$\frac{b_o - c_s}{v_3 - v_4} \geq R_d \geq \frac{c_c - c_s}{v_1 - v_2}$	$\theta_D \geq \frac{v_a \cdot (R_a - R_o)}{c_c - c_w}$, $\theta_D \geq \frac{R_a \cdot v_a}{c_c}$, $\gamma < \frac{v_a \cdot R_a}{c_c}$, $\gamma < \frac{v_a \cdot R_o}{c_w}$
E10	('H','H') - (A,R)	$\frac{c_c - c_s}{v_1 - v_2} > R_d > \frac{b_o - c_s}{v_3 - v_4}$	
E11	('N','N') - (O,A)	$\frac{c_s + c_c - c_w}{v_2 - v_1} \geq R_d \geq \frac{c_s + b_o}{v_4 - v_3}$	$\theta_D < \frac{v_a \cdot (R_a - R_o)}{c_c - c_w}$, $\theta_D \geq \frac{R_o \cdot v_a}{c_w}$, $\gamma \geq \frac{v_a \cdot (R_a - R_o)}{c_c - c_w}$, $\gamma \geq \frac{v_a \cdot R_a}{c_c}$
E12	('H','H') - (O,A)	$\frac{c_s + b_o}{v_4 - v_3} > R_d > \frac{c_s + c_c - c_w}{v_2 - v_1}$	
E13	('N','N') - (O,O)	$\frac{c_s}{v_2 - v_1} \geq R_d \geq \frac{c_s}{v_4 - v_3}$	$\theta_D < \frac{v_a \cdot (R_a - R_o)}{c_c - c_w}$, $\theta_D \geq \frac{R_o \cdot v_a}{c_w}$, $\gamma < \frac{v_a \cdot (R_a - R_o)}{c_c - c_w}$, $\gamma \geq \frac{v_a \cdot R_o}{c_w}$
E14	('H','H') - (O,O)	$\frac{c_s}{v_4 - v_3} > R_d > \frac{c_s}{v_2 - v_1}$	
E15	('N','N') - (O,R)	$\frac{c_w}{v_1 - v_2} \geq R_d \geq \frac{c_s}{v_4 - v_3}$	$\theta_D < \frac{v_a \cdot (R_a - R_o)}{c_c - c_w}$, $\theta_D \geq \frac{R_o \cdot v_a}{c_w}$, $\gamma < \frac{v_a \cdot R_a}{c_c}$, $\gamma < \frac{v_a \cdot R_o}{c_w}$
E16	('H','H') - (O,R)	$\frac{c_s}{v_4 - v_3} > R_d > \frac{c_w}{v_1 - v_2}$	
E17	('N','N') - (R,A)	$\frac{c_s + c_c}{v_2 - v_1} \geq R_d \geq \frac{c_s + b_o}{v_4 - v_3}$	$\theta_D < \frac{R_a \cdot v_a}{c_c}$, $\theta_D < \frac{R_o \cdot v_a}{c_w}$, $\gamma \geq \frac{v_a \cdot (R_a - R_o)}{c_c - c_w}$, $\gamma \geq \frac{v_a \cdot R_a}{c_c}$
E18	('H','H') - (R,A)	$\frac{c_s + b_o}{v_4 - v_3} > R_d > \frac{c_s + c_c}{v_2 - v_1}$	
E19	('N','N') - (R,O)	$\frac{c_s + c_w}{v_2 - v_1} \geq R_d \geq \frac{c_s}{v_4 - v_3}$	$\theta_D < \frac{R_a \cdot v_a}{c_c}$, $\theta_D < \frac{R_o \cdot v_a}{c_w}$, $\gamma < \frac{v_a \cdot (R_a - R_o)}{c_c - c_w}$, $\gamma \geq \frac{v_a \cdot R_o}{c_w}$
E20	('H','H') - (R,O)	$\frac{c_s}{v_4 - v_3} > R_d > \frac{c_s + c_w}{v_2 - v_1}$	
E21	('N','N') - (R,R)	$\frac{c_s}{v_2 - v_1} \geq R_d \geq \frac{c_s}{v_4 - v_3}$	$\theta_D < \frac{R_a \cdot v_a}{c_c}$, $\theta_D < \frac{R_o \cdot v_a}{c_w}$, $\gamma < \frac{v_a \cdot R_a}{c_c}$, $\gamma < \frac{v_a \cdot R_o}{c_w}$
E22	('H','H') - (R,R)	$\frac{c_s}{v_4 - v_3} > R_d > \frac{c_s}{v_2 - v_1}$	

