Research Article

A Novel Attack-and-Defense Signaling Game for Optimal Deceptive Defense Strategy Choice

Yongjin Hu, Han Zhang, Yuanbo Guo, Tao Li, and Jun Ma

1Information Engineering University, Zhengzhou 450001, China
2Zhengzhou University, Zhengzhou 450001, China
3School of Telecommunications Engineering, Xidian University, Xi’an 710071, China

Correspondence should be addressed to Jun Ma; sijunhan@163.com

Received 9 April 2020; Revised 2 June 2020; Accepted 14 September 2020; Published 12 October 2020

Copyright © 2020 Yongjin Hu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Increasingly, more administrators (defenders) are using defense strategies with deception such as honeypots to improve the IoT network security in response to attacks. Using game theory, the signaling game is leveraged to describe the confrontation between attacks and defenses. However, the traditional approach focuses only on the defender; the analysis from the attacker side is ignored. Moreover, insufficient analysis has been conducted on the optimal defense strategy with deception when the model is established with the signaling game. In our work, the signaling game model is extended to a novel two-way signaling game model to describe the game from the perspectives of both the defender and the attacker. First, the improved model is formally defined, and an algorithm is proposed for identifying the refined Bayesian equilibrium. Then, according to the calculated benefits, optimal strategies choice for both the attacker and the defender in the game are analyzed. Last, a simulation is conducted to evaluate the performance of the proposed model and to demonstrate that the defense strategy with deception is optimal for the defender.

1. Introduction

IoT networks and devices are highly vulnerable to sophisticated cyber-attacks. Despite the widespread deployment of security monitoring tools, which include firewalls and intrusion detection systems (IDSs), attackers can infiltrate target IoT devices by leveraging multiple attack vectors [1].

Recently, honeypot-enabled deceptive security mechanisms were introduced as an emerging proactive cyber defense strategy for confusing or misleading attackers and showed significant advantages over traditional security techniques [2]. For attackers, deceptive behaviors of defenders increase the uncertainty of the target to be compromised [3]. Attackers must spend additional resources (e.g., time and money) to deal with the uncertainty via reconnaissance and to develop situational awareness. In addition, deceptive behaviors prevent attackers from launching efficient custom attacks. For example, by collecting an attacker’s information when he is compromising a target device that is disguised by honeypots, the defender can use the learned knowledge to enhance the IoT network security [4]. As a result, deception by providing seemingly convincing yet misleading information to deceive attackers has become a major defense mechanism. With the wide utilization of deception, the security status of organizations has been substantially improved. When attackers are following the seven phases of the cyber kill chain [5] in launching an attack, deception approaches can be performed effectively in disrupting each stage of the cyber kill chain, as illustrated in Figure 1.

The contributions of the paper are the following.

(1) A two-way signaling game model based on the signaling game is formally defined to describe the confrontation from the perspectives of both the defender and the attacker.
(2) With the two-way signaling game model, an algorithm is defined to identify the refined Bayesian equilibrium in the game.
(3) With the deception strategy introduced, the
optimal strategies choice for both the attacker and the defender in the game is analyzed.

2. Related Works

In previous work [6], due to a lack of clarity regarding the concept of deception, deploying honeypots to detect an attacker and to obtain information on the attacker’s intentions is the primary deception mode for the defender to use. For instance, Rowe et al. [7] showed how to decrease the number of attacks to which a network is subjected by utilizing fake honeypots, namely, by disguising normal systems as honeypots. Garg and Grosu [8] used a honeynet system to characterize deception, where defenders may have the choice to conceal a regular host as a honeypot (or inversely) in response to the attackers’ probe. Seamus et al. [9] created a honeypot that simulates a ZigBee gateway to assess the presence of the ZigBee attack intelligence on a SSH attack vector in Wireless Sensor Networks (WSNs).

Until recent years, as deception became a powerful tool for protecting IoT networks and devices against attackers [10], game theory was introduced into the field of cybersecurity to model the interaction between defender and attacker and to identify the optimal defense strategies for both players. Cohen [11] comprehensively discussed deception as a technique for protecting information systems and concluded that deception has a positive effect for the defenders and a negative effect for the attackers. Carroll and Grosu [12] modeled the way deception affects the attack-defense interactions based on a game in which the players (defenders and attackers) have incomplete knowledge of each other. Pawlick and Zhu [13] extended the signaling game by assuming that the adversary can obtain evidence of the true state of the system, and they concluded that the effectiveness of deceptive defenders sometimes increases if an adversary develops the ability to detect deception. Duan et al. [14] proposed an energy-aware trust derivation scheme using the game theoretic approach to manage overhead while maintaining adequate security of WSNs. Fugate and Ferguson [15] discussed techniques for combining artificial intelligence algorithms with game theory models to estimate hidden states of the attacker using feedback through payoffs to learn how to optimally defend the system using cyber deception. Additional works are listed in Table 1.

