IEEE Open Journal of the
Computer Society

Received 27 July 2020; accepted 6 October 2020. Date of publication 13 October 2020;
date of current version 23 November 2020. The review of this paper was arranged by Guest Editors Zhou Su, Abderrahim Benslimane,
David (Bong Jun) Choi, Jiliang Li, and Dongfeng Fang.

Digital Object Identifier 10.1109/OJCS.2020.3030825

Anti-Honeypot Enabled Optimal Attack Strategy for Industrial Cyber-Physical Systems

BEIBEI LI [1] (Member, IEEE), YUE XIAO [1], YAXIN SHI [1], QINGLEI KONG [2], YUHAO WU [1], AND HAIYONG BAO [3]

[1] College of Cybersecurity, Sichuan University, Chengdu 610065, China
[2] Future Network of Intelligence Institute (FNii), The Chinese University of Hong Kong (Shenzhen), Shenzhen 518172, China
[3] School of Computer Science and Information Engineering, Zhejiang Gongshang University, Hangzhou 310018, China

CORRESPONDING AUTHOR: QINGLEI KONG (email: kongqinglei@cuhk.edu.cn)

This work was supported in part by the National Key Research and Development Program of China under Grant 2020YFB1805400, in part by the National Natural Science Foundation of China under Grants U1736212, U19A2068, 62002248, and 62072404, in part by the China Postdoctoral Science Foundation under Grants 2019TQ0217, 2020M673277, and 2020M671897, in part by the Provincial Key Research and Development Program of Sichuan under Grant 20ZDYF3145, in part by the Fundamental Research Funds for the Central Universities under Grant YJ201933, and in part by the China International Postdoctoral Exchange Fellowship Program (Talent-Introduction).

ABSTRACT Honeypots have been widely used in the security community to understand the cyber threat landscape, for example to study unauthorized penetration attempts targeting industrial cyber-physical systems (ICPS) and observing the behaviors in such activities. However, some better-resourced cyber attackers may attempt to identify honeypots and develop strategies to compromise them, aka anti-honeypot. In this paper, we present an anti-honeypot enabled optimal attack strategy for ICPS, by employing a novel game-theoretical approach. Specifically, the interactions between the attacker and ICPS defender are captured with a proposed hybrid signaling and repeated game, i.e., a non-cooperative two-player one-shot game with incomplete information. By taking into account both various possible defenses of an ICPS and diverse offensive acts of attackers, a Nash equilibrium is derived, which exhibits an optimal attack strategy for attackers with varying technical sophistication. Extensive simulation experiments on multiple test cases demonstrate that, the derived strategy offers the attackers an optimal tactic to compromise the target ICPS protected by honeypots, while having only incomplete knowledge of the defensive mechanisms.

INDEX TERMS Cyber-physical system, game theory, honeypots, industrial cyber-physical system, repeated game, signaling game.

I. INTRODUCTION

Cyber-physical system (CPS) can be broadly defined as a multi-dimensional complex system connecting both the cyber- and physical-environments [1]. Such an architecture facilitates real-time perception, dynamic control, and information/service delivery in large-scale engineering systems; thus, achieving integrated computing, communication, control (3C) capabilities [2]. As we move towards Industry 4.0 (or Industrial Internet) supported by more advanced communication technologies (e.g., 5G), industrial cyber-physical system (ICPS) will become a norm. A typical/basic ICPS is a three-layer industrial system that integrates numerous sensors, actuators and other Industrial Internet of Things (IIoT) devices and systems [3] (see Fig. 1).

Similar to many other industrial technologies [4], there are a number of challenges in the design and implementation of CPS and ICPS. One such challenge is how do we design a secure and efficient ICPS and securely implement it in a real-world complex environment. The consequences of a successful cyber attack on an ICPS can be fatal and/or have broad societal impact [5], as these systems are usually found in critical infrastructure sectors (e.g., chemical sector, transportation systems sector, dams sector, and energy sector). Common attacks include but not limited to denial-of-service (DoS), distributed DoS (DDoS), and false measurement/command injection attacks.