s_1 and s_2 represent the signals sent by normal type and honeypot defenders. a_1 and a_2 represent attacker's responses against normal type and honeypot defenders.
* γ becomes μ in the equation when defenders' signals are ('H','H')



(The legend icons consist of normal type and honeypot defenders' strategies ('s1','s2'), and attacker's strategy against each defender type (a1,a2). In circle ◯ deception, the normal type defender signals 'H', the honeypot defender sends message H, and the attacker chooses to attack against both types)

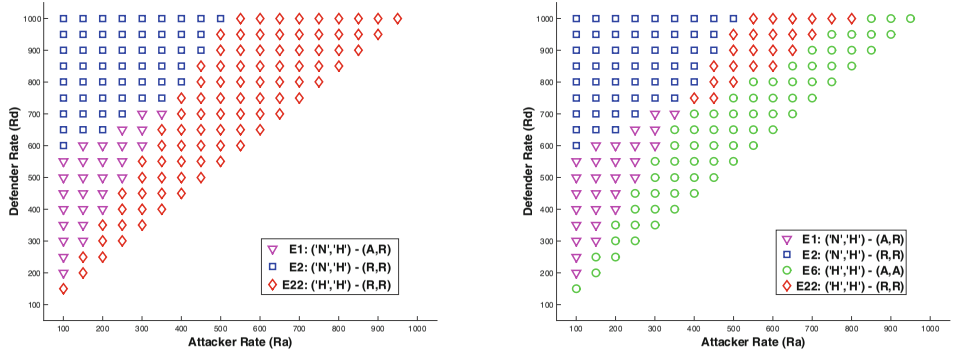
Fig. 6. Nash equilibria by attacker/defender rate & histogram

type is honeypot. In this case, the attacker not only fails to attack and consume his resources but also is observed by the defender. In other words, the defender takes advantage of the confusion caused on the attacker's side by sending the same signals to the attacker.

In Fig. 6, we remove the cases where the attacker's rate exceeds the defender's service rate. Since those cases signify that the attack is already successful and the defender cannot serve her customers, we do not include the equilibrium analysis for the bottom right side of the figure.

Another interesting inference that can be drawn from Fig. 6 is that the defender doesn't anticipate signaling while the attacker's rate is approximately less than 50 % of the defender's rate (the square □ and triangle ▽ area). This result might depend on our game setting and the nature's probability of choosing defender type. Nevertheless, it is of paramount importance to point out that the defender might not need to deploy honeypots if she believes the attacker's rate is below a certain threshold. That is, on the defender side, she can come up with a tolerance rate that the attacker can consume up to without a major degradation on customer satisfaction.

Now that we observe the interaction between the players, we can focus on specific equilibrium cases and examine how they behave under different circumstances. Figure 7a and b show how the equilibria change when we modify the nature's probability of deciding if a system is of a normal type. We pick two extreme cases where $\theta_D = 0.1$ and $\theta_D = 0.9$. In Fig. 7a, since the probability of a system being normal type is very low ($\theta_D = 0.1$), the server that the attacker



(a) $\theta_D = 0.1$ (b) $\theta_D = 0.9$

Fig. 7. Nash equilibria with different θ_D settings

targets is more likely to be a honeypot. Accordingly, we see that the attacker is less likely to choose attacking, and all circles in Fig. 6 (◯) turn into diamonds (◊). Whereas, in Fig. 7b, the circles expand more and constitute a larger area as the likelihood of a system being normal type is set high. The attacker anticipates attacking whichever the signal he receives since the server that he will attack is more likely to be a normal type. In other words, the overall benefit of attacking (despite it can rarely be a honeypot) becomes an always-advantageous option for the attacker, when the nature decides the probability of being a normal server to be high ($\theta_D = 0.9$).