As discussed above, in contrast to the previous focus on the analysis of the defender, our work will describe the process from not only the perspective of the defender but also that of the attacker.

3. An Improved Signaling Game Model

3.1. Analysis of the Novel Attack–And–Defense Signaling Game

According to [22–24], the information that is released by the defender actively or the information that is leaked via defensive behavior passively is an important decision-making basis for the attacker. Such information is referred to as the signal that is sent by the defender, and the defense signal can affect the behavior of the attacker by changing the benefits to both the attacker and the defender. Furthermore, we believe that the information that is released by the
transmission. By constructing the attack–defense behavior interaction model with incomplete information. According to signaling game theory, we analyze the dynamic game process and the signal mechanism from the perspectives of both attack and defense, and we investigate the influence of defense signals on the game equilibrium and strategy choice for both the attacker and the defender. We describe this process as a novel attack–defense signaling game that is defined as a two-way signaling game model, as illustrated in Figure 2.

The defender is defined as the leader of the signaling game, and the attacker is the follower when analyzing the forward signal transmission. The roles of the attacker and the defender will be exchanged when analyzing the reverse signal transmission. By constructing the attack–defense game process in both the forward and reverse directions, the influencing factors for both the attacker and the defender will also affect the defense decision and change the final attack-and-defense benefits. We construct an attack-and-defense behavior interaction model with incomplete information. According to signaling game theory, we analyze the dynamic game process and the signal mechanism from the perspectives of both attack and defense, and we investigate the influence of defense signals on the game equilibrium and strategy choice for both the attacker and the defender. We describe this process as a novel attack-and-defense signaling game that is defined as a two-way signaling game model, as illustrated in Figure 2.

The defender is defined as the leader of the signaling game, and the attacker is the follower when analyzing the forward signal transmission. The roles of the attacker and the defender will be exchanged when analyzing the reverse signal transmission. By constructing the attack–defense game process in both the forward and reverse directions, the influences of two examples on the defense strategy are analyzed: (1) in the forward phase, the defender sends a signal $m_d$ to the attacker, who will infer the type of the defender $\theta$ and choose the action $a$; the reverse direction is defined as the attacker sending a signal $m_a$ to the defender, who will infer the type $\eta$ of the attacker and choose the action $d$.

| Author                     | Focus of the study                                                                 |
|----------------------------|-----------------------------------------------------------------------------------|
| Çeker et al. [16]          | Modeled with a similar approach that uses game theory and provides the option of disguising a real system as a honeypot (or vice versa) to mitigate denial of service (DoS) attacks |
| Hichem et al. [17]         | Proposed a game theoretic technique to activate anomaly detection technique only when a new attack’s signature is expected to occur |
| Aaron et al. [18]          | To increase the uncertainty of adversarial reconnaissance and introduce a novel game theoretic model of deceptive interactions between a defender and a cyber-attacker into responses to network scans or reconnaissance |
| Somdip [19]               | Proposed a methodology in which game theory can be used to model the activity of stakeholders in the networks to detect anomalies such as collusion by using a supervised machine learning algorithm and algorithmic game theory |
| Pawlick and Zhu [20]       | Investigated a model of signaling games in which the receiver can detect deception with a specified probability |
| Kun et al. [21]            | Employed Nash equilibrium in the noncooperative game model and analyzes its efficiency in vehicular ad hoc networks |

**Figure 2:** In a two-way signaling game model, the forward direction is defined as the defender sending a signal $m_d$ to the attacker, who will infer the type of the defender $\theta$ and choose the action $a$; the reverse direction is defined as the attacker sending a signal $m_a$ to the defender, who will infer the type $\eta$ of the attacker and choose the action $d$.

**Table 1:** Research on modeling deception defense by game theory.

| Game Model | Description |
|------------|-------------|
| GD         | Two-way signaling game model for defense strategy selection with deception |

**Definition 1.** The two-way signaling game model for defense strategy selection with deception $G_{DS}$ can be represented by a nine-tuple $G_{DS} = (N, \Theta, M, S, P_A, P_A', P_D, P_D', U)$, in which:

- $N = (N_D, N_A)$ denotes the player set for a two-play game, where $N_D$ denotes the set for the defender and $N_A$ for the attack.
- $\Theta = (\Theta_D, \Theta_A)$ denotes the type set for the defender and the attacker.
- The type of defender $\Theta_D = (\theta_i | i = 1, 2, \cdots, n)$
The type of defender, where, signal name is consistent with the defender type name. The set signal release mechanism. For ease of representation, the defender selects and releases the signal according to the action that is taken.