With the purpose of designing effective cyber security solutions for CPS and ICPS, many security and protection

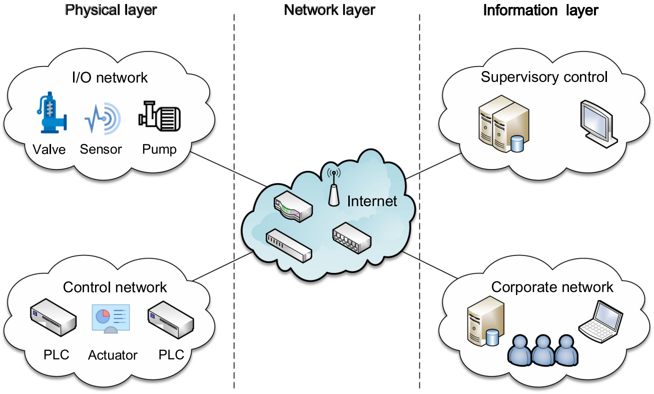


FIGURE 1. A basic ICPS architecture.

mechanisms have been developed. One important approach is to design honeypots [6]–[8], such as dynamic honeypots [9], [10] and fake honeypots (which are masqueraded by normal system as an obvious honeypot to avoid attack) [11], [12], to capture (potentially) malicious cyber activities and study these activities as well as the attackers' behaviors in the honeypot environment. However, it is also known that attackers, especially well-resourced attackers (e.g., state-sponsored, or advanced persistent threat (APT) actors) tend to conduct reconnaissance on their potential targets or targets of interest, which include identification of honeypots, prior to carrying out the actual attack (e.g., false flag cyber operations) [13]. This defeats the purpose of honeypots, hence it aka anti-honeypot. As such, it becomes critical to address this growing problem.

Recently, there have been attempts to model the interactions between the attacker and the ICPS defender using a real interactive game [14]. Such game theoretical approaches generally focused on designing more effective cyber defensive strategies, where the ICPS defenders can employ a variety of strategies to identify, detect and mitigate cyber attacks. In such a model, the attackers are often modeled as having only a fixed, direct attack strategy. In other words, the potential of the attackers to mount more sophisticated and effective attacks is often underestimated [15]. And for such an attacker, the defenders must correspondingly adopt novel and optimal security measures [16]–[18].

In this paper, we focus on investigating an optimal attack strategy, which can be used to circumvent ICPS defensive mechanisms using honeypots. Specifically, we formulate a one-shot signaling game model between the attacker and the ICPS defender with incomplete information. Using this game model, we explain how the attacker could and should react to the different possible defensive activities in one shot and achieve an optimal attack strategy. Following the initial one-shot interaction, both the attacker and the ICPS defender can proceed to adapt their own strategy in their future activities relevant to repeated game. Therefore, we also propose a hybrid game model integrating the signaling game and repeated game to describe their further interactions [19].

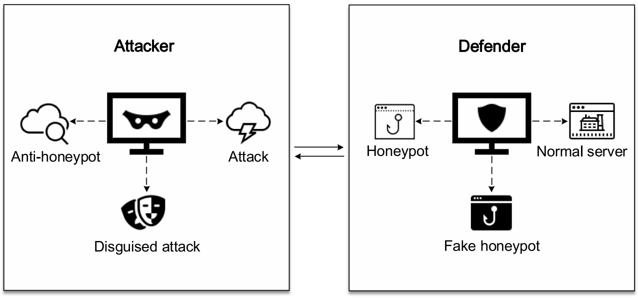


FIGURE 2. The attack-defense network model.

Furthermore, we consider a more realistic attack-defense network model for ICPS in our novel hybrid game (see Fig. 2 the network model). In this model, the ICPS defender analyzes traffic flows and, possibly, reroutes them to relevant honeypots, activates fake-honeypots on a normal server to circumvent an attack in real-time. The attacker can also respond to the ICPS defender, such as proactively identifying potential honeypots or mounting disguised attacks to circumvent defensive mechanisms. In a real-world scenario, cyber attackers have varying sophistication and capabilities. Hence, we model them based on these different levels of their capabilities. Although each level of them is capable of initiating normal attacks, anti-honeypots, and disguised attacks, the associated costs and benefits (e.g., revenues) vary. For example, a nation-state attacker may seek to achieve the maximal impact (e.g., in terms of costs, by exfiltrating intellectual property or carrying out attacks against the nuclear plant) and at a high cost (e.g., using more than one zero-day vulnerabilities and having a large team of cyber attackers working together on the attack). In other words, we seek to design an optimal strategy for different levels of attackers.

