Honeypot game-theoretical model for defending against APT attacks with limited resources in cyber-physical systems

Article *in* Etri Journal · September 2019

DOI: 10.4218/etrij.2019-0152

Xiao-Peng Ji
Nanjing University of Information Science & Technology
49 PUBLICATIONS **254** CITATIONS
SEE PROFILE

Weiwei Liu
Nanjing University of Science and Technology
42 PUBLICATIONS **410** CITATIONS
SEE PROFILE

Jiangtao Zhai
Jiangsu University of Science and Technology
35 PUBLICATIONS **285** CITATIONS
SEE PROFILE

Guangjie Liu
Nanjing University of Science and Technology
119 PUBLICATIONS **1,385** CITATIONS
SEE PROFILE

Received: 1 April 2019 | Revised: 9 July 2019 | Accepted: 29 July 2019

DOI: 10.4218/etrij.2019-0152

SPECIAL ISSUE

ETRI Journal WILEY

Honeypot game-theoretical model for defending against APT attacks with limited resources in cyber-physical systems

Wen Tian[1] | Xiao-Peng Ji[1] | Weiwei Liu[1] | Jiangtao Zhai[2] | Guangjie Liu[1] | Yuewei Dai[2] | Shuhua Huang[1]

[1]School of Automation, Nanjing University of Science and Technology, Nanjing, China

[2]School of Electrics and Information Engineering, Jiangsu University of Science and Technology, Zhenjiang, China

Correspondence
Xiao-Peng Ji, School of Automation, Nanjing University of Science and Technology, Nanjing, China
Email: jixiaopeng_nj@163.com

Funding information
Fundamental Research Funds for the Central Universities, Grant/Award Number: 30918012204; Natural Science Foundation of Jiangsu Province, Grant/Award Number: BK20160840; National Natural Science Foundation of China, Grant/Award Number: 61602247, 61702235, U1636117 and U1836104

Abstract

A cyber-physical system (CPS) is a new mechanism controlled or monitored by computer algorithms that intertwine physical and software components. Advanced persistent threats (APTs) represent stealthy, powerful, and well-funded attacks against CPSs; they integrate physical processes and have recently become an active research area. Existing offensive and defensive processes for APTs in CPSs are usually modeled by incomplete information game theory. However, honeypots, which are effective security vulnerability defense mechanisms, have not been widely adopted or modeled for defense against APT attacks in CPSs. In this study, a honeypot game-theoretical model considering both low- and high-interaction modes is used to investigate the offensive and defensive interactions, so that defensive strategies against APTs can be optimized. In this model, human analysis and honeypot allocation costs are introduced as limited resources. We prove the existence of Bayesian Nash equilibrium strategies and obtain the optimal defensive strategy under limited resources. Finally, numerical simulations demonstrate that the proposed method is effective in obtaining the optimal defensive effect.

KEYWORDS

advanced persistent threat, cyber security, game theory, honeypot, limited resources

1 | INTRODUCTION

A cyber-physical system (CPS) is a new mechanism controlled or monitored by computer algorithms, which intertwines physical and software components such as smart grids, autonomous automobile systems, medical monitoring, process control systems, robotics systems, and automatic pilot avionics [1]. Unlike traditional systems, a full-fledged CPS is typically designed as a network of interacting elements with physical inputs and outputs, rather than as standalone devices. Therefore, although the development of algorithms and technologies can significantly improve the resilience of integrated systems, as the number of cyber-attacks continues to increase, CPS security has become an important subject of research and development [2].

Cyber security is constantly evolving in response to increasingly sophisticated cyber attacks. Advanced persistent threats (APTs) [3] are becoming a major cyber security issue, making traditional defense mechanisms gradually ineffective. Their salient features are as follows: First, they are usually initiated by an incentive-driven entity with specific targets. Second, they are persistent in achieving their goals and may involve multiple stages or long-term ongoing operations. Third, they are highly adaptive and stealthy to avoid being detected. In fact, there are hundreds of malware variations, which render the protection from APT attacks extremely challenging [4]. However, APT-related command and control network traffic can be detected using sophisticated methods at the cyber layer, where both deep log analyses and log correlation from various sources can assist in detecting APT activities [5].

Honeypots are an active defense technology [6] whereby some hosts, network services, or information are arranged as bait so that attack behaviors may be detected and analyzed [7]. Therefore, honeypots are an effective complement to traditional security systems against APT attacks. Unlike other security tools, most honeypots can only generate logs, owing to their low degree of automation; hence, human involvement is required to detect and analyze the attacks on most honeypots. In addition, honeypots may be either high-interaction (HIH) or low-interaction (LIH). The former can completely mimic real servers [8], whereas the latter can provide only partial service [9]. To the best of our knowledge, there is currently little work on the use of honeypots in the APT attack-defense game. Considering their limited resources and classification, honeypots are not sufficient for handling actual attacks, which motivates the present study.

In this study, the traditional honeypot cost requirement is exceeded because the human analysis cost is also considered [10]. Hence, we propose a honeypot game-theoretical model with low- and high-interaction modes (LHHG) to study the offensive and defensive CPS interactions and processes as an incomplete information game with limited resources. We prove the existence of several Bayesian Nash equilibria (BNE) in different situations and obtain the optimal defensive strategy. We further optimize the detection effect by allocating deployment resources and distributing human analysis costs between LIHs and HIHs. The results demonstrate that the proposed model and method can optimize the defensive effect with limited resources. The main contributions are summarized below.

1. We introduce a new honeypot game-theoretical model for CPS security against APT-attacks. Moreover, we classify honeypots into high- and low-interaction modes for a more accurate interaction process.
2. We also introduce honeypot allocation and human analysis costs as limited resources in the honeypot game-theoretical model and optimize the defense payoff, as the defender's budget is usually insufficient in practice.

The rest of the paper is organized as follows. Section 2 provides a summary of related work. Section 3 describes the proposed honeypot game-theoretical model based on limited resources. In Section 4, the existence of BNE is proved, and the defensive effect with limited resources is optimized. In Section 5, extensive numerical simulations using MATLAB are carried out to evaluate the proposed method. Finally, Section 6 concludes the paper.

2 | RELATED WORK

In this section, we briefly summarize related work on security issues in CPSs, honeypots for network attacks, and the use of game theory for modeling offense and defense processes.

2.1 | Security issues in cyber-physical systems

This study is related to recent investigations into several prominent security issues in CPSs, such as smart grids, high confidence medical devices and systems, robots, distributed robotics, and transportation. Some studies primarily focus on intrusion detection. For example, Faisal et al [11] proposed an intrusion detection system (IDS) architecture that uses the AMI data flow in a smart grid to analyze the performance of existing data flow mining algorithms and IDS data sets. However, IDSs are less effective in defending against several long-term delitescence attacks such as APT attacks. Howser et al [12] proposed a modal model for Stuxnet attacks that use the operator's trust to remain undetected. They defined operators that allow the manipulation of belief and trust states within the model. In fact, trust in a CPS is a key to the success of the attack.

We list several possible APT threats related to CPS security as follows: (i) high complexity may cause unknown vulnerabilities; (ii) CPSs contain different networks, whose interaction may easily lead to new types of attacks and, eventually, to the collapse of the defense system; and (iii) multiple nodes in the network are potential threats because they are highly vulnerable to attackers.

2.2 | Honeypots for advanced persistent threat attacks

Existing studies focus on the use of different types of defense mechanisms for APT-related attacks on both the cyber and physical layers of the system. Cyber solutions include moving target defense [13], trust mechanisms, and defense-in-depth techniques [14]. Physical-layer solutions include watermarking, adding redundancies, and resilient control mechanisms. In addition, holistic cyber-physical solutions for APT-related attacks have been studied in [15]. That study presents a secure and resilient mechanism that employs customized cryptographic tools to encrypt the data of a control problem and develops verification methods to ensure the integrity of the computational results from the cloud. Although this mechanism can achieve data confidentiality and integrity, its defensive process is passive and leads to increased security input cost. Honeypots are an active defense technology and are used to induce attacks so that attack behaviors may be detected and analyzed. Therefore, honeypots are an effective supplement to CPS defense systems against APT attacks.

The concept of honeypot first appeared in the book "The Cuckoo's Egg" [16], where honeypot technology is used to discover and trace the story of a commercial espionage case. Since 1998, this technology has gradually attracted the attention of security researchers who have developed honeypot software tools specifically designed to deceive attackers. Provos [17] presented "honeyd," which is a honeypot software package that monitors large-scale honeynets. Vetsch [18] focused on Web application attacks, such as remote and local file packages, to simulate the exploit process and generate response results. In addition, the realization of the spoofing environment construction mechanism determines the degree of interaction that the honeypot can provide to the attacker.

To the best of our knowledge, most APT-related research primarily uses security vulnerabilities or configuration weaknesses in network services to pose a threat to the target CPS. Xiao et al [19] proposed a Q-learning-based cloud storage defense scheme for detecting APTs and investigated its performance against subjective APT attackers in dynamic subjective APT games. However, most existing APT games ignore the strict resource constraints in the APT defense, such as the limited number of central processing units (CPUs) of a storage defender and an APT attacker. Therefore, Min et al [20] proposed a hot booting PHC-based CPU allocation scheme that chooses the number of CPUs on each storage device based on the current state. However, as effective security vulnerability defense tools, honeypots have not been widely adopted or used to defend APT attacks in CPSs. Fronimos et al [21] discussed the utilization of LIHs that could indicate early signs of jeopardy from APT attacks. Jasek et al [22] described the methods and procedures of APT attacks, and analyzed and proposed solutions for detecting these threats using HIHs. In addition, some previous studies pointed out the idea that honeypots can be deployed in a CPS for defense against DDoS attacks [23]. It should be noted that the impact of human analysis cost on the honeypot defensive effect has been ignored in previous studies.