\( M = (M_D, M_A) \) denotes the signal set for the defender and the attacker. \( M_D = \{ m_d | d = 1, 2, \cdots \} \) denotes the defender selects and releases the signal according to the signal set release mechanism. For ease of representation, the signal name is consistent with the defender type name. The type of attacker \( \Theta_A = \{ \eta_j | j = 1, 2, \cdots n \} \) is the private information of the attacker, which is determined by the attack action that is taken.

\( S = (D, A) \) denotes the strategy set for the defender and the attacker, where \( D = \{ a_g | g = 1, 2, \cdots \} \) and \( A = \{ a_h | h = 1, 2, \cdots \} \) denote the defense strategy and the attack strategy, respectively.

\( P_A \) is the belief set of the attacker on the type of defender, where \( P_A = (p_A(\eta_1), p_A(\eta_2), \cdots, p_A(\eta_n)) = (\gamma_1, \cdots, \gamma_n) \).

\( P_A' \) is the posterior probability set of the attacker on the type of defender, where, \( P_A' = P_A'(\eta_j | m_d) = (\mu_1, \cdots, \mu_n) \) denotes the posterior probability of the type of defender, which follows the Bayesian rule, after the attacker observes the defensive signal \( m_d \).

\( P_D \) is the belief set of the defender on the type of attacker, where \( P_D = (p_D(\eta_1), p_D(\eta_2), \cdots, p_D(\eta_n)) = (\sigma_1, \cdots, \sigma_n) \).

\( P_D' \) is the posterior probability set of the defender on the type of attacker, where \( P_D' = P_D'(\eta_j | m_d) = (\delta_1, \cdots, \delta_n) \) denotes the posterior probability of the type of attacker, which follows the Bayesian rule, after the defender observes the defensive signal \( m_d \).

\( U = (U_D, U_A) \) denotes the expected utility set of the defender and the attacker, whose value is determined by the strategies that are chosen by all players. The corresponding utility functions will be discussed in the next section.

3.3. Refined Bayesian Equilibrium Solution and the Optimal Defense Strategy Choice. According to Definition 1, this section extends the refined Bayesian equilibrium to the two-way signaling game model based on the definition of the refined Bayesian equilibrium [25] and proposes a refined Bayesian equilibrium algorithm for the two-way signaling game. Instances in the forward direction and in the reverse direction for the two-way signaling game model were constructed to show the details.

Definition 2. The equilibrium in a two-way signaling game model for defense strategy choice with deception is a refined Bayesian equilibrium if the following requirements are satisfied:

(I) \( a^*(m) \in \arg\max_{a} \sum_{m, \eta} P_A'(\eta | m) U_2(m, a, \eta) \).

(II) \( m^*(\eta) \in \arg\max_{m} U_1(m, a^*(m), \eta) \).

In (I), \( a^*(m) \) denotes the optimal action that is adopted by the signal receiver after obtaining the posterior probability \( P'(\eta | m) \) of the type to which the signal sender belongs; \( U_2 \)
(m, a, θ) denotes the utility function of the signal receiver, which is the expected utility function of attacker \(U_d(m_j, d_j, a_0, \theta_j)\) in the forward direction and the expected utility function of the defender \(U_p(m_j, d_j, a_0, \theta_j)\) in the reverse direction; and \(\theta \in \Theta = (\Theta_d, \Theta_A)\) denotes the type set for the defender and the attacker, where \(\theta \in \Theta_d = (\theta_j | j = 1, 2, \cdots n)\) in the forward direction and \(\theta \in \Theta_A = (\eta_j | j = 1, 2, \cdots n)\) in the reverse direction.

In (II), \(m^*(\theta)\) denotes the optimal strategy that is selected by the signal sender after predicting the optimal action \(a^*(m)\) of the signal receiver; \(U_j(m, a^*(m), \theta)\) denotes the utility function of the signal sender, which is \(U_d(m_j, d_j, a_0, \theta_j)\) in the forward direction, and \(U_p(m_j, d_j, a_0, \theta_j)\) in the reverse direction.

In (III), \(P'_i(\theta | m)\) indicates the posterior probability calculated by signal receiver according to the signal sent by the signal sender followed by the Bayesian rule, which is \(P_A^\ast\) in the forward direction and \(P_B^\ast\) in the reverse direction.