Figure 8 shows how the equilibria change when we vary the signaling cost by the defender rate (keeping $R_a = 500$ constant). The changes in equilibrium points indicate important implications about how the players switch strategies with respect to the parameters. The equilibria line where $R_d = 500$ begins with honeypot defender's deception strategy (plus sign +), but she switches to truthful disclosure (diamond ◊) as the cost of signaling increases. From the attacker's perspective, as we increase the defender's rate (R_d) while keeping the cost of signaling low ($c_s = 0$ or $c_s = 50$), the attacker's choices switch first from fully attacking (A,A) (plus sign +) to (A,R) (square □) and then to (R,R) (cross × or circle ○) because the attacker's degradation incurred on the customer satisfaction becomes relatively smaller. Similarly, after a certain R_d value ($R_d \geq 1000$), the defenders do not involve (do not need) any deceptions since the attacker retreats in both options because of the high defender rate.

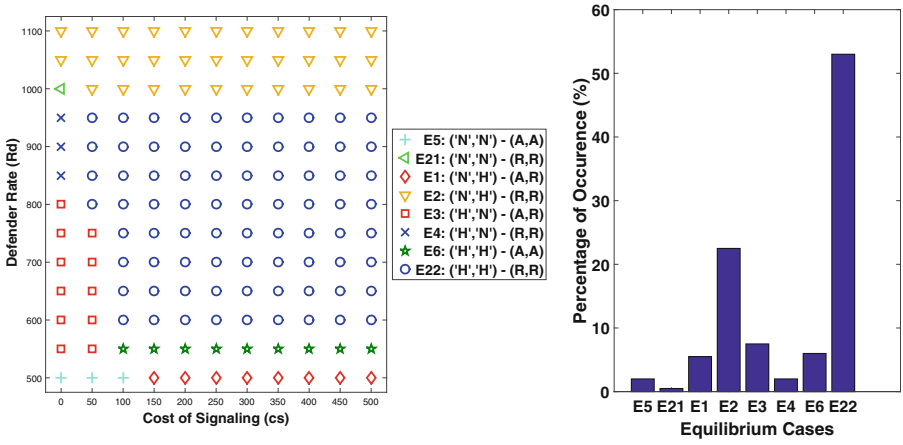


Fig. 8. Nash equilibria by cost of signaling & histogram

When we examine the strategies taken by both players in this work, we see strategy O is never the best response. Since the game is single period and the attacker takes action only once, naturally he never finds *observing* more advantageous than other strategies. In game theory, this fact can be easily proven

by the dominant strategy notion in which for every possible play of strategy O, keeping everything else constant, there is at least one other strategy that yields higher payoff. It can be seen in Fig. 3 that A is always more beneficial than O for normal type defender after substituting the corresponding formulas and constant values. Similarly, strategy R is the dominant strategy for the attacker in response to the honeypot defender type. Therefore, O is a dominated strategy.

7 Discussion

For ease of calculation, the utility functions of the defender and the attacker are kept simple in this study. However, the defender's utility should be based not only on the effect of the attacks but also the satisfaction of the customers she is providing service to. In real systems (Fig. 9), attackers might not be able to drop the entire traffic but only a part of it. Similarly, when the defender blocks certain attackers, she may be preventing some legitimate users from accessing to servers, too. Therefore, it is desirable to come up with an advanced and more capable model which involves the satisfaction rate of customers and the degradation caused by the attackers [22].

In our game, when the defender sends honeypot (H) signal for the normal (N) type, she basically informs the attacker as if the system is slowing down and the attack is successful. However, the system might send the same signal to legitimate users and degrade their experience. Similarly, the defender can send 'N' signal even if the type is H to attract the attacker and have him attack so that the defender can get information about his plans and strategies. This option requires a forwarding mechanism for customers to access that server from Domain Name Server (DNS). Since it is not a real system, the transactions to that server are not turned into real actions, so the defender must be incurred a cost to take the legitimate users to real servers after she makes sure they're not attackers.