2.3 | Game theory for modeling

The application of game theory (which is a useful method for modeling offensive and defensive process in CPSs) to APT modeling has been studied in [24] and [25]. In [24], the FlipIt game is proposed as the framework for an offensive and defensive process in which players compete to obtain a shared resource. The attacker can periodically compromise a system completely, in the sense of learning its entire state, including its secret keys. In [25], moving target defense is used as a defense mechanism to mitigate the impact of APT attacks. Both studies analyze the offensive and defensive strategy based on a complete information game. However, the information of both offensive and defensive sides is usually not equal in practice. Therefore, a Bayesian game is a suitable model, as the interaction between the attacker and the defender is usually an incomplete information game in which the defender or attacker is not sure of the type of other players. Wang et al [23] analyzed the interactions between the attacker and the defender, derived optimal strategies for both sides through a Bayesian game, and assumed that the resources of the defender are sufficient. In addition, some studies proposed using deception in game models. Zhuang et al [26] applied game theory to model strategies of secrecy and deception in a multiple-period attacker—defender resource allocation and signaling game with incomplete information. Ceker et al [27] used a formulation method similar to Zhuang's for single-period games. References [26] and [27] focused on cyber security and did not consider physical components. Rao et al [28] studied the strategic interactions between an attacker and a defender using game-theoretic models that consider both cyber and physical components. Moreover, Rao et al [29] further studied a class of infrastructures characterized by the number of discrete components that can be disrupted by either cyber or physical attacks and are protected from cyber and physical reinforcements. In contrast with the above studies, the present study introduces honeypot technology as an active defense mechanism for detecting APT attacks.

Under normal circumstances, the defense resource is budgeted. Although most studies currently consider defensive resources to be sufficient, the reality is that defensive resources are always insufficient. In addition, owing to the incomplete information, a reasonable CPS security assumption is that an attacker can observe and learn the defender's behavior before taking action, and the defender may not even be aware of the attacker's existence. Therefore, we consider the constraints of the honeypot allocation and human analysis costs in the study of defensive strategy and effect; this is closer to reality. Regardless of the behavior analysis of an industrial or virtual network, application scenarios are essentially based on strategy selection. Accordingly, an investigation of strategy selection with limited resources is more general.

3 | GAME MODEL

In this section, we describe the proposed honeypot game-theoretical model, including its information structure, the action spaces of both attacker and defender, and their payoffs. The model extends the single-mode honeypot in [23] to a multimode honeypot and includes limited resources for the defender.

TABLE 1 List of symbols

Symbols	Description	Symbols	Description
Z_1	LIH	Z_2	HIH
W_1	Weak offensive access	W_2	Strong offensive access
ν_1	Access attack launched	ν_2	Access attack not launched
ε_1	Reward of LIH	ε_2	Reward of HIH
γ_1	The cost of weak access attack	γ_1	Cost of strong access attack
lc	Human analysis cost of LIH	hc	Human analysis cost of HIH
Ω_1	SP provides service	Ω_2	SP does not provide service
ζ_1	Allocation cost of LIH	ζ_2	Allocation cost of HIH
$\hat{n}$	Number of LIHs with human analysis cost	$\bar{n}$	Number of LIHs without human analysis cost
$\hat{m}$	Number of HIHs with human analysis cost	$\bar{m}$	Number of HIHs without human analysis cost
N	Number of honeypots	m	Number of HIHs
n	Number of LIHs	C	Total cost of deployment
C_h	Total cost of human analysis	β	Reward of CPS under normal operation

3.1 | Basic game model

In the proposed honeypot game-theoretical model, we study the interaction between visitors and a CPS. When a visitor is a legitimate user, the router assigns the visitor to the normal server. However, if the visitor is an attacker, he/she will be tricked into accessing a honeypot that actively exposes its vulnerability. Despite the assumption that HIHs and LIHs can be accessed with equal probability, the extension from the single-mode to the multi-node case is still challenging owing to the complexity of the generalized BNE with limited resources. The player, who is the legitimate user/owner of the honeypots, is called the service provider (SP), whereas the other player is called the attacker.

The SP benefits from detecting APT attacks through LIHs and HIHs, where an HIH imitates server activities in the CPS and collects large amounts of information. The attacker can access all commands and files in the system with access right. Thus, this honeypot mode has the greatest chance of collecting APT information but consumes the greatest defense resources as well. Unlike HIHs, an LIH imitates partial server activities and is thus less risky and less complex to maintain. The attacker benefits from identifying honeypots and compromising real servers. In addition, we assume that the attacker has two types of APTs: strong and weak access attacks. In the former, compromised systems are exploited so that other systems may be attacked and restrictions such as those set by firewalls may be avoided; the latter indicates an APT attack type that has been publicly exploited [3]. Compared with other threats, an APT first invades the system, then continuously collects data and passes them on to the attacker, and finally decides whether to interrupt the normal operation of physical devices. In this scenario, we did not model the entire APT attack. Instead, we modeled an important stage in which the APT intrusion invaded the system to identify the honeypots. For CPS security, we will use vulnerabilities to enter the network and identify honeypots so that a real server attack may be detected; this is considered the early stage of an APT attack. Hence, it is conceivable that the SP participating in the game includes only honeypots without real servers. In this study, we introduce a strict defense resource constraint for the SP. This is a practical assumption that has been ignored in most previous studies.

We define the honeypot game-theoretical model as a tuple $G \overset{\Delta}{=} <Z, W, F_Z, F_W, U_Z, U_W>$. $Z \in \{Z_1, Z_2\}$ is the SP mode, where Z_1 denotes an LIH and Z_2 denotes an HIH. $W \in \{W_1, W_2\}$ is the type of access attack, where W_1 denotes weak access attack and W_2 denotes strong access attack. $F_Z \in \{\Omega_1, \Omega_2\}$ is a binary strategy used by SP in mode Z, where Ω_1 indicates that the SP operates normally and Ω_2 indicates that services are not provided. $F_W \in \{\nu_1, \nu_2\}$ is a binary strategy used by attackers of type W, where ν_1 indicates that access attack is launched and ν_2 indicates attack access is not launched. $(F_{W_1}, F_{W_2}, F_{Z_1}, F_{Z_1})$ is a set of game strategies for the attacker and SP. U_Z and U_W represent the payoffs of the SP and attacker, respectively. The detailed list of notations is provided in Table 1.

Specifically, ε_1 or ε_2 is the value of the attacker identifying the honeypot and interrupting the normal operation of physical devices; lc or hc denotes the human analysis cost required for LIH or HIH, respectively; ς_1 or ς_2 is the deployment cost required for LIH or HIH, respectively; β indicates the value of the physical system under normal operation. For example, if the CPS is a power grid, ε_1 and ε_2 represent the load cut by the grid, and β represents the electricity fee charged by the grid under normal operation.

As in [30], we consider an asymmetric model in which the attacker's information is stealthy and the SP's information is observable. This asymmetric information structure is crucial in modeling stealthy attacks in cyber security.

3.2 | Service provider's problem

The probability of honeypots detecting APT attacks is related to the mode of honeypots. Table 2 shows the probability P_i

of failing to detect APT attacks, which is also the probability that LIHs and HIHs fail to detect the two types of APT attacks. Hence, when an LIH provides effective service and a weak access attack is not detected, the payoff for the SP is $-\varsigma_1$ ($\varsigma_1 > 0$ denotes the reward for successfully attacking LIHs). However, if a weak access attack is detected, the payoff for the SP is β ($\beta > 0$ denotes the reward of CPS under normal operation). Similarly, when an LIH provides services and a strong access attack is not detected, the payoff for the SP is $-\varsigma_1$. In contrast, when a strong access attack is detected, the payoff for the SP is β. Furthermore, if an HIH provides effective service and a weak access attack is not detected, the payoff for the SP is $-\varsigma_2$ ($\varsigma_2 > \varsigma_1$ denotes the reward for attacking HIHs). Moreover, if an HIH provides effective service and a strong access attack is not detected, the payoff for the SP is $-\varsigma_2$.

The detection probability for LIHs and HIHs varies with their number. The expected non-detection probability of strong and weak access attacks with respect to the number num of LIHs and HIHs is given by the function $\Psi_i\left(\text{num}|p_i, a_i, k\right)$, where (a) $p_i \overset{\Delta}{=} \{\hat{p}_i, \bar{p}_i\}$ is a binary variable, and $\hat{p}_i$ denotes the non-detection probability with human analysis cost, (b) $\Psi_i\left(\text{num} = 1|p_i, a_i, k\right) = p_i$ because if there is only one honeypot, the non-detection probability of access attacks for the SP is the non-detection probability for the honeypot, (c) $a_i \overset{\Delta}{=} \{\hat{a}_i, \bar{a}_i\}$ is a binary variable, and $\hat{a}_i$ is the minimum non-detection probability of an access attack with human analysis cost, (d) k is also a binary variable, and $k = 1$ indicates that human analysis cost is included, and (e) Ψ_i is strictly decreasing and convex because the non-detection probability of similar access attacks by similar honeypots decreases and finally flattens out as the number of similar honeypots increases [31]. This set of conditions on the function Ψ_i is referred to as generic conditions, and those functions that satisfy the generic conditions are referred to as generic functions.

In the honeypot game-theoretical model, the SP does not know the type of access attacks in advance, but it has a priori information about certain statistical metrics, such as the distribution of access types. Hence, we assume that $p(W_1) = 1 - \alpha$, $p(W_2) = \alpha$, where α is the probability of strong access attack. In addition, as the SP should understand the attacker's strategy, we use Bayesian rules to obtain the posterior probability of the SP's behavior and use it to calculate the expected maximum benefit of the SP. Obviously, the strategies (F_{Z_1}, F_{Z_2}) that the SP may use are as follows: $\{(\Omega_1, \Omega_1), (\Omega_1, \Omega_2), (\Omega_2, \Omega_1), (\Omega_2, \Omega_2)\}$, where (F_{Z_1}, F_{Z_2}) indicates the strategies of both LIHs and HIHs. We call these strategies as follows: (Ω_1, Ω_1) is strategy1, (Ω_1, Ω_2) is strategy2, (Ω_2, Ω_1) is strategy3, and (Ω_2, Ω_2) is strategy4.

TABLE 2 Probability of failing to detect access attack

Probability	LIH	HIH
Weak access attack	$\hat{p}_1$	$\hat{p}_2$
Strong access attack	$\hat{p}_3$	$\hat{p}_4$

3.3 | Attacker's problem

In the honeypot game-theoretical model, the attacker should be trapped by a honeypot and should therefore attack on either an LIH or an HIH. Accordingly, the attacker should select an attack strategy that maximizes its payoff. If a weak access attack on an LIH is not detected, the payoff for the attacker is $\varsigma_1 - \gamma_1$ (γ_1 represents the cost of a weak access attack). However, if a weak access attack is detected by an LIH, the payoff for the attacker is $-\gamma_1$. Similarly, if a strong access attack on an LIH is not detected, the payoff for the attacker is $\varsigma_1 - \gamma_2$ ($\gamma_2 > \gamma_1$ represents the cost of a strong access attack). By contrast, if a strong access attack is detected by an LIH, the payoff for the attacker is $-\gamma_2$. Furthermore, if a weak access attack on an HIH is not detected, the payoff for the attacker is $\varsigma_2 - \gamma_1$. However, if a weak access attack is detected by an HIH, the payoff for the attacker is $-\gamma_1$. Similarly, if a strong access attack on an HIH is not detected, the payoff for the attacker is $\varsigma_2 - \gamma_2$. By contrast, if a strong access attack is detected by an HIH, the payoff for the attacker is $-\gamma_2$.