### 3.4. Method of Refined Bayesian Equilibrium in the Two-Way Signaling Game Model

The steps are as follows:

1. Construct the posterior inference \(P(\theta | m)\) of various information sets on the signaling game tree

2. Calculate the optimal strategy for the signal receiver according to the posterior inference

When observing the signal \(m \in M\), the signal receiver will choose optimal strategy \(a^*(m)\) according to \(P(\theta | m)\) for the type \(\theta\) of the sender to maximize the expected utility \(U_2\), namely, the signal receiver will identify his optimal strategy \(a^*(m)\) by calculating \(\max P(\theta | m)U_2(m(\theta), a, \theta)\).

3. Calculate the optimal strategy for the signal sender according to the posterior inference

The signal sender foresees that the signal receiver will select the optimal strategy based on observations of the signal that is released by him and chooses the strategy that maximizes the expected utility \(U_1\), namely, the signal sender identifies his optimal strategy \(m^*(\theta)\) based on the posterior inference by calculating \(\max U_1(m, a^*(m), \theta)\).

4. Calculate the refined Bayesian equilibrium

---

**Algorithm 1: Optimal strategy choice algorithm description based on a two-way signaling game model**

Input: Model \(G_{DS}\), Signal direction parameter \(w\)

Output: Optimal strategy for the defender

BEGIN

if \((w = 1)\) // forward-direction signalling game

\[\begin{align*}
&\text{// Initialize } (\theta \in \Theta_d = (\theta_j | j = 1, 2, \cdots n)) \\
&\text{// Initialize the type of the defender} \\
&\text{Initialize } (M_d = m_d | d = 1, 2, \cdots), P = P_A(\theta_1, \cdots, \theta_n))); \\
&\text{// Initialize the signal of the defender and the belief of the defender regarding the attacker} \\
&\end{align*}\]

\} if \((w = 0)\) // reverse-direction signalling game

\(\begin{align*}
&\text{// Initialize } (\theta \in \Theta_A = (\eta_j | j = 1, 2, \cdots n)) \\
&\text{// Initialize the type of the attacker} \\
&\text{Initialize } (M_A = m_A | a = 1, 2, \cdots) \\
&\text{Initialize } \left(P_B = \{p_{B_1}(\eta_1), p_{B_2}(\eta_2), \cdots, p_{B_n}(\eta_n)\}\right); \\
&\text{// Initialize the signal of the attacker and the belief of the attacker regarding the defender} \\
&\end{align*}\]

\} Initialize \((S = (D, A), D = \{d_1, \cdots, d_s\}, A = \{a_1, \cdots, a_s\})\); \n
// Initialize the strategies for both players

\(\begin{align*}
&\text{while } (a_0 \in A & \& m_j \in M & \& d \in D) \\
&\text{// Calculate the utility} \\
&\text{\(U_A(m_j, d_j, a_0, \theta) = \sum_{a_0} C_a(d_j, a_0) - C_{a_0}\);} \\
&\text{\(U_D(m_j, d_j, a_0, \theta) = \sum_{a_0} C_a(d_j, a_0) - C_{a_0} - C_{d_j}\);} \\
&\end{align*}\]

// Obtain the refined Bayesian Equilibrium

\(\begin{align*}
&\text{\(a^*(m) = \arg \max_{a \in A} \sum_{m \in M} P'_i(\theta | m) U_A(m^*(\theta), a, \theta);\)} \\
&\text{\(m^*(\theta) = \arg \max_{m \in M} U_D(m, a^*(m), d^*(m^*), \theta);\)} \\
&\end{align*}\]

// Calculate the optimal strategy for attack and defence

\(\text{Bayesian } (P'_i(\theta));\)

// Calculate the posterior probability and apply the Bayesian rule for the defender

\(\text{Create } (m^*(\theta), a^*(m), P'_i(\theta)); \text{// Construct the refined Bayesian equilibrium} \)

\(\text{Sort } (m^*(\theta)) \text{ by descending};\)

\(\text{Output } (m^*(\theta)); \text{// output the optimal strategy for the defender} \)