The main contributions of this paper are summarized as follows:

- We propose a realistic attack-defense model in ICPS, involving both honeypots and fake honeypots at the ICPS defender, and regular attacks, anti-honeypots, and disguised attacks at the attacker.
- We design a novel hybrid game model, which integrates a signaling game and a repeated game. This allows us to more realistically capture the real-world interactions between cyber attackers and cyber defenders, including attackers with incomplete information about the target(s).
- We demonstrate how an optimal attack strategy can be developed by attackers with different capabilities, using the Nash equilibrium in our game model, when honeypots are present in ICPS for better defense. Our research achievement will help inspire the design of a comprehensive, effective industrial cyber-physical systems.

The remainder of the paper is organized as follows. We introduce the related works in Section II. The one-shot signaling game and repeated game are respectively presented in Sections III and IV. In Section V, we conduct simulation experiments to verify our findings. We then conclude this paper in the last section.

II. RELATED WORK

In this section, we discuss the related work of anti-honeypots and the application of game theory in CPSs.

Krawetz *et al.* [20] introduced the theory and application of anti-honeypot, and they claimed that the ability to detect a honeypot is unlikely to remain limited to spammers; other hostile or malicious groups could benefit from similar identification systems. To promote anti-honeypot systems in relevant technologies. Lin *et al.* [21] developed a model, which is a repeated two-way signaling game, called MSADSs on confidentiality. They facilitated the equilibrium to find the actions maximizing the expected payoffs. The proposed model reacted on the signal received from every intrusion detection system alert, then the ICPS defender gradually reduces the uncertainty about the attacker's targets and calculate the maximizing expected revenue of the ICPS defender by the means of following the equilibrium. Quang *et al.* [22] introduced a mechanism where the ICPS defender and attacker may deceive each other, using honeypots and disguising attack technology. Then he modeled these encounters as a Bayesian game of incomplete information to calculate the equilibrium revenue of one-shot game and the repeated game. Wang *et al.* [23] introduced honeypots technology into the AMI network as a decoy system to analyze the interactions between the attackers and the defenders. Then they proved the existence of several Bayesian-Nash Equilibriums and eventually derive optimal strategies for both sides. Edwards *et al.* [24] presented a game-theoretic model, where the attacker's vulnerability, the knowledge level of the victim, payoffs for different outcomes, and the beliefs about their opponent are taken into account to obtain the best strategic choice.

Furthermore, Some scholars combine honeypots and anti-honeypots technology with knowledge structures in other fields, such as machine learning and automation. Uitto *et al.* [25] reviewed the research status of anti-honeypot and anti-introspection methods and also presented their taxonomy of detecting vectors used by malware. The analysis provides valuable data for threat assessment, malware identification, and prevention. Huang *et al.* [26] emphasized that how to improve the honeypot mechanism that the attacker can't recognize, and how to capture data for the ordinary security researchers, are urgent problems to be solved. Therefore, they proposed a new honeypot automatic recognition model based on the random forest algorithm to automatically and remotely check whether the server is running honeypot services.

As we can see, existing research works mainly focus on the stand-alone utilization of either honeypots, anti-honeypots, or game theory (e.g., the signaling game model, or repeated game model, etc.) in a CPS environment. However, in real-world scenarios, both the attacker and the defender may have various measures, such as honeypots and fake honeypots for the ICPS defender, and disguised attacks and anti-honeypots for the attacker. Besides, the attack-defense network model is always highly dynamic, where the interactions between the attacker and the defender are usually repeated once and once again until one equilibrium is reached or either one side is defeated. In this regard, a mixed game model integrating a signaling game with a repeated game might be a good way to describe the attacker-defender interactions in CPSs. Following these two points, the focus of this paper is on a novel hybrid game in a highly dynamic ICPS environment, where honeypots, fake honeypots, anti-honeypots, disguised attacks, etc., are all considered. This game model can be utilized to derive an optimal attack strategy for the ICPS attackers.

III. ONE-SHOT SIGNALING GAME

In this section, we propose a one-shot signaling game model explaining how the attacker and ICPS defender react to each other's possible actions in one shot, where the equilibrium solutions for this model are also determined.