In addition, the attacker does not know the probability distribution of the SP mode, where $p(Z_1) = n/(m+n)$, $p(Z_2) = m/(m+n)$. Analogously, all potential strategies (F_{W_1}, F_{W_2}) that the attackers can use are $\{(\nu_1, \nu_1), (\nu_1, \nu_2), (\nu_2, \nu_1), (\nu_2, \nu_2)\}$, which indicates the strategies for both weak and strong access attacks. These strategies are called as follows: (ν_1, ν_1) is strategy1, (ν_1, ν_2) is strategy2, (ν_2, ν_1) is strategy3, and (ν_2, ν_2) is strategy4.

4 | OPTIMAL DEFENSIVE STRATEGY OF SERVICE PROVIDER

In this section, we study the set of BNE of the honeypot game-theoretical model and analyze the optimal strategies for both players. We then optimize the defensive effect to maximize the payoff for the SP by allocating limited resources between LIHs and HIHs under certain BNE.

4.1 | Bayesian Nash equilibria of game model

To analyze the set of BNE, we first express the payoff of the SP based on different modes under different strategies. When an LIH provides service, the payoff is

$$U_{Z_1}\left(\Omega_1\right) = (1-\alpha) \times U_{\text{LIH,Weak}}(\Omega_1) + \alpha \times U_{\text{LIH,Strong}}(\Omega_1), \quad (1)$$

where $U_{\mathrm{LIH,Weak}}(\Omega_1)$ indicates that the LIH faces weak access attack and provides service, whereas $U_{\mathrm{LIH,Strong}}(\Omega_1)$ indicates that the LIH faces strong access attack and provides service. $U_{\mathrm{LIH,Weak}}(\Omega_1)$ and $U_{\mathrm{LIH,Strong}}(\Omega_1)$ are defined below.

$$\begin{aligned} &U_{\mathrm{LIH,Weak}}(\Omega_1)\\ &\quad=\frac{\hat{n}}{n}\left[\Psi_1(k=1)(-\varepsilon_1-\varsigma_1-\mathrm{lc})+(1-\Psi_1(k_1=1))(\beta-\mathrm{lc})\right]\\ &\qquad+\frac{\bar{n}}{n}\left[\Psi_1(k=0)(-\varepsilon_1-\varsigma_1)+(1-\Psi_1(k=0))\beta\right],\\ &U_{\mathrm{LIH,Strong}}(\Omega_1)\\ &\quad=\frac{\hat{n}}{n}\left[\Psi_3(k=1)(-\varepsilon_1-\varsigma_1-\mathrm{lc})+(1-\Psi_3(k=1))(\beta-\mathrm{lc})\right]\\ &\qquad+\frac{\bar{n}}{n}\left[\Psi_3(k=0)(-\varepsilon_1-\varsigma_1)+(1-\Psi_3(k=0))\beta\right].\end{aligned}\tag{2}$$

When an LIH does not provide service, the payoff can be computed as

$$U_{Z_1}\left(\Omega_2\right)=\frac{\hat{n}}{n}(-\mathrm{lc})-\varepsilon_1-\varsigma_1.\tag{3}$$

Similarly, when a HIH provides service, the payoff $U_{Z_2}(\Omega_1)$ is

$$U_{Z_2}\left(\Omega_1\right)=(1-\alpha)\times U_{\mathrm{HIH,Weak}}(\Omega_1)+\alpha\times U_{\mathrm{HIH,Strong}}(\Omega_1),\tag{4}$$

where $U_{\mathrm{HIH,Weak}}(\Omega_1)$ indicates that an HIH faces weak access attack and provides service, whereas $U_{\mathrm{HIH,Strong}}(\Omega_1)$ indicates that an HIH faces strong access attack and provides service. $U_{\mathrm{HIH,Weak}}(\Omega_1)$ and $U_{\mathrm{HIH,Strong}}(\Omega_1)$ are defined below.

$$\begin{aligned} &U_{\mathrm{HIH,Weak}}(\Omega_1)\\ &\quad=\frac{\hat{m}}{m}\left[\Psi_2(k=1)(-\varepsilon_2-\varsigma_2-\mathrm{hc})+(1-\Psi_2(k=1))(\beta-\mathrm{hc})\right]\\ &\qquad+\frac{\bar{m}}{m}\left[\Psi_2(k=0)(-\varepsilon_2-\varsigma_2)+(1-\Psi_2(k=0))\beta\right],\\ &U_{\mathrm{HIH,Strong}}(\Omega_1)\\ &\quad=\frac{\hat{m}}{m}\left[\Psi_4(k=1)(-\varepsilon_2-\varsigma_2-\mathrm{hc})+(1-\Psi_4(k=1))(\beta-\mathrm{hc})\right]\\ &\qquad+\frac{\bar{m}}{m}\left[\Psi_4(k=0)(-\varepsilon_2-\varsigma_2)+(1-\Psi_4(k=0))\beta\right].\end{aligned}\tag{5}$$

Analogously, when an HIH does not provide service, the payoff can be computed as

$$U_{Z_2}\left(\Omega_2\right)=\frac{\hat{m}}{m}(-\mathrm{hc})-\varepsilon_2-\varsigma_2.\tag{6}$$

From (1), (3), (4), and (6), regardless of the change of ς_1, ς_2, Ψ_1, Ψ_2, Ψ_3, Ψ_4, hc, lc, and α in the feasible domain, the relations $U_{Z_1}(\Omega_1)>U_{Z_1}(\Omega_2), U_{Z_2}(\Omega_1)>U_{Z_2}(\Omega_2)$ always hold true. Therefore, it is obvious that the SP has a strict dominant strategy (Ω_1, Ω_1).

For the attacker, the payoff for a weak access attack using strategy ν_1 is as follows:

$$U_{W_1}\left(\nu_1\right)=U_{\mathrm{Weak,HIH}}(\nu_1)+U_{\mathrm{Weak,LIH}}(\nu_1),\tag{7}$$

where $U_{\mathrm{Weak,HIH}}(\nu_1)$ denotes a weak access attack on an HIH, whereas $U_{\mathrm{Weak,LIH}}(\nu_1)$ denotes a weak access attack on an LIH. $U_{\mathrm{Weak,HIH}}(\nu_1)$ and $U_{\mathrm{Weak,LIH}}(\nu_1)$ are defined below.

$$\begin{aligned} &U_{\mathrm{Weak,HIH}}(\nu_1)\\ &\quad=\frac{\hat{m}}{N}\left[\Psi_2(k=1)(\varepsilon_2-\gamma_1)+(1-\Psi_2(k=1))(-\gamma_1)\right]\\ &\qquad+\frac{\bar{m}}{N}\left[\Psi_2(k=0)(\varepsilon_2-\gamma_1)+(1-\Psi_2(k=0))(-\gamma_1)\right],\\ &U_{\mathrm{Weak,LIH}}(\nu_1)\\ &\quad=\frac{\hat{n}}{N}\left[\Psi_1(k=1)(\varepsilon_1-\gamma_1)+(1-\Psi_1(k=1))(-\gamma_1)\right]\\ &\qquad+\frac{\bar{n}}{N}\left[\Psi_1(k=0)(\varepsilon_1-\gamma_1)+(1-\Psi_1(k=0))(-\gamma_1)\right].\end{aligned}\tag{8}$$

The payoff for a weak access attack using strategy ν_2 is

$$U_{W_1}\left(\nu_2\right)=0.\tag{9}$$

Similarly, the payoff for a strong access attack using strategy ν_1 is

$$U_{W_2}\left(\nu_1\right)=U_{\mathrm{Strong,HIH}}(\nu_1)+U_{\mathrm{Strong,LIH}}(\nu_1),\tag{10}$$

where $U_{\mathrm{Strong,HIH}}(\nu_1)$ denotes a strong access attack on an HIH, whereas $U_{\mathrm{Strong,LIH}}(\nu_1)$ denotes a strong access attack on an LIH. $U_{\mathrm{Strong,HIH}}(\nu_1)$ and $U_{\mathrm{Strong,LIH}}(\nu_1)$ are defined below.

$$\begin{aligned} &U_{\mathrm{Strong,HIH}}(\nu_1)\\ &\quad=\frac{\hat{m}}{N}\left[\Psi_4(k=1)(\varepsilon_2-\gamma_2)+(1-\Psi_4(k=1))(-\gamma_2)\right]\\ &\qquad+\frac{\bar{m}}{N}\left[\Psi_4(k=0)(\varepsilon_2-\gamma_2)+(1-\Psi_4(k=0))(-\gamma_2)\right],\\ &U_{\mathrm{Strong,LIH}}(\nu_1)\\ &\quad=\frac{\hat{n}}{N}\left[\Psi_3(k=1)(\varepsilon_1-\gamma_2)+(1-\Psi_3(k=1))(-\gamma_2)\right]\\ &\qquad+\frac{\bar{n}}{N}\left[\Psi_3(k=0)(\varepsilon_1-\gamma_2)+(1-\Psi_3(k=0))(-\gamma_2)\right].\end{aligned}\tag{11}$$

Analogously, the payoff for a strong access attack using strategy ν_2 is as follows:

$$U_{W_2}\left(\nu_2\right)=0.\tag{12}$$

By (7), (9), (10), and (12), the payoffs are dependent on the value of the parameters. Hence, the attacker does not have a strict dominant strategy.