End
is

3.5. Refined Bayesian Equilibrium Solution Method for the Forward Signaling Game. A game of incomplete information can be transformed into a game of imperfect information by adding a hypothetical player, namely, nature (denoted by $C$ here), and by conditioning the payoffs on Nature’s unknown moves. The nature player moves first by randomly choosing the defender type with the prior probability distribution over all defender types. In the forward direction, nature assigns type $\theta_N$ with probability $p_D(\theta_N)$ and type $\theta_H$ with $p_D(\theta_H)$. Once the defender has learned her type, she decides what signal or message to send to the attacker. The signal provides indirect information for the attacker about the defender type. In our example, the defender can send either signal $m_N$ (signaling that the defender type is $\theta_N$) or $m_H$ (signaling that the defender type is $\theta_H$). The defender can send signal $m_N$, even in the case that her real type is $\theta_N$, or send signal $m_H$, even in the case that her real type is $\theta_H$. The attacker revises his judgement on the defender type and takes action $\{O^*_N, O^*_H\}$ if observing signal $m_N$, and action $\{W^*_N, W^*_H\}$ if observing the signal $m_H$, as the posterior probability for the defender type $\{\theta_N, \theta_H\}$. In the game tree, $a_i$ indicates eight outcomes, which results in a corresponding payoff. The forward signaling game tree $G_{DS}(F)$ is presented in Figure 3.

3.6. Refined Bayesian Equilibrium Solution Method for the Reverse Signaling Game. Nature moves first by randomly choosing the attacker type with the prior probability distribution over the attacker types. The reverse signaling game tree $G_{DS}(R)$ is presented in detail in Figure 4.

![Game scenario with deception](Image)

**Figure 5:** Game scenario with deception, which considers two decision makers, namely, a defender and an attacker. The defender deploys a honeypot in the IoT network as either a system or a service host. In the specified scenario, the forward and reverse transmissions occur simultaneously. The sequences of moves, type sets, and action sets follow the modeling elements that were discussed in the previous section. The incomplete information comes from the attacker’s uncertainty regarding the type of the system.
According to the definition, \( m^* = m_a^*(a^*, \eta) = m_a^*(\eta) \) indicates that attacker \( \eta \) sends signal \( m_a^* \) and chooses strategy \( a^*(m_a^*) \) according to the signal, which is denoted as \( m_a^*(\eta) \); \( a^* = a^*(d_g, m_a) \) indicates the defender’s responding action \( a^*(d_g, m_a) \), which is denoted as \( a^*(m_a) \); \( P' = P'_{D|f}(m_a) \) indicates that the defender calculated \( P'_{D|f}(\eta | m_a) \) as the posterior probability for the attacker type, which is denoted as \( P'_{D|f} \) and the existence of a refined Bayesian equilibrium is denoted as \( EQ = (m_a^*(\eta), a^*(m_a), P'_{D|f}) \). Based on the two examples above and the algorithm in [26], the optimal strategy selection algorithm for the two-way signaling game model is presented as Algorithm 1.

### 4. Simulation Results and Analysis

#### 4.1. Simulation Environment

To evaluate the proposed attack-and-defense signaling game model and the algorithm for optimal strategy selection, we construct the simulation environment illustrated in Figure 5.

#### 4.2. Calculating the Utility

According to Richard [27], common vulnerability [28] and the database of attack-and-defense behaviors from MIT [29], attack strategies that are composed of basic options are described in Table 2.

Common defense strategies with deception that are composed of basic operations are described in Table 3.

For selecting the optimal strategy more scientifically and intuitively, the most basic approach is to quantify the utilities of the strategies that are selected by the defender and the attacker. In this paper, we utilize the scheme that was proposed by Zhang and Li [30] to calculate the expected utility functions of the defenders and the attackers as follows:

\[
U_A(m_j, d_g, a_h, \theta) = \sum_{g, h} C_{i_c}(d_g, a_h) - C_a, \tag{1}
\]

\[
U_D(m_j, d_g, a_h, \theta) = \sum_{g, h} C_{i_c}(d_g, a_h) - C_d - C_{i_d}. \tag{2}
\]

The notations that are used in equations (1) and (2) are described in Table 4.

For the defender type \( \{ \theta_{N_L}, \theta_{H_L} \} \), the defense strategy is assumed to be \( D_1 \{ d_1, d_2 \} \) or \( D_2 \{ d_2, d_6 \} \), and for the attacker type \( \{ \eta_{H}, \eta_L \} \), the attack strategy is \( A_1 = \{ a_1, a_2 \} \) or \( A_2 = \{ a_1, a_2 \} \). Based on historical data and experience, \( C_a = \{ C_A, C_{A_1} \} = \{ 590, 320 \} \), \( C_d = \{ C_D, C_{D_1} \} = \{ 360, 285 \} \), and \( C_{i_d} = \{ C_{i_d}, C_{i_d_1} \} = \{ 20, 10 \} \).