A. MODEL DEFINITION

In this work, we consider a game model comprising two players, i.e., the attacker (Player 1) and the ICPS defender (Player 2). For Player 2, in order to protect the critical assets in an ICPS (e.g., data servers, SMTP servers, etc.), the ICPS defender deploys honeypots, and fake-honeypots, etc., where a honeypot is employed to trap the attackers and a fake-honeypot is used to mislead and redirect potential attacks. For Player 1, regular attacks, anti-honeypots, as well as disguised attacks are utilized to counter the defensive actions of Player 2, where anti-honeypots are employed to reconnoiter and identify potential honeypots, and disguised attacks are used to hide its offensive actions.

In this model, the ICPS attackers can be classified into three levels according to the attacker's type, the strength of intrusion influence, the cost of launching an attack and other factors in the real scene. In this case, we define the set of types for the attacker as P1:

$$P1 = \{high\ capability, medium\ capability, low\ capability\}$$

Under our classification, low-level attackers tend to use some simple scanning tools to identify ICPS vulnerabilities, medium-level attackers tend to launch ordinary attacks which may be easily noticed by systems, while high-level attackers tend to launch more difficult-to-detect and more destructive attacks. There are three signals (actions) for each type of attacker which are defined as follows:

- **Signal I**: *Attacker scans the targeted system for potential honeypots through anti-honeypots.*
- **Signal A**: *Attacker takes destructive actions to the targeted system.*
- **Signal D**: *Attacker attacks the targeted system by disguising destructive actions as a normal access.*

The ICPS defender is set to only have one type, which is defined by:

$$P2 = \{ICPS\ defender\}$$

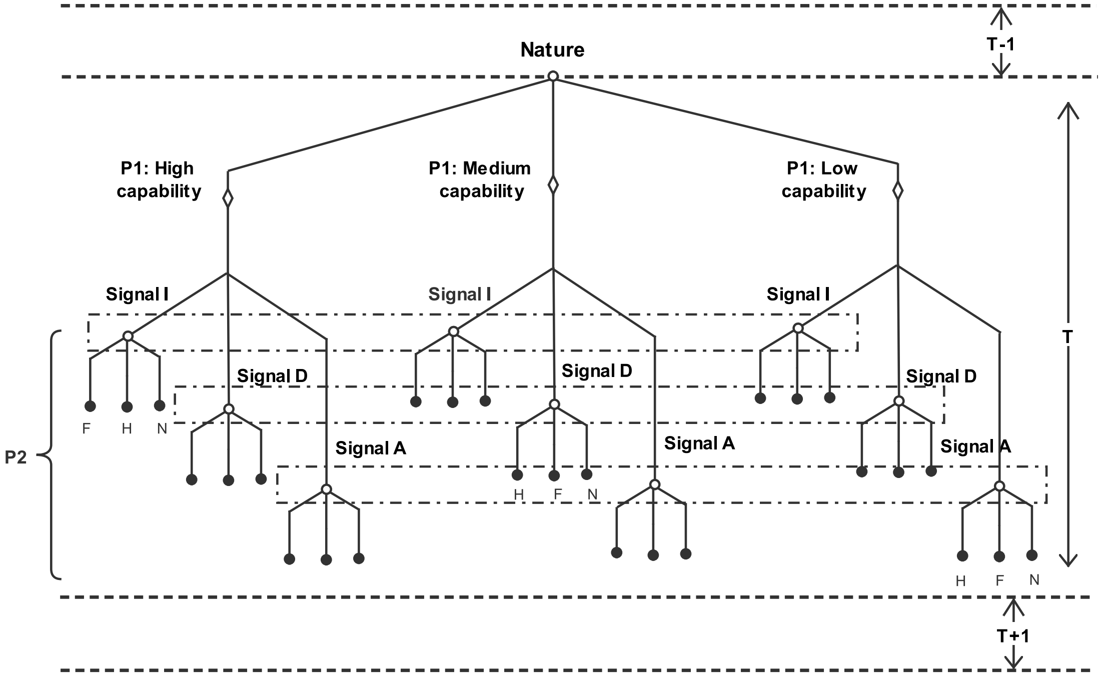


FIGURE 3. The proposed hybrid signaling and repeated game model.