Theorem 1 *A BNE strategy (ν_1, ν_1, Ω_1, Ω_1) exists in the LHHG model if*

$$\begin{aligned}&\frac{\hat{m}}{N}\Psi_2(k=1)\,\varepsilon_2+\frac{\bar{m}}{N}\Psi_2(k=0)\,\varepsilon_2\\ &\quad+\frac{\hat{n}}{N}\Psi_1(k=1)\,\varepsilon_1+\frac{\bar{n}}{N}\Psi_1(k=0)\,\varepsilon_1-\gamma_1\geq 0,\end{aligned}$$

$$\begin{aligned}&\frac{\hat{m}}{N}\Psi_4(k=1)\,\varepsilon_2+\frac{\bar{m}}{N}\Psi_4(k=0)\,\varepsilon_2\\ &\quad+\frac{\hat{n}}{N}\Psi_3(k=1)\,\varepsilon_1+\frac{\bar{n}}{N}\Psi_3(k=0)\,\varepsilon_1-\gamma_2\geq 0.\end{aligned}$$

Proof To make $(\nu_1, \nu_1, \mathit{\Omega}_1, \mathit{\Omega}_1)$ a BNE strategy for attacker, the payoff from an access attack is greater than the payoff from not attacking, that is, $U_{W_1}(v_1) > U_{W_1}(v_2)$ and $U_{W_2}(v_1) > U_{W_2}(v_2)$. Then,

$$\frac{\hat{m}}{N}\Psi_2\,(k=1)\,\varepsilon_2 + \frac{\bar{m}}{N}\Psi_2\,(k=0)\,\varepsilon_2 + \frac{\hat{n}}{N}\Psi_1\,(k=1)\,\varepsilon_1 + \frac{\bar{n}}{N}\Psi_1\,(k=0)\,\varepsilon_1 - \gamma_1 > 0, \tag{13}$$

$$\frac{\hat{m}}{N}\Psi_4\,(k=1)\,\varepsilon_2 + \frac{\bar{m}}{N}\Psi_4\,(k=0)\,\varepsilon_2 + \frac{\hat{n}}{N}\Psi_3\,(k=1)\,\varepsilon_1 + \frac{\bar{n}}{N}\Psi_3\,(k=0)\,\varepsilon_1 - \gamma_2 > 0. \tag{14}$$

When the SP is an LIH and the parameters satisfy (13), ν_1 is the optimal strategy for the attacker; otherwise, ν_2 is the optimal strategy, and the attacker will not launch an access attack to identify the LIH. Similarly, if the SP is an HIH and the parameters satisfy (14), ν_1 is the optimal strategy for attacker. Therefore, we can obtain the optimal strategy (v_1, v_1) when the parameters satisfy (13) and (14).

We now further check whether the strategy $(\mathit{\Omega}_1, \mathit{\Omega}_1)$ is the strict dominant strategy from the perspective of the SP. Assuming that $U_{Z_1}(\Omega_1) > U_{Z_1}(\Omega_2)$ and $U_{Z_2}(\Omega_1) > U_{Z_2}(\Omega_2)$, we consider the following:

$$\begin{aligned}&(1-\alpha)\left\{\frac{\hat{n}}{n}\left[\Psi_1(k=1)(-\varepsilon_1-\varsigma_1-\ \mathrm{lc})\right.\right.\\&+(1-\Psi_1(k=1))(\beta-lc)\Big]+\frac{\bar{n}}{n}\left[\Psi_1(k=0)(-\varepsilon_1-\varsigma_1)\right.\\&\left.\left.+(1-\Psi_1(k=0))\beta\right]\right\}+\alpha\left\{\frac{\hat{n}}{n}[\Psi_3(k=1)\right.\\&\times(-\varepsilon_1-\varsigma_1-\mathrm{lc})+(1-\Psi_3(k=1))(\beta-\mathrm{lc})]+\frac{\bar{n}}{n}\\&\left.\times\left[\Psi_3(k=0)(-\varepsilon_1-\varsigma_1)+(1-\Psi_3(k=0))\beta\right]\right\}\\&\geq\frac{\hat{n}}{n}(-\ \mathrm{lc})-\varepsilon_1-\varsigma_1,\end{aligned} \tag{15}$$

$$\begin{aligned}&(1-\alpha)\left\{\frac{\hat{m}}{m}[\Psi_2(k=1)(-\varepsilon_2-\varsigma_2-hc)\right.\\&+(1-\Psi_2(k=1))(\beta-hc)]+\frac{\bar{m}}{m}[\Psi_2(k=0)(-\varepsilon_2\\&\left.-\varepsilon_2)+(1-\Psi_2(k=0))\beta]\right\}+\alpha\left\{\frac{\hat{m}}{m}[\Psi_4(k=1)\right.\\&\times(-\varepsilon_2-\varsigma_2-hc)+(1-\Psi_4(k=1))(\beta-hc)]+\frac{\bar{m}}{m}\\&\left.\times[\Psi_4(k=0)(-\varepsilon_2-\varsigma_2)+(1-\Psi_4(k=0))\beta]\right\}\\&\geq\frac{\hat{m}}{m}(-hc)-\varepsilon_2-\varsigma_2.\end{aligned} \tag{16}$$

When the parameters satisfy (13) and (14), (15) and (16) hold true because $0 < \Psi_i < 1$. We verify (15) as an example:

$$\begin{aligned}&U_{Z_2}(\Omega_1)\\&=(1-\alpha)\left\{\tfrac{\hat{n}}{n}[\Psi_1(k=1)(-\varepsilon_1-\varsigma_1-\mathrm{lc})\right.\\&\quad+(1-\Psi_1(k=1))(\beta-\mathrm{lc})]+\tfrac{\bar{n}}{n}[\Psi_1(k=0)(-\varepsilon_1-\varsigma_1)\\&\quad\left.+(1-\Psi_1(k=0))\beta]\right\}+\alpha\left\{\tfrac{\hat{n}}{n}[\Psi_3(k=1)(-\varepsilon_1-\varsigma_1-\mathrm{lc})\right.\\&\quad+(1-\Psi_3(k=1))(\beta-\mathrm{lc})]+\tfrac{\bar{n}}{n}[\Psi_3(k=0)(-\varepsilon_1-\varsigma_1)\\&\quad\left.+(1-\Psi_3(k=0))\beta]\right\}\\&=\tfrac{\hat{n}}{n}(-\mathrm{lc})+(-\varepsilon_1-\varsigma_1)\left[(1-\alpha)\tfrac{\hat{n}}{n}\Psi_1(k=1)+(1-\alpha)\tfrac{\bar{n}}{n}\right.\\&\quad\left.*\Psi_1(k=0)+\alpha\tfrac{\hat{n}}{n}\Psi_3(k=1)+\alpha\tfrac{\bar{n}}{n}\Psi_3(k=0)\right]+\beta\\&\quad*\left[(1-\alpha)\tfrac{\hat{n}}{n}(1-\Psi_1(k=1))+(1-\alpha)\tfrac{\bar{n}}{n}(1-\Psi_1(k=0))\right.\\&\quad\left.+\alpha\tfrac{\hat{n}}{n}(1-\Psi_3(k=1))+\alpha\tfrac{\bar{n}}{n}(1-\Psi_3(k=0))\right]\\&\quad>\tfrac{\hat{n}}{n}(-\mathrm{lc})+(-\varepsilon_1-\varsigma_1)\left[\tfrac{\hat{n}}{n}\Psi_3(k=0)+\tfrac{\bar{n}}{n}\Psi_3(k=0)\right]\\&\quad+\beta\left[(1-\alpha)\tfrac{\hat{n}}{n}(1-\Psi_1(k=1))+(1-\alpha)\tfrac{\bar{n}}{n}(1-\Psi_1(k=0))\right.\\&\quad\left.+\ \alpha\tfrac{\hat{n}}{n}(1-\Psi_3(k=1))+\alpha\tfrac{\bar{n}}{n}(1-\Psi_3(k=0))\right]\\&=U_{Z_2}(\Omega_2)+\beta\left[(1-\alpha)\tfrac{\hat{n}}{n}(1-\Psi_1(k=1))\right.\\&\quad+(1-\alpha)\tfrac{\bar{n}}{n}(1-\Psi_1(k=0))+\alpha\tfrac{\hat{n}}{n}(1-\Psi_3(k=1))\\&\quad\left.+\alpha\tfrac{\bar{n}}{n}(1-\Psi_3(k=0))\right].\end{aligned} \tag{17}$$

Specifically,

$$\begin{aligned}&\beta\left[(1-\alpha)\frac{\hat{n}}{n}(1-\Psi_1(k=1))+(1-\alpha)\frac{\bar{n}}{n}(1-\Psi_1(k=0))\right.\\&\left.+\alpha\frac{\hat{n}}{n}(1-\Psi_3(k=1))+\alpha\frac{\bar{n}}{n}(1-\Psi_3(k=0))\right]>0\end{aligned} \tag{18}$$

always holds true. Therefore, it is obvious that the strategy $\mathit{\Omega}_1$ will be the dominant strategy, and the attacker strategy (ν_1, ν_1) is the strict dominant strategy for the SP. Analogously, the proof of (16) is similar to that of (17). Hence, when the SP is an HIH, the strategy $\mathit{\Omega}_1$ is also a dominant strategy for the SP.

In addition, when $U_{W_1}(v_1) = U_{W_1}(v_2)$ and $U_{W_1}(v_1) > U_{W_1}(v_2)$, both attacker strategies (v_1, v_1) and (v_2, v_1) are the same; furthermore, both $(\nu_1, \nu_1, \mathit{\Omega}_1, \mathit{\Omega}_1)$ and $(\nu_2, \nu_1, \mathit{\Omega}_1, \mathit{\Omega}_1)$ are BNE. Hence, an attacker can randomly choose a strategy for weak offensive access. Analogously, when $U_{W_1}(v_1) > U_{W_1}(v_2)$ and $U_{W_1}(v_1) = U_{W_1}(v_2)$, both $(\nu_1, \nu_1, \mathit{\Omega}_1, \mathit{\Omega}_1)$ and $(\nu_1, \nu_2, \mathit{\Omega}_1, \mathit{\Omega}_1)$ are BNE.