![Figure 6: Forward signaling game tree with the calculated utilities.](image)

![Figure 7: Reverse signaling game tree with the calculated utilities.](image)
Table 5: Possible equilibria in the forward direction.

| Condition           | Equilibrium | Type of equilibrium |
|---------------------|-------------|---------------------|
| $O^N > P^A(\theta_N \mid m_A)$, $W^N > P^A(\theta_H \mid m_H)$ | $EQ = [(m_H, m_H) \to (A_1, A_1), O^N = 0.7, W^H = 0.5]$ | Pooling equilibrium |
| $O^N > P^A(\theta_N \mid m_A)$, $W^N < P^A(\theta_H \mid m_H)$ | $EQ = [(m_H, m_H) \to (A_1, A_2), O^N = 0.7, W^H = 0.5]$ | Pooling equilibrium |
| $O^N < P^A(\theta_N \mid m_A)$, $W^N > P^A(\theta_H \mid m_H)$ | $EQ = [(m_H, m_N) \to (A_2, A_1), O^N = 1, W^H = 0]$ | Separating equilibrium |
| $O^N < P^A(\theta_N \mid m_A)$, $W^N < P^A(\theta_H \mid m_H)$ | $EQ = [(m_N, m_N) \to (A_2, A_2), O^N = 0.7, W^H = 0.5]$ | Separating equilibrium |

Table 6: Possible equilibria in the reverse direction.

| Condition           | Equilibrium | Type of equilibrium |
|---------------------|-------------|---------------------|
| $S^N_H > P^A_D(\eta_N \mid m_A), D^N_H > P^A_D(\eta_H \mid m_P)$ | $EQ = [(m_A, m_A) \to (D_1, D_1), S^N_H = 0.4, D^N_H = 0.7]$ | Pooling equilibrium |
| $S^N_H > P^A_D(\eta_N \mid m_A), D^N_H < P^A_D(\eta_H \mid m_P)$ | $EQ = [(m_A, m_A) \to (D_1, D_2), S^N_H = 0.4, D^N_H = 0.7]$ | Pooling equilibrium |
| $S^N_H < P^A_D(\eta_N \mid m_A), D^N_H > P^A_D(\eta_H \mid m_P)$ | $EQ = [(m_A, m_P) \to (D_2, D_1), S^N_H = 0, D^N_H = 1]$ | Separating equilibrium |
| $S^N_H < P^A_D(\eta_N \mid m_A), D^N_H < P^A_D(\eta_H \mid m_P)$ | $EQ = [(m_P, m_P) \to (D_2, D_2), S^N_H = 0.4, D^N_H = 0.7]$ | Pooling equilibrium |

Table 7: Comparison of approaches in terms of static or dynamic type, complete information or incomplete information, and signal direction.

| Author            | Type of game       | Number of players | Signal direction |
|-------------------|--------------------|-------------------|------------------|
| Wang et al. [31]  | Complete information static | $N$              | Single           |
| Lin et al. [32]   | Incomplete information static | $3$              | Single           |
| Zhang et al. [33] | Incomplete information dynamic | $3$              | Single           |
| Zhu et al. [34]   | Incomplete information dynamic | $N$              | Single           |
| Our work          | Incomplete information dynamic | $N$              | Two-way          |

To calculate the utility of the forward-direction signaling game, we set

$$p_D(\theta_N) = 0.6,$$
$$p_D(\theta_H) = 0.4,$$
$$O^N + O^P = 1,$$
$$W^P + W^H = 1. \quad (3)$$

All the utilities that are specified in Figures 6 and 7 were calculated via equations (1) and (2).

The posterior inferences can be constructed on various sets of information. Via Algorithm 1, we obtain possible equilibria in the forward direction, as presented in Table 5.

To calculate the utility of the reverse-direction signaling game, we set $p_A(\eta_H) = 0.4$, $p_A(\eta_L) = 0.6$, $S^N_H + S^N_L = 1$, and $D^N_H + D^N_L = 1$.

The posterior inferences that can be constructed on the two sets of information are $P^A_D(\eta_H \mid m_A) = 0.46$ and $P^A_D(\eta_L \mid m_P) = 0.65$. Via Algorithm 1, we obtain the possible equilibria in the reverse direction, which are presented in Table 6.

The algorithm proposed, and the game simulated in the paper is compared with other approaches in Table 7. We have analyzed both directions of signal transmission in a dynamic incomplete information game, which is more in line with the actual attack-and-defense scenario, and the results can guide the defense decision much more precisely.

4.3. Result Analysis. By implementing the simulation above, we obtain the following results:

1. In the forward-signaling game model, if $(P^A_D(\theta_N \mid m_A), P^A_D(\theta_H \mid m_P))$ and $(S^N_H, D^N_H)$ do not conflict, the refined Bayesian equilibrium is a pooling equilibrium. Hence, the defender chooses a honey system and releases the honey system signal, which deceives the attacker, thereby influencing the attacker's judgement on the defender type and on the choice of attack strategy. Thus, the defender uses the signal to demonstrate a capability that exceeds the actual capability, thereby reducing the likelihood of suffering a loss.