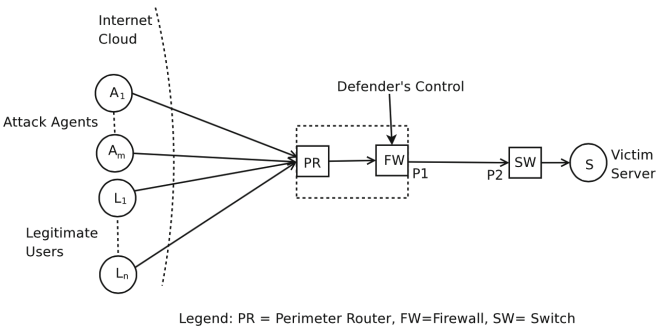


Fig. 9. A generic network topology in DoS attack [27]

Similarly, the constant costs that set in our experiments, e.g., c_s, v_a can be converted into a function that may reflect more realistic effect on the equilibria.

8 Conclusion and Future Work

We propose a new defense framework by proactively using deception as a means to assist in developing effective responses to DoS-type attacks and threats emanating from adversaries who may employ unconventional multi-stage stealth. Furthermore, our methodology can be generalized to be used through a game-theoretic formulation and simulation of any kind of attacks. We use game theory-based approach to gain insights and recommendations so as to increase the probability of surviving advanced and complicated attacks. The framework itself is concrete with quantification of the cost variables and can be generalized to protect critical enterprise systems such as data centers and database servers, and military fault-tolerant mission-critical systems from a persistent adversary.

In this paper, for simplicity, we examine a single target/one period game between an attacker and a defender. Investigation of multiple players (e.g., decentralized attacks by various agents and bots) in multi-period (taking turns) games is of paramount importance to explore the real-life scenarios taking place during a distributed DoS attack. Employing an advanced network configuration and a real-world DoS attack scenario for our model is also left as future work to involve the satisfaction rate of customers and reflect effects of attacks on the defender.

References

1. Agah, A., Das, S.K.: Preventing DoS attacks in wireless sensor networks: a repeated game theory approach. IJ Netw. Secur. **5**(2), 145–153 (2007)
2. Bagwell, K., Ramey, G.: Advertising and pricing to deter or accommodate entry when demand is unknown. Int. J. Indus. Organ. **8**(1), 93–113 (1990)
3. Balas, E.: Know Your Enemy: Learning About Security Threats. Addison Wesley, Boston (2004)
4. Basagiannis, S., Katsaros, P., Pombortsis, A., Alexiou, N.: Probabilistic model checking for the quantification of DoS security threats. Comput. Secur. **28**(6), 450–465 (2009)
5. Bell, J.B., Whaley, B.: Cheating and Deception. Transaction Publishers, Brunswick (1991)
6. Carroll, T.E., Grosu, D.: A game theoretic investigation of deception in network security. Secur. Commun. Netw. **4**, 1162–1172 (2011)
7. Center, C.C.: Results of the distributed-systems intruder tools workshop. Software Engineering Institute (1999)
8. Cohen, F., Koike, D.: Misleading attackers with deception. In: Proceedings from the Fifth Annual IEEE SMC Information Assurance Workshop, pp. 30–37. IEEE (2004)
9. Fong, Y.: Private information of nonpaternalistic altruism: exaggeration and reciprocation of generosity. Adv. Theor. Econ. **9**(1), 1 (2009)
10. Fu, X., Yu, W., Cheng, D., Tan, X., Streff, K., Graham, S.: On recognizing virtual honeypots and countermeasures. In: 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, pp. 211–218. IEEE (2006)
11. Fudenberg, D., Tirole, J.: Perfect Bayesian equilibrium and sequential equilibrium. J. Econ. Theor. **53**(2), 236–260 (1991)