In summary, from (13)–(17), we can obtain a BNE strategy $(\nu_1, \nu_1, \mathit{\Omega}_1, \mathit{\Omega}_1)$ for the honeypot game-theoretical model, and Theorem 1 can be proved. Analogously, three other BNE strategies $(\nu_1, \nu_2, \mathit{\Omega}_1, \mathit{\Omega}_1)$, $(\nu_2, \nu_1, \mathit{\Omega}_1, \mathit{\Omega}_1)$, and $(\nu_2, \nu_2, \mathit{\Omega}_1, \mathit{\Omega}_1)$ exist in the game under other previously discussed conditions. Furthermore, the Bayesian Nash strategies for the honeypot game-theoretical model can be obtained by Algorithm 1. ■

We have assumed that the participants are fully rational in the game. However, according to [26,32], the participants are often boundedly rational in the model. Therefore, to compare the fully rational case with the boundedly rational

Algorithm 1 Bayesian-Nash Strategy for Honeypot Game-Theoretical Model

```
Input: $\varsigma_1, \varsigma_2, \gamma_1, \gamma_2, p_1, p_2, p_3, p_4, a_1, a_2, a_3, a_4, \alpha, n, m, \hat{n}, \bar{n}$,
  $\hat{m}, \bar{m}, lc, \beta$ and $hc$
Output: Optimal strategy $\left(\nu_{ii}, \nu_{jj}, \Omega_{ii}, \Omega_{jj}\right)$
  /* Initialize the strategy, $\left(\nu_{ii}, \nu_{jj}\right)$*/
  /* Find the stable state*/
  if $\frac{\hat{m}}{N}\Psi_2(k=1)\varepsilon_2 + \frac{\bar{m}}{N}\Psi_2(k=0)\varepsilon_2$
      $+\frac{\hat{n}}{N}\Psi_1(k=1)\varepsilon_1 + \frac{\bar{n}}{N}\Psi_1(k=0)\varepsilon_1 - \gamma_1 \geq 0$ then
    if $\frac{\hat{m}}{N}\Psi_4(k=1)\varepsilon_2 + \frac{\bar{m}}{N}\Psi_4(k=0)\varepsilon_2 + \frac{\hat{n}}{N}\Psi_3(k=1)$
  $* \varepsilon_1 + \frac{\bar{n}}{N}\Psi_3(k=0)\varepsilon_1 - \gamma_2 \geq 0$ then
      choose optimal strategy $(\nu_1, \nu_1, \Omega_1, \Omega_1)$
    else
      choose optimal strategy $(\nu_1, \nu_2, \Omega_1, \Omega_1)$
    end if
  else
    if $\frac{\hat{m}}{N}\Psi_4(k=1)\varepsilon_2 + \frac{\bar{m}}{N}\Psi_4(k=0)\varepsilon_2$
      $+\frac{\hat{n}}{N}\Psi_3(k=1)\varepsilon_1 - \gamma_2 \geq 0$ then
      choose optimal strategy $(\nu_2, \nu_1, \Omega_1, \Omega_1)$
    else
      choose optimal strategy $(\nu_2, \nu_2, \Omega_1, \Omega_1)$
    end if
  end if
```

model, we use the Prelec function [32] defined below for accurately modeling the subjective probability perceptions of each player.

$$w(\Psi_i) = e^{-(-\ln \Psi_i)^{\sigma}}, \quad 0 < \sigma < 1. \tag{19}$$

For example, the BNE strategy (ν_1, ν_1, Ω_1, Ω_1) exists by the following (cf. (13) and (14)):

$$\begin{aligned}&\frac{\hat{m}}{N}w(\Psi_2(k_1=1))\varepsilon_2 + \frac{\bar{m}}{N}w(\Psi_2(k_1=0))\varepsilon_2\\&\quad+\frac{\hat{n}}{N}w(\Psi_1(k_1=1))\varepsilon_1 + \frac{\bar{n}}{N}w(\Psi_1(k_1=0))\varepsilon_1 - \gamma_1 \geq 0,\end{aligned} \tag{20}$$

$$\begin{aligned}&\frac{\hat{m}}{N}w(\Psi_4(k_1=1))\varepsilon_2 + \frac{\bar{m}}{N}w(\Psi_4(k_1=0))\varepsilon_2\\&\quad+\frac{\hat{n}}{N}w(\Psi_3(k_1=1))\varepsilon_1 + \frac{\bar{n}}{N}w(\Psi_3(k_1=0))\varepsilon_1 - \gamma_2 \geq 0.\end{aligned} \tag{21}$$

Therefore, when the parameters satisfy (13), (14), (20), and (21), the BNE strategy is still (ν_1, ν_1, Ω_1, Ω_1). However, when the parameters satisfy (13) and (14) but not (20) and (21), the BNE strategy will change.

4.2 | Simplified optimization problems

In the last subsection, we derived the BNE for the attacker and the SP. However, the payoff of the SP still changes although the BNE has been determined. To maximize the payoff, we should also maximize its utilization with limited resources. Therefore, the payoff optimization problem for the SP can then be simplified as follows. First, we express the payoff:

$$\text{Payoff}_{\text{SP}} = \sum_{d=1}^{n} \frac{U_{Z_{1,j}}(\Omega_1)}{N} + \sum_{g=1}^{m} \frac{U_{Z_{2,i}}(\Omega_1)}{N}. \tag{22}$$

Then, we propose a simplified method to solve the optimization problem. Here, we introduce UP as evaluation factors. There are two types of UP: UPH and UPD. UPH denotes the unit payoff of human analysis cost and UPD denotes the unit payoff of honeypot allocation cost. Furthermore, the expressions of UP can be obtained as follows (see the previous subsection):

$$\text{UPH}_{Z_1} = \frac{U_{Z_1}(\Omega_1)}{\text{lc}}, \tag{23}$$

$$\text{UPH}_{Z_2} = \frac{U_{Z_2}(\Omega_1)}{\text{hc}}, \tag{24}$$

$$\text{UPD}_{Z_1} = \frac{\sum_{d=1}^{n} U_{Z_{1,i}}(\Omega_1)}{n \times \varsigma_1}, \tag{25}$$

$$\text{UPD}_{Z_2} = \frac{\sum_{g=1}^{m} U_{Z_{2,j}}(\Omega_1)}{m \times \varsigma_2}. \tag{26}$$

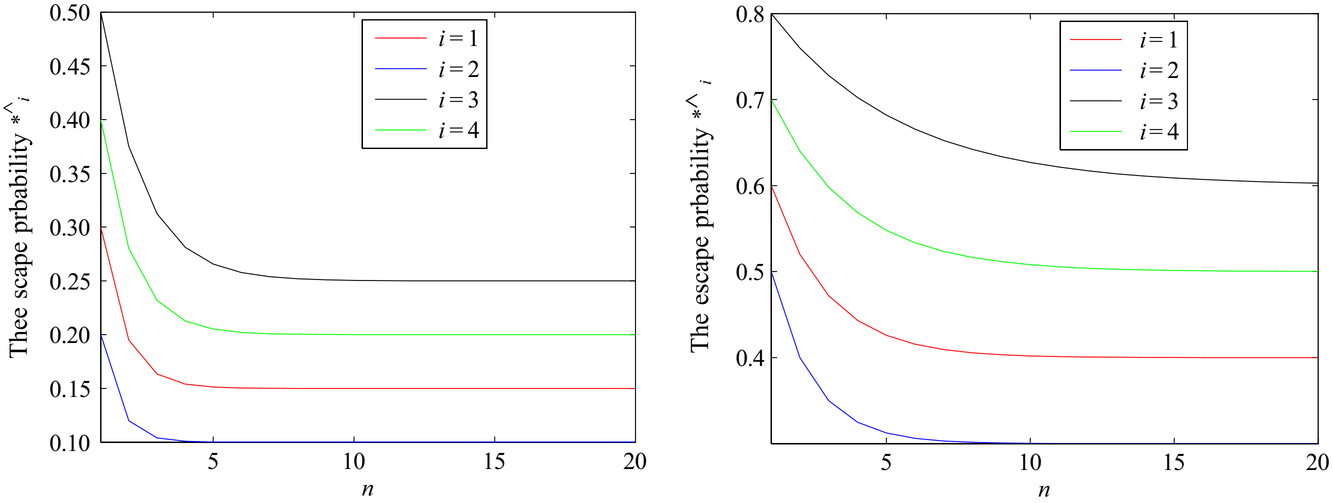
Equations (23) and (24) represent the unit human analysis cost payoff for LIHs and HIHs, respectively. We can obtain the optimal human analysis cost allocation method as follows: If UPH_{Z_1} is greater than UPH_{Z_2}, we tend to allocate more human analysis cost to LIHs. By contrast, if UPH_{Z_2} is greater than UPH_{Z_1}, we tend to allocate more human analysis cost to HIHs.

In addition, (25) and (26) represent the unit payoff of honeypot allocation cost for LIHs and HIHs, respectively. We can obtain the optimal honeypot allocation cost allocation as follows: If UPD_{Z_1} is greater than UPD_{Z_2}, then initially, we tend to allocate more allocation cost to LIHs. By contrast, if UPD_{Z_2} is greater than UPD_{Z_1}, then initially, we tend to allocate more allocation cost to HIHs.

To this end, the optimal payoff of the SP can be obtained as follows:

$$(m, n, \hat{m}, \hat{n})^* = \underset{m, n, \hat{m}, \hat{n}}{\arg\max}\, \text{payoff}_{\text{SP}}, \tag{27}$$

$$\begin{cases} m + n = N \\ m \times \varsigma_2 + n \times \varsigma_1 \leq C \\ \hat{m} \times \text{hc} + \hat{n} \times lc \leq C_{\text{h}} \\ \hat{m} + \bar{m} = m \\ \hat{n} + \bar{n} = n \end{cases}. \tag{28}$$



(A)

(B)

FIGURE 1 Non-detection probability varies with the number of honeypots. (A) With human analysis cost; (B) without human analysis cost

It is well known that the payoff of the SP is related to the parameters in the utility function. Thus, we further analyze the impact of the parameters on the payoff. For example, we analyze the impact of the number of LIHs with human analysis cost on the utility of weak access attack:

$$\frac{\partial U_{W_1}\left(\nu_1\right)}{\partial \hat{m}} = \frac{1}{N}\Psi_2\left(k_1=1\right) + \frac{\hat{m}}{N}\frac{\partial \Psi_2\left(k_1=1\right)}{\partial \hat{m}}, \tag{29}$$

where $(\partial\Psi_2(k_1=1))/\partial\hat{m}<0$ always hold true by property (e) of $\Psi_i(\mathrm{num}|p_i,a_i,k)$ and $1>\Psi_2(k_1=1)>0$ always hold true. Therefore, if $(\partial\Psi_2(k_1=1))/\partial\hat{m}>-[(\Psi_2(k_1=1))/\hat{m}]$, the utility of weak access attack increases with the number of LIHs with human analysis cost. In contrast, if $(\partial\Psi_2(k_1=1))/\partial\hat{m}<-[(\Psi_2(k_1=1))/\hat{m}]$, the utility of weak access attack decreases as the number of LIHs with human analysis cost increases. In addition, other parameters in the utility of weak access attack are linear. For example, we consider the cost of weak offensive access:

$$\begin{aligned}\frac{\partial U_{W_1}(\nu_1)}{\partial \varsigma_1} = \frac{\hat{m}}{N}&\left[-\Psi_2(k_1=1)-(1-\Psi_2(k_1=1))\right]\\ &+\frac{\bar{m}}{N}\times\left[-\Psi_2(k_1=0)-(1-\Psi_2(k_1=0))\right]\\ &+\frac{\hat{n}}{N}\times\left[-\Psi_1(k_1=1)-(1-\Psi_1(k_1=1))\right]\\ &+\frac{\bar{n}}{N}\times\left[-\Psi_1(k_1=1)-(1-\Psi_1(k_1=1))\right].\end{aligned} \tag{30}$$

Obviously, $[\partial U_{W_1}(\nu_1)]/\partial\varsigma_1<0$ always hold true, and therefore the utility of weak access attack decreases as the cost of LIHs increases. Other parameters can be analyzed analogously.