2. In the reverse-signaling game model, the attacker moves first. He can be of type $\eta_H$ and send signal $m_A$ (presenting himself as an advanced attacker) or $m_P$ (pretending to be the primary attacker). He can also be of type $\eta_L$ and send the signal $m_P$ (presenting himself as the primary attacker) or $m_A$ (pretending to be an advanced attacker). According to Table 6, the refined Bayesian equilibrium is realized when the advanced attacker pretends to be the primary attacker and the defender chooses strategy $D_1$ with the deception technique. The advanced attacker...
(3) From the perspective of utility for both the defender and the attacker in a two-way signaling game, regardless of whether the attacker’s ability is low or high, the choice of the deception defense strategy would increase the payoff of the defender compared with the normal system without deception. The defense strategy with deception is the optimal strategy for the defender. Therefore, the defender would choose the deceptive strategy, namely, the normal system would be disguised as a honeypot.

5. Conclusions

We model the confrontation between a defender and an attacker by utilizing signaling game theory. Additionally, we propose the concept of a two-way signaling game and propose an algorithm for identifying optimal defense strategies. Finally, we conduct an extensive simulation analysis to evaluate the performance of the proposed approaches by fortifying the attack-and-defense confrontation in a two-way signal releasing mechanism and calculating the utilities for both sides.

This paper mainly proposes a proactive defense mechanism that utilizes signal selection and release methods and does not consider other defense mechanisms. There are several limitations in our methods, one is that the expected utility functions used in equations (1) and (2) could not be extended to multistage games, and another is that the example shown in the simulation part did not consider the synchronous affect between the attacker and the defender during the game, both of which will be studied in the future work. However, the proposed two-way signaling game model is of substantial importance for subsequent research in the IoT network security. For example, with the method proposed, the defender of the IoT network could infer the optimal strategy of the attacker and take action such as improving the protection level in advance to defense attacks. In the future, we will integrate the analysis via mathematical description, implement the attack-and-defense model for multiple stage games, and explore the security defense decision-making method in IoT networks.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (grant no. 61602515).

References

[1] M. A. Khan and K. Salah, “IoT security: review, blockchain solutions, and open challenges,” Future Generation Computer Systems, vol. 82, pp. 395–411, 2018.
[2] Y. M. P. Pa, S. Suzuki, K. Yoshioka, and T. Matsumoto, “IoTPOT: analysing the rise of IoT compromises,” in 9th USENIX Workshop on Offensive Technologies (WOOT 15), pp. 9–10, Washington, D.C, 2015.
[3] M. H. Almeshkah and E. H. Spafford, Cyber security deception, Springer International Publishing, 2016.
[4] Y. M. P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rosso, “IoTPOT: a novel honeypot for revealing current IoT threats,” Journal of Information Processing, vol. 24, no. 3, pp. 522–533, 2016.
[5] G. Briskin, D. Fayette, N. Evancich, V. Rajabian-Schwart, A. Macera, and J. Li, “Design considerations for building cyber deception systems,” in Cyber Deception, S. Jajodia, V. Subrahmanian, V. Swarup, and C. Wang, Eds., pp. 69–95, Springer, Cham, 2016.
[6] L. Y. Shi, J. N. Zhao, Q. Li, W. Xiao, and L. Xin, “Signaling game analysis and simulation on network decoy defense strategies,” Journal of System Simulation, vol. 28, no. 2, pp. 348–353, 2016.
[7] N. C. Rowe, E. J. Custy, and B. T. Duong, “Defending cyberspace with fake honeypots,” Journal of Computers, vol. 2, no. 2, pp. 25–36, 2007.
[8] N. Garg and D. Grosu, “Deception in honeynets: a game-theoretic analysis,” in 2007 IEEE SMC Information Assurance and Security Workshop, pp. 107–113, West Point, NY, USA, 2007.
[9] S. Dowling, M. Schukat, and H. Melvin, “A ZigBee honeypot to assess IoT cyberattack behaviour,” in 2017 28th Irish Signals and Systems Conference (ISSC), pp. 1–6, Killarney, Ireland, 2017.
[10] H. Šemić and S. Mrdović, “IoT honeypot: a multi-component solution for handling manual and Mirai-based attacks,” in 2017 25th Telecommunication Forum (TELFOR), pp. 1–4, Belgrade, Serbia, 2017.
[11] F. Cohen, “A note on the role of deception in information protection,” Computers and Security, vol. 17, no. 6, pp. 483–506, 1998.
[12] T. E. Carroll and D. Grosu, “A game theoretic investigation of deception in network security,” Security and Communication Networks, vol. 4, no. 10, pp. 1162–1172, 2011.
[13] J. Pawlick and Q. Zhu, “Deception by design: evidence-based signaling games for network defense,” 2015, https://arxiv.org/abs/1503.05458.
[14] J. Duan, D. Gao, D. Yang, C. H. Foh, and H. H. Chen, “An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications,” IEEE Internet of Things Journal, vol. 1, no. 1, pp. 58–69, 2014.
[15] S. Fugate and K. Ferguson-Walter, “Artificial intelligence and game theory models for defending critical networks with cyber deception,” AI Magazine, vol. 40, no. 1, pp. 49–62, 2019.
[16] H. Çeker, J. Zhuang, S. Upadhyaya, Q. D. Ia, and B. H. Soong, “Deception-Based Game Theoretical Approach to Mitigate DoS Attacks,” in Decision and Game Theory for Security. GameSec 2016, Q. Zhu, T. Alpcan, E. Panaousis, M. Tambe, and W. Casey, Eds., vol. 9996 of Lecture Notes in Computer Science, Springer, Cham, 2016.