12. Gao, X., Zhu, Y.-F.: DDoS defense mechanism analysis based on signaling game model. In: 2013 5th International Conference on Intelligent Human-Machine Systems and Cybernetics, pp. 414–417 (2013)
13. Hamilton, S.N., Miller, W.L., Ott, A., Saydjari, O.S.: The role of game theory in information warfare. In: 4th Information Survivability Workshop (ISW-2001/2002), Vancouver, Canada (2002)
14. Heitzenrater, C., Taylor, G., Simpson, A.: When the winning move is not to play: games of deterrence in cyber security. In: Khouzani, M.H.R., Panaousis, E., Theodorakopoulos, G. (eds.) Decision and Game Theory for Security, pp. 250–269. Springer, Heidelberg (2015)
15. Jiang, Z., Ge, Y., Li, Y.: Max-utility wireless resource management for best-effort traffic. IEEE Trans. Wirel. Commun. **4**(1), 100–111 (2005)
16. La, Q.D., Quek, T., Lee, J., Jin, S., Zhu, H.: Deceptive attack and defense game in honeypot-enabled networks for the internet of things. IEEE Internet Things J. **PP(99)**, 1 (2016)
17. Lau, F., Rubin, S.H., Smith, M.H., Trajkovic, L.: Distributed denial of service attacks. In: 2000 IEEE International Conference on Systems, Man, and Cybernetics, vol. 3, pp. 2275–2280. IEEE (2000)
18. Lye, K.W., Wing, J.M.: Game strategies in network security. Int. J. Inf. Secur. **4**(1–2), 71–86 (2005)
19. McCarty, B.: The honeynet arms race. IEEE Secur. Priv. **1**(6), 79–82 (2003)
20. Meadows, C.: A cost-based framework for analysis of denial of service in networks. J. Comput. Secur. **9**(1), 143–164 (2001)
21. Píbil, R., Lisý, V., Kiekintveld, C., Bošanský, B., Pěchouček, M.: Game theoretic model of strategic honeypot selection in computer networks. In: Decision and Game Theory for, Security, pp. 201–220 (2012)
22. Rasouli, M., Miehling, E., Teneketzis, D.: A supervisory control approach to dynamic cyber-security. In: Poovendran, R., Saad, W. (eds.) Decision and Game Theory for Security, pp. 99–117. Springer, Heidelberg (2014)
23. Rass, S., Rainer, B.: Numerical computation of multi-goal security strategies. In: Poovendran, R., Saad, W. (eds.) Decision and Game Theory for Security, pp. 118–133. Springer, Heidelberg (2014)
24. Rowe, N.C., Custy, E.J., Duong, B.T.: Defending cyberspace with fake honeypots. J. Comput. **2**(2), 25–36 (2007)
25. Shen, S., Yue, G., Cao, Q., Yu, F.: A survey of game theory in wireless sensor networks security. J. Netw. **6**(3), 521–532 (2011)
26. Wang, W., Chatterjee, M., Kwiat, K.: Coexistence with malicious nodes: a game theoretic approach. In: International Conference on Game Theory for Networks, GameNets 2009, pp. 277–286. IEEE (2009)
27. Wu, Q., Shiva, S., Roy, S., Ellis, C., Datla, V.: On modeling and simulation of game theory-based defense mechanisms against DoS and DDoS attacks. In: Proceedings of the 2010 Spring Simulation Multiconference, p. 159. Society for Computer Simulation International (2010)
28. Yang, L., Mu, D., Cai, X.: Preventing dropping packets attack in sensor networks: a game theory approach. Wuhan Univ. J. Nat. Sci. **13**(5), 631–635 (2008)
29. Zhuang, J., Bier, V.M.: Reasons for secrecy and deception in homeland-security resource allocation. Risk Anal. **30**(12), 1737–1743 (2010)
30. Zhuang, J., Bier, V.M.: Secrecy and deception at equilibrium, with applications to anti-terrorism resource allocation. Defence Peace Econ. **22**(1), 43–61 (2011)
31. Zhuang, J., Bier, V.M., Alagoz, O.: Modeling secrecy and deception in a multiple-period attacker-defender signaling game. Eur. J. Oper. Res. **203**(2), 409–418 (2010)