In general, the conditions for determining the BNE strategy selection are mutually exclusive. These conditions divide the parameter space into four parts and correspond to different BNE strategies. When a parameter changes within a subspace, it affects only a specific value of the utility and does not affect the strategy selection; when the parameter changes across the boundary into another subspace, it not only affects the specific value of the utility but also causes the strategy to change.

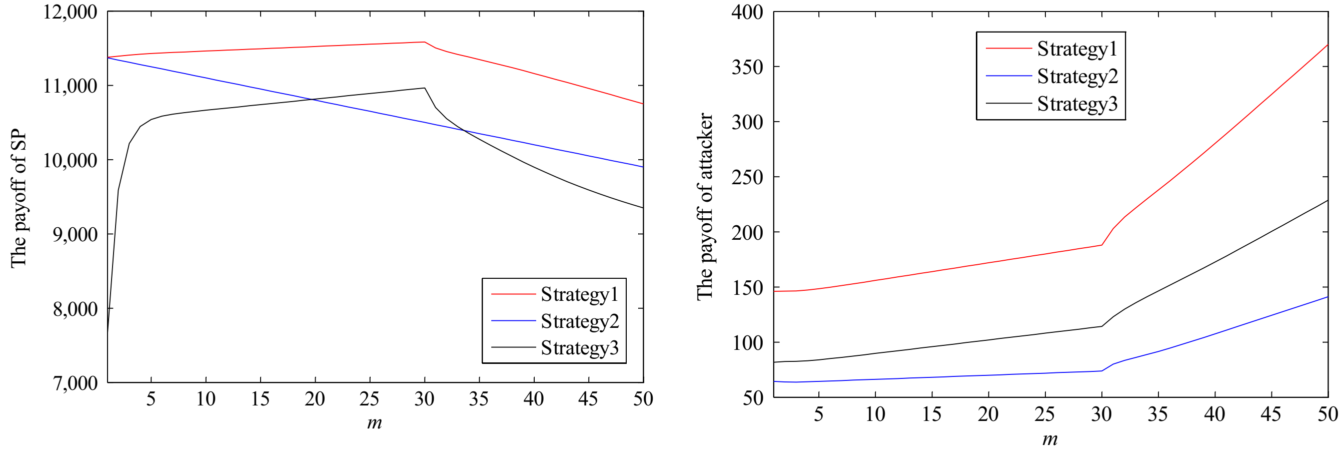
5 | NUMERICAL RESULTS

In this section, we present numerical simulation results for the proposed honeypot game-theoretical model. We study the payoffs of both the attacker and the SP in N = 100 honeypots and analyze the impact of various parameters, including limited resources C, C_h, α, and $\varepsilon_2/\varepsilon_1$. We further study the payoffs and strategies for both players in the BNE strategy (ν_1, ν_1, Ω_1, Ω_1) and analyze the impact of limited resources. In addition, we verify the impact of bounded rationality on the selection of BNE strategies. The details of the numerical simulation settings are explained first, and numerical simulation results are given later.

5.1 | Numerical simulation settings

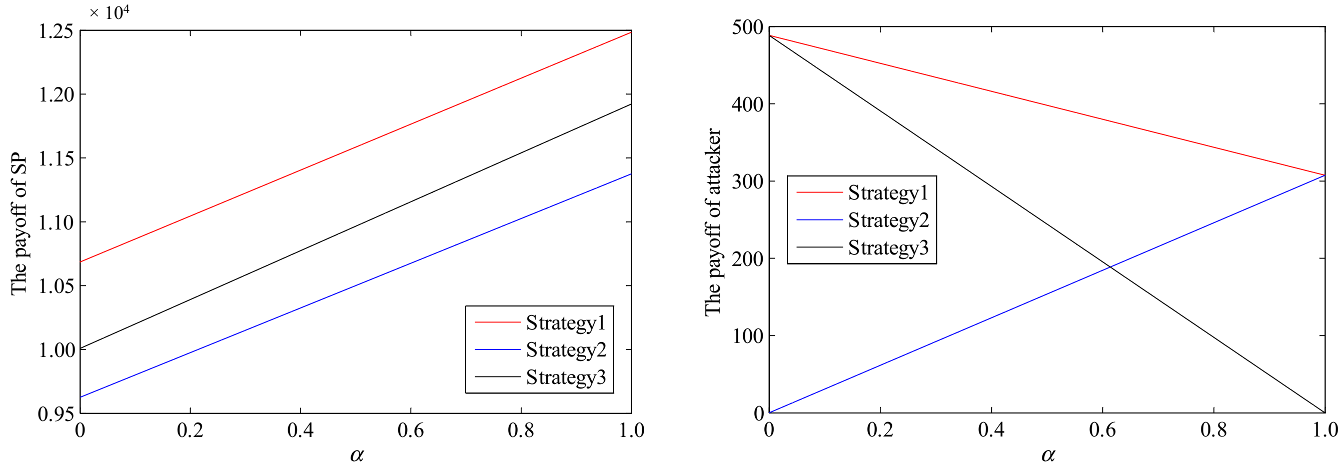
To study the payoffs and analyze the impact of various parameters, we first assume the performance of LIHs and HIHs: the non-detection probabilities for the combinations of LIHs and HIHs are (p_1, p_2, p_3, p_4) = (0.5, 0.4, 0.7, 0.6) and the minimum non-detection probabilities are assumed to be (a_1, a_2, a_3, a_4) = (0.20, 0.15, 0.30, 0.25). In addition, considering the generic condition of the function $\Psi_i(\mathrm{num}|p_i,\ a_i,\ k)$ [33], we assume one simple case as follows:

$$\Psi_i = |k-1|\left(\bar{h}_i\bar{p}_i^{\mathrm{num}}+\bar{a}_i\right)+k\left(\hat{h}_i\hat{p}_i^{\mathrm{num}}+\hat{a}_i\right). \tag{31}$$



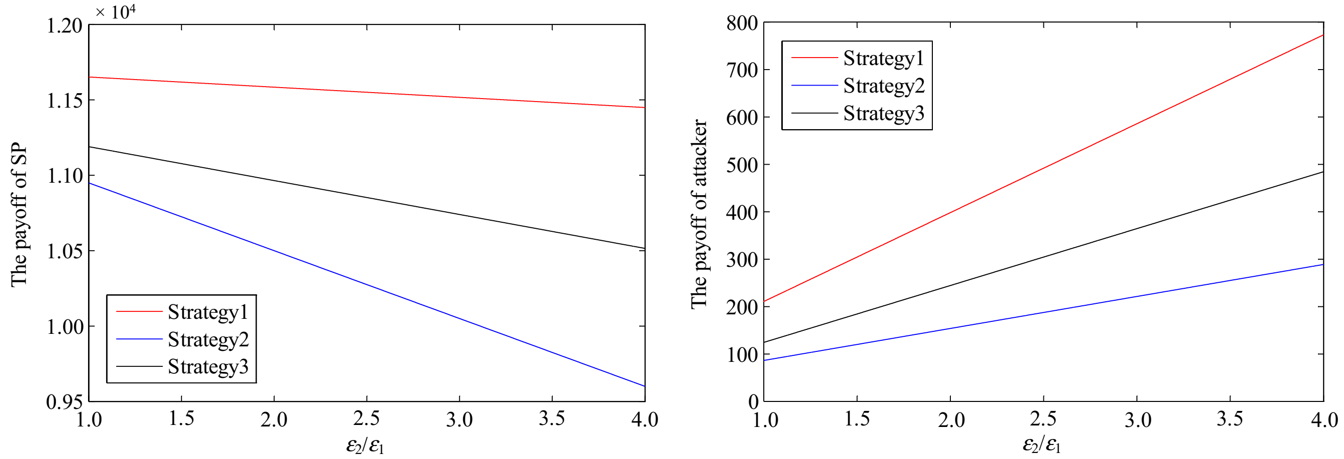
(A) (B)

FIGURE 2 Effects of C, C_h, where in all figures, lc = 1, hc = 1.14lc, $\alpha = 0.5$, $\varsigma_2 = 30$, $\varsigma_1 = 10$, $\gamma_2 = 2$, $\gamma_1 = 1$, $\varepsilon_2 = 30$, $\varepsilon_1 = 15$, and $\beta = 150$ in (A) and (B). (A) SP's payoffs; (B) Attacker's payoffs



(A) (B)

FIGURE 3 Effects of α, where in all figures, $\mathrm{lc}=1, \mathrm{hc}=1.14\mathrm{lc}, \varsigma_2=30, \varsigma_1=10, m=50, \hat{m}=30, \gamma_2=2, \gamma_1=1, \varepsilon_2=30, \varepsilon_1=15$, and $\beta = 150$ in (A) and (B). (A) SP's payoffs; (B) Attacker's payoffs



(A) (B)

FIGURE 4 Effects of $\varepsilon_2/\varepsilon_1$, where in all figures, $\mathrm{lc}=1, \mathrm{hc}=1.14\mathrm{lc}, \varsigma_2=30, \varsigma_1=10, m=50, \hat{m}=30, \gamma_2=2, \gamma_1=1, \varepsilon_1=15, \alpha=0.5$, and $\beta = 150$ in (A) and (B). (A) SP's payoffs; (B) Attacker's payoffs