[17] H. Sedjelmaci, S. M. Senouci, and T. Taleb, “An accurate security game for low-resource IoT devices,” IEEE Transactions on Vehicular Technology, vol. 66, no. 10, pp. 9381–9393, 2017.

[18] A. Schlenker, O. Thakoor, H. Xu et al., “Deceiving cyber adversaries: a game theoretic approach,” in The 17th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2018), vol. 9996, pp. 18–38, Stockholm, Sweden, 2016.

[19] S. Dey, “Securing majority attack in blockchain using machine learning and algorithmic game theory: a proof of work,” in 2018 10th Computer Science and Electronic Engineering (CCEC), pp. 7–10, Colchester, UK, 2018.

[20] J. Pawlick and Q. Y. Zhu, “Quantitative models of imperfect deception in network security using signaling games with evidence [IEEE CNS 17 Poster],” in 2017 IEEE Conference on Communications and Network Security (CNS), pp. 394–395, Las Vegas, NV, USA, 2017.

[21] K. Hua, X. Liu, Z. Chen, and M. Liu, “A Game Theory Based Approach for Power Efficient Vehicular Ad Hoc Networks,” Wireless Communications and Mobile Computing, vol. 2017, 9 pages, 2017.

[22] J. M. Huang and H. W. Zhang, “A method for selecting defense strategies based on stochastic evolutionary game model,” Acta Electronica Sinica, vol. 46, no. 9, pp. 2222–2228, 2018.

[23] X. Chen, A. Li, X. Zeng, W. Guo, and G. Huang, “Runtime model based approach to IoT application development,” Frontiers of Computer Science, vol. 9, no. 4, pp. 540–553, 2015.

[24] S. Shen, L. Huang, H. Zhou, S. Yu, E. Fan, and Q. Cao, “Multistage signaling game-based optimal detection strategies for suppressing malware diffusion in fog-cloud-based IoT networks,” IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1043–1054, 2018.

[25] W. Y. Zhang, Game Theory and Information Economics, Shanghai People’s Publishing House, 2004.

[26] W. Guo, J. Chen, G. Chen, and H. F. Zheng, “Trust dynamic task allocation algorithm with Nash equilibrium for heterogeneous wireless sensor network,” Security and Communication Networks, vol. 8, no. 10, pp. 1865–1877, 2015.

[27] R. Lippmann, J. W. Haines, D. J. Fried, J. Korba, and K. Das, “Analysis and Results of the 1999 DARPA Off-Line Intrusion Detection Evaluation,” in Recent Advances in Intrusion Detection. RAID 2000, H. Debar, L. Mé, and S. F. Wu, Eds., vol. 1907 of Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 2000.

[28] A. Feutrill, D. Ranathunga, Y. Yarom, and M. Roughan, “The effect of common vulnerability scoring system metrics on vulnerability exploit delay,” in 2018 Sixth International Symposium on Computing and Networking (CANDAR), pp. 1–10, Takayama, Japan, 2018.

[29] L. Gordon, M. Loeb, W. Lucyshyn, and R. Richardson, “2005 CSI/FBI computer crime and security survey,” Computer Security Journal, vol. 21, no. 3, 2005.

[30] H. W. Zhang and T. Li, “Optimal active defense based on multi-stage attack-defense signaling game,” Acta Electronica Sinica, vol. 45, no. 2, pp. 431–439, 2017.