The ICPS defender also has the defensive action set: $\{normal\ service, honeypot, fake\ honeypot\}$. The proposed hybrid signaling and repeated game model is presented in Fig. 3. Each leaf node corresponds to the revenue of the attacker and the ICPS defender. We define and calculate the revenue of one-shot single game and repeated game in the next section.

Note that, in the proposed game model, we also take into account the following special conditions:

1) The revenue of anti-honeypots is only related to the honeypots and fake-honeypots, rather than normal service.
2) The anti-honeypot may be deceived by the fake honeypot that the normal system is pretending to be.
3) Attacker may get trapped by the honeypots.

B. ONE-SHOT SIGNALING MODEL

We built a game model between the attacker and the ICPS defender. In this model, the attacker takes the first action, while the ICPS defender observes the attacker's action and responds to it. The two players in this game can only interact once, hence the model is a one-shot game model.

We denote three levels of the attacker's by **H** (high capability), **M** (medium capability), and **L** (low capability). The ICPS defender's actions can be denoted as **H** (honeypot), **F** (fake honeypot), or **N** (normal server). At the start of this game, the type of an attacker is randomly chosen from a priori probability distribution over all attacker's types with $\theta_H = P(\mathbf{H})$, $\theta_M = P(\mathbf{M})$, and $\theta_L = P(\mathbf{L})$, where $\theta_H + \theta_M + \theta_L = 1$. At this point, the ICPS defender can not get specific information about the attacker. The attacker then sends three signals to the ICPS defender. Regardless of the attacker's type, all the attacker has the action of attacking (**A**), identifying (**I**), and disguising an attack (**D**). We regard the actions as the signals sent by ICPS attackers. After observing the signal sent by the attacker, the ICPS defender uses Bayes rule to obtain a posteriori probability from a priori probability and then chooses an action from his/her own set of possible actions: **H** for rerouting the traffic to honeypots, **F** for providing fake honeypot service, and **N** for offering normal services.

In Fig. 3, some of the ICPS defender's nodes are dotted out, indicating that the ICPS defender can not distinguish these nodes because the attacker's type is unknown. Nodes that the ICPS defender can not distinguish form an information set. Therefore, the attacker has three sets of information: **H**, **M**, and **L**, which correspond to the nodes that indicate the type of attack. The ICPS defender also has three information sets, $H = \{(H|\mathbf{H}), (H|\mathbf{M}), (H|\mathbf{L})\}$, $F = \{(F|\mathbf{H}), (F|\mathbf{M}), (F|\mathbf{L})\}$ or $N = \{(N|\mathbf{H}), (N|\mathbf{M}), (N|\mathbf{L})\}$.

After one round interaction, the attacker and the ICPS defender obtain different payoffs [27]. The calculation of the payoffs will take into account all aspects of the complex factors. In Table 1, we give the definitions of the attacker's and ICPS defender's rewards and costs. For the attacker, rewards mainly come from successfully attacking the right targets (A_r) or from successfully identifying the honeypots (I_r). Besides, when the identification action identifies the fake honeypot successfully, the attacker gains a certain reward (I_g). On the contrary, if the attack behavior is caught by the honeypot, the attacker suffers penalties ($-A_p$). An attacker pays an attack cost ($-A_c$) or identification cost ($-I_c$) when launching an attack and use anti-honeypot technology. Here we assume that $A_r \gg A_c$ and $I_r \gg I_c$.

TABLE 1. Notations About the ICPS Defender and Attacker's Payoffs

Notation	Description
A_r	Attacker's reward for attacking a (fake honeypot/normal) system
A_c	Attacker's cost for launching an attack
A_p	Attacker's penalty for being trapped by a honeypot
I_r	Anti-honeypot's reward for identifying a honeypot
I_c	Anti-honeypot's cost for identification
I_g	Anti-honeypot's gain from identifying a fake honeypot
D_p	Defender's penalty due to a successful attack
H_r	Defender's reward for (the honeypot) traping the attacker successfully
H_p	Defender's penalty for (the honeypot) being identified by anti-honeypot
H_c	Defender's cost for deploying honeypots
F_p	Defender's penalty for (the fake honeypot) being identified
F_c	Defender's cost for providing fake honeypot service
E_c	Extra cost
E_r	Extra reward
α	Attacker's damage factor
β	Attacker's cost factor
γ	Anti-honeypot's identification factor
δ	Anti-honeypot's cost factor

The ICPS defender benefits when the honeypot succeeds in catching the attacker (H_r). However, there is a loss when the normal system is attacked by an attacker ($-D_p$) or when the honeypot or fake honeypot is successfully identified ($-H_p$), ($-F_p$). Meanwhile, the ICPS defender has the cost of deploying honeypots ($-H_c$) and providing fake honeypot service ($-F_c$). Here $H_r \gg H_c$.