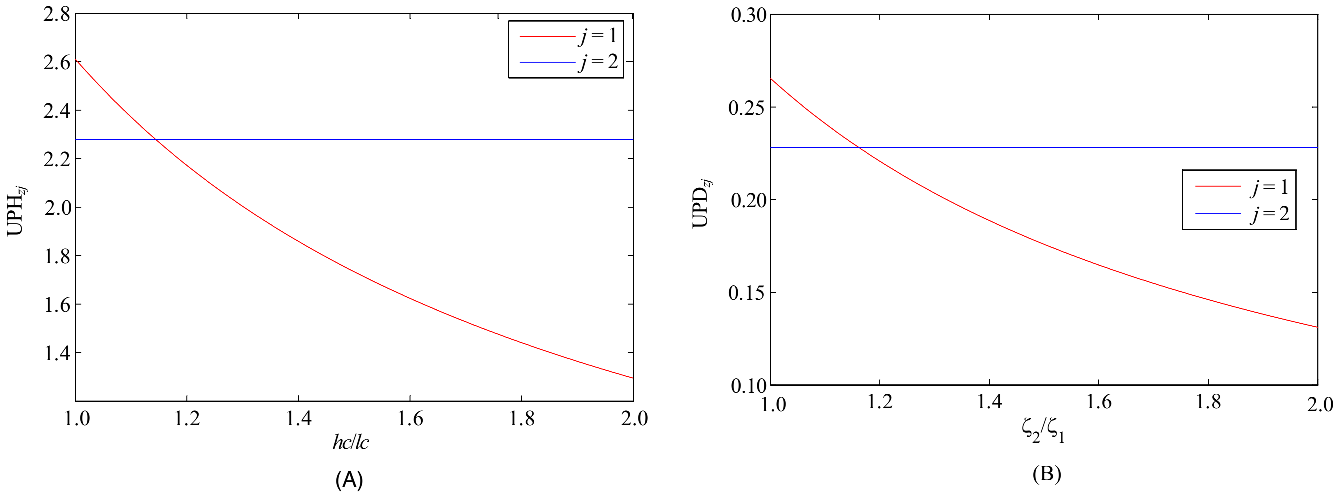


FIGURE 5 Effects of UPH and UPD, where in all figures, $\text{lc} = 1, \varsigma_1 = 10, m = 50, \hat{m} = 30, \gamma_2 = 2, \gamma_1 = 1, \varepsilon_2 = 30, \varepsilon_1 = 15, \alpha = 0.5$, and $\beta = 150$ in (A) and (B). (A) UPH with varying hc/lc; (B) UPD with varying ς_2/ς_1

In particular, $\hat{h}_i = 1 - \hat{a}_i/\hat{p}_i$ and $\bar{h}_i = 1 - \bar{a}_i/\bar{p}_i$. We investigate the properties of the function $\Psi_i\left(\text{num}|p_i, a_i, k\right)$ by adopting four sets of parameters h_i, p_i, a_i in two cases: with and without human analysis cost. As shown in Figure 1, as the number of deployed honeypots increases, the non-detection probability of strong and weak access attacks decreases and asymptotically tends to the minimum non-detection probability. This property is consistent with the theoretical prediction.

Obviously, the human analysis cost and the allocation cost of an LIH and an HIH are different. Specifically, if $C_\text{h} < [n/(m+n)]\text{lc}$, the human analysis cost is not sufficient for an LIH, and no honeypot will function properly. Analogously, if $C < N\varsigma_1$, the allocation cost is not sufficient to deploy N honeypots. Hence, we consider the case $[m/(m+n)]\text{hc} \geq C_\text{h} \geq [n/(n+m)]\text{lc}$ and $C_\text{h} = [(3\text{hc} + 7\text{lc})/10]N$, and the case $N\varsigma_1 < C < N\varsigma_2$ and $C = [N\left(\varsigma_2 + \varsigma_1\right)]/2$.

5.2 | Numerical simulation results

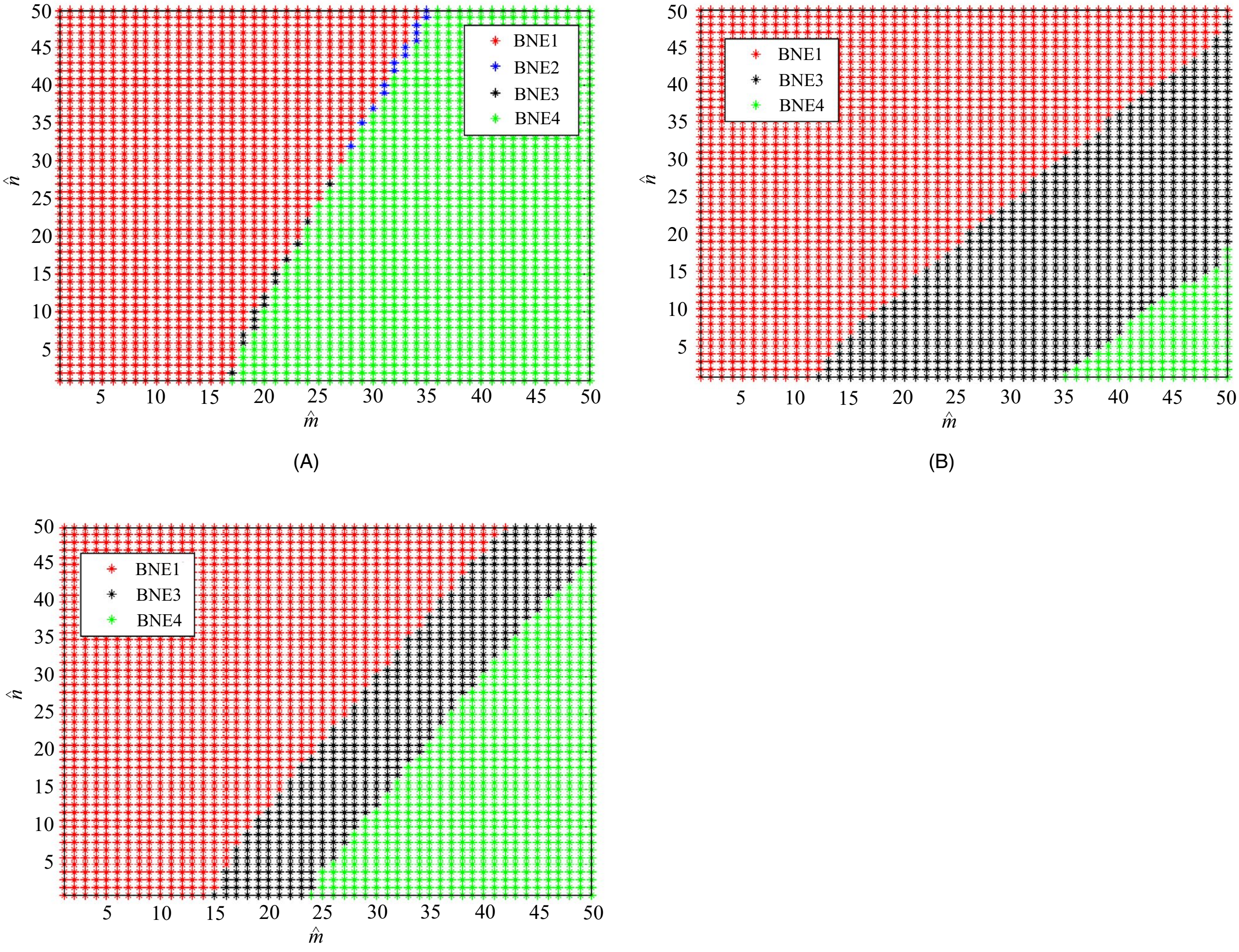
To verify that $(\nu_1, \nu_1, \Omega_1, \Omega_1)$ is the BNE strategy based on the previous simulation setting, we first study the impact of C, C_h, α and $\varepsilon_2/\varepsilon_1$ on the payoffs in Figures 2, 3, and 4. In Figure 2, the payoffs of strategy1, strategy2 and strategy3 for the SP and the attacker have been plotted, where the first strategy is the BNE strategy, and the payoff of strategy1 is larger than that of other strategies. In addition, the payoffs of strategy1 and strategy2 for the SP increase when the number of HIHs is smaller than 30 and decrease otherwise. This is because the deployment of 30 HIHs will reach the upper limit of human analysis costs according to the setting. In contrast, the payoffs of strategy1, strategy2, and strategy3 for the attacker are decreasing owing to the human analysis cost constraints. Furthermore, we have not simulated strategy4 for either player because if a player prefers not to participate in the game, the payoff will be none. Finally, we perform numerical simulations to verify the impact of bounded rationality and full rationality on BNE strategy selection.

In Figure 3, the payoffs of strategy1, strategy2, and strategy3 for the SP and the attacker have been plotted to study the impact of α. When the probability of strong access attack increases, the payoff of the SP increases. Moreover, the payoff of strategy1 is still larger than that of other strategies, as we discussed in Section 4. It is interesting to observe that the payoffs of strategy1 and strategy2 for the attacker tend to be equal as α tends to 1 because when $\alpha = 1$, there is no weak access attack.

In Figure 4, we vary $\varepsilon_2/\varepsilon_1$ and fix the other parameters. It is obvious that the payoffs of strategy1 for both the SP and the attacker are larger than those of other strategies, which verifies the selection of the BNE strategy in Section 4. In addition, as the reward ratio of HIHs and LIHs increases, the payoffs of the SP decrease, whereas the payoffs of the attacker increase.

We then study the rational allocation of resources to maximize the payoff of the SP by comparing $\text{UPD}_{Z_1}, \text{UPD}_{Z_2}$ and $\text{UPH}_{Z_1}, \text{UPH}_{Z_2}$ in Figure 5. It is obvious that when hc/lc is greater than 1.14, we tend to allocate human analysis costs to LIHs; otherwise, we tend to allocate human analysis costs to HIHs. Analogously, if ς_2/ς_1 is greater than 1.14, we tend to deploy LIHs first; otherwise, we tend to deploy HISs first.

We compare the full rationality case with the bounded rationality case in Figure 6. We analyze the two parameters $\hat{m}$ and $\hat{n}$, which directly affect the non-detection probabilities. Obviously, when full rationality changes into bounded rationality, the BNE strategy is not fixed. For example, when



(A)

(B)

(C)

FIGURE 6 Effects of σ, where in all figures, lc = 1, hc = 1.14lc, $\alpha = 0.5$, $\varsigma_2 = 30$, $\varsigma_1 = 10\gamma_2 = 5.5$, $\gamma_1 = 3$, $\varepsilon_2 = 30$, $\varepsilon_1 = 15$, $m = 50$, $n = 50$, and $\beta = 150$ in (A), (B), and (C). (A) $\sigma = 1$; (B) $\sigma = 0.8$; (C) $\sigma = 0.6$

$\hat{m} = 28, \hat{n} = 32$, BNE2 is the selection strategy in full rationality, whereas BNE1 is the selection strategy in bounded rationality.

6 | CONCLUSIONS

We proposed a honeypot game-theoretical model for protecting the servers of a CPS against APT attacks, where the defender's behavior is observable and the defender has limited resources. We proved the existence of several BNEs in the honeypot game-theoretical model and obtained the optimal defensive strategy. We further studied the impact of limited resources and proposed a simplified optimization method. Finally, the proposed method was evaluated through numerical simulations and proved to be effective in obtaining the optimal defensive effect.

CONFLICT OF INTEREST

The authors declare no potential conflict of interests.

ORCID

Wen Tian https://orcid.org/0000-0003-1648-3863

Xiao-Peng Ji https://orcid.org/0000-0001-6094-4626

REFERENCES

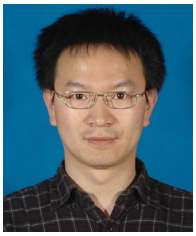
1. Y.F. Li et al, *Nonlane-discipline-based car-following model for electric vehicles in transportation-cyber-physical systems*, IEEE Trans. Intell. Transp. Syst **19** (2017), no. 1, 38–47.
2. O. Yagan et al, *Optimal allocation of interconnecting links in cyber-physical systems: Interdependence, cascading failures, and*

robustness, IEEE Trans. Parallel. Distrib. Syst. **23** (2012), no. 9, 1708–1720.

3. C. Tankard, *Advanced persistent threats and how to monitor and deter them*, Netw. Secur. **8** (2011), 16–19.
4. K. Sood and R.J. Enbody, *Targeted cyberattacks: a superset of advanced persistent threats*, IEEE Secur. Priv. **11** (2013), 54–61.
5. P. Giura and W. Wang, *A context-based detection framework for advanced persistent threats*, in Int. Conf. CyberSecurity, Washington, DC, USA, 2012, pp. 69–74.
6. K. Wang et al, *Game-theory-based active defense for intrusion detection in cyber-physical embedded systems*, ACM Trans. Embed. Comput. Syst. **16** (2016), no. 1, 1–18.
7. A.J. Cao, B.X. Liu, and R.S. Xu, *Summary of the honeynet and entrapment defense technology*, Comput. Eng. **30** (2004), no. 9, 1–3.
8. F. Zhang et al, *Honeypot: a supplemented active defense system for network security*, in Int. Conf. Parallel Distrib. Comput., Chengdu, China, 2003, pp. 231–235.
9. G. Portokalidis and H. Bos, *Sweetbait: zero-hour worm detection and containment using low-and high-interaction honeypots*, Comput. Netw. **51** (2007), no. 5, 1256–1274.
10. M. Nawrocki et al, *A survey on honeypot software and data analysis*, 2016, Available from: arXiv preprint arXiv:1608.06249.
11. M.A. Faisal et al, *Data-stream-based intrusion detection system for advanced metering infrastructure in smart grid: a feasibility study*, IEEE Syst. J. **9** (2015), 31–44.
12. G. Howser and B. McMillin, *A modal model of stuxnet attacks on cyber-physical systems: A matter of trust*, in Eighth Int. Conf. Softw. Security Reliability, San Francisco, USA, 2014, pp. 225–234.
13. S. Jajodia et al, Moving Target Defense II: Application of Game Theory and Adversarial Modeling, Springer, New York, 2012.
14. J. Pawlick, S. Farhang, and Q. Zhu, *Flip the cloud: cyber-physical signaling games in the presence of advanced persistent threats*, in Int. Conf. Decision Game Theory Security, London, UK, Nov. 2015, pp. 289–308.
15. Z. Xu and Q. Zhu, *Secure and resilient control design for cloud enabled networked control systems*, in Proc. ACM Workshop Cyber-Phys. Syst.-Security, Denver, CO, USA, Oct. 2015, pp. 31–42.
16. C. Stoll, The cuckoo's egg: tracking a spy through the maze of computer espionage, Simon and Schuster, New York, 1989.
17. N. Provos, *A virtual honeypot framework*, USENIX Secur. Symp. **173** (2004), 1–14.
18. S. Vetsch, Glastopfng: A web attack honeypot, VDM Verlag, New York, 2011.
19. L. Xiao et al, *Cloud storage defense against advanced persistent threats: a prospect theoretic study*, IEEE J. Sel. Areas Commun. **35** (2017), no. 3, 534–544.
20. M.H. Min et al, *Defense against advanced persistent threats in dynamic cloud storage: a colonel blotto game approach*, IEEE Internet Things J. **5** (2018), no. 6, 4250–4261.
21. D. Fronimos, E. Magkos, and V. Chrissikopoulos, *Evaluating low interaction honeypots and on their use against advanced persistent threats*, in Proc. Panhellenic Conf. Inform., Athens, Greece, Oct. 2014, pp. 1–2.
22. R. Jasek, M. Kolarik, and T. Vymola, *Apt detection system using honeypots*, in Proc. Int. Conf. Appl. Inform. Commun., Valencia, Spain, Aug. 2013, pp. 25–29.
23. K. Wang et al, *Strategic honeypot game model for distributed denial of service attacks in the smart grid*, IEEE Trans. Smart Grid **8** (2017), no. 5, 2474–2482.
24. M. Van Dijk et al, *Flipit: the game of "stealthy takeover"*, J. Cryptol. **26** (2013), 655–713.
25. Q. Zhu and T. Başar, *Game-theoretic approach to feedback-driven multi-stage moving target defense*, in Int. Conf. Decision Game Theory Security, Fort Worth, TX, USA, Nov. 2013, pp. 246–263.
26. J. Zhuang, V.M. Bier, and O. Alagoz, *Modeling secrecy and deception in a multiple-period attacker–defender signaling game*, Eur. J. Oper. Res. **202** (2010), no. 3, 409–418.
27. H. Ceker et al, *Deception-based game theoretical approach to mitigate dos attacks*, in Int. Conf. Decision Game Theory Security, New York, NY, USA, Nov. 2016, pp. 13–38.
28. N.S.V. Rao et al, *Defense of cyber infrastructures against cyber–physical attacks using game-theoretic models*, Risk Anal. **36** (2016), no. 4, 694–710.
29. N.S.V. Rao et al, *Cyber–physical correlation effects in defense games for large discrete infrastructures*, Games **9** (2018), no. 52, 1–24.
30. S. Saha, A. Vullikanti, and M. Halappanavar, *Flipnet: Modeling covert and persistent attacks on networked resources*, in IEEE Int. Conf. Distrib. Comput. Syst., Atlanta, GA, USA, June 2017, pp. 2444–2451.
31. J. Levine et al, *The use of honeynets to detect exploited systems across large enterprise networks*, IEEE Syst. Man Cybern. Soc., West Point, NY, USA, June 2003, pp. 92–99.
32. A. Sanjab, W. Saad, and T. Basar, *Prospect theory for enhanced cyber-physical security of drone delivery systems: a network interdiction game*, IEEE Int. Conf. Commun. (ICC), Paris, France, May 2017, pp. 1–6.
33. W. Tian et al, *Defense strategies against network attacks in cyber-physical systems with analysis cost constraint based on honeypot game model*, Comput. Mater. Continua **60** (2019), no. 1, 193–211.

AUTHOR BIOGRAPHIES

Wen Tian received the BS degree in physics from Changsha University of Science and Technology, Changsha, P.R. China, in 2014 and the MS degree in control theory and control engineering from the Jiangsu University of Science and Technology, Zhenjiang, P.R. China, in 2017. He is currently a PhD candidate with the Nanjing University of Science and Technology, Nanjing, P.R. China. His research interests include cyber–physical systems and network security.



Xiao-Peng Ji received the BS degree in electronics and information engineering and the PhD degree in control science and engineering from the Nanjing University of Science and Technology, Nanjing, P.R. China, in 2005 and 2010, respectively. From 2010 to 2016, he was a senior research and development engineer and technical manager in microgrid and active distribution systems with Beijing Sifang Automation Co., Ltd. He is currently a lecturer with the School of Automation, Nanjing University of Science and Technology. His research interests include smart grids, cyber-physical systems and cyber-security dynamics.

Weiwei Liu received the BS degree in automation and the PhD degree in control science and engineering from the Nanjing University of Science and Technology, Nanjing, P.R. China, in 2010 and 2015, respectively. From 2014 to 2015, he was a Visiting Student with the Department of Computer Science, University of California, Davis, CA, USA. He is currently an associate professor with the School of Automation, Nanjing University of Science and Technology, and a Postdoctoral Researcher with the School of Computer and Software, Nanjing University of Information Science and Technology. His research interests include information hiding, multimedia signal processing, and network security.

Jiangtao Zhai received the BS degree in electrical and computer engineering and the MS and PhD degrees in control science and engineering from the Nanjing University of Science and Technology, Nanjing, P.R. China, in 2007, 2009, and 2013, respectively. He is currently an associate professor with the Jiangsu University of Science and Technology, Zhenjiang, P.R. China. His research interests include network security and wireless sensor networks.

Guangjie Liu received the BS degree in electrical and computer engineering and the PhD degree in control science and engineering from the Nanjing University of Science and Technology, Nanjing, P.R. China, in 2002 and 2007, respectively. He is currently an associate professor with the School of Automation, Nanjing University of Science and Technology. His research interests are in wireless sensor networks, information hiding, and network security.

Yuewei Dai received the BS and MS degrees in system engineering from the East China Institute of Technology, Nanjing, P.R. China, in 1984 and 1987, respectively, and the PhD degree in control science and engineering from the Nanjing University of Science and Technology, in 2002. He is currently a professor with the School of Automation, Nanjing University of Science and Technology. His research interests are in multimedia security, system engineering theory, and network security.

Shuhua Huang received the BS degree in automation from the Nanjing University of Science and Technology, Nanjing, P.R. China, in 2015. He is currently a PhD candidate with the Nanjing University of Science and Technology, Nanjing. His research interests include detection of wireless covert communication and network security.