Extra reward and cost apply to particular scenarios. It costs the attacker more to disguise the attack ($-E_c$), and because the ICPS defender can not correctly identify the attack, the ICPS defender is more likely to lose valuable information ($-E_r$).

The four factors α, β, γ and δ distinguish three types of attack, can affect the payoffs of the **A** (attack) action, **D** (disguise, or hidden attack) action and **I** action (identification). The higher the level of the attacker type, the greater the attacker's damage factor and cost factor, the greater the gain of the attack and the cost of launching an attack. The anti-honeypot's identification factor (γ) and cost factor (δ) are random factors, independent of the attacker's level. Similarly, they affect the payoffs of the **I** (identify) action. Here, $\alpha, \beta, \gamma, \delta \in [0, 1]$. The detailed payoffs for the attacker and ICPS defender are shown in Table 2.

C. EQUILIBRIA ANALYSIS

We have formulated a signaling game of one shot and incomplete information. The standard solution of such games is the perfect Bayesian equilibrium (PBE) [28]. In our proposed game, we can roughly define a PBE as follows.

Definition 1: The strategy of the attacker and ICPS defender is respectively set to σ and τ. A PBE exists, if and only if the strategy set (σ, τ) and belief set (μ, λ, φ) meet the following two conditions:

- Each player has beliefs about the type of the opponent, but uses Bayes'law to derive these beliefs from observed behavior.
- Given each player's beliefs about the type of the opponent, that player's strategic choice is optimal.

The strategy in the Bayesian game describes the player's entire course of action, that is, each information set represents an action. For the attacker, whether his/her type is **H**, **M**, or **L**, he/she can take one of the **I**, **A**, or **D** actions. If we denote (X, Y, Z) the strategy that type-**H** attacker plays X, type-**M** attacker plays Y while type-**L** attacker plays Z, then there would be $3^3 = 27$ pure strategies [29] for σ. For the ICPS defender, we let (X, Y, Z) represent the strategy for the ICPS defender to play X, Y, and Z under the information sets **H**, **F**, and **N**, respectively. The list of pure strategies for both players are given in Table 3. Also, a mixed strategy can be used in which a player plays a game based on a probability distribution of multiple pure strategies. In a word, (σ, τ) describes a strategy profile for the game.

Next, if a player's information set has already been reached, the probability distribution on his/her information set nodes is the player's belief [30]. In other words, the belief represents the player's likelihood of believing that a signal is coming from a certain type of opponent. A belief system is a combination of all the individual information. For the game we proposed, since only the attacker has multiple types, we only need to define beliefs for an attacker on three sets of information. Thus, the system of beliefs in this game consists of (μ, λ, φ), where $\mu_1 = P(H|I)$, $\mu_2 = P(M|I)$, $\mu_3 = P(L|I)$, $\lambda_1 = P(H|D)$, $\lambda_2 = P(M|D)$, $\lambda_3 = P(L|D)$, $\varphi_1 = P(H|A)$, $\varphi_2 = P(M|A)$, and $\varphi_3 = P(L|A)$.

The first condition for a PBE is the requirement of beliefs, which requires that Bayes' rule to determine the beliefs, i.e.,

$$\mu_1 = \frac{P(\mathbf{H})P(I|\mathbf{H})}{P(\mathbf{H})P(I|\mathbf{H}) + P(\mathbf{M})P(I|\mathbf{M}) + P(\mathbf{L})P(I|\mathbf{L})}, \tag{1}$$

$$\lambda_1 = \frac{P(\mathbf{H})P(D|\mathbf{H})}{P(\mathbf{H})P(D|\mathbf{H}) + P(\mathbf{M})P(D|\mathbf{M}) + P(\mathbf{L})P(D|\mathbf{L})}, \tag{2}$$

$$\varphi_1 = \frac{P(\mathbf{H})P(A|\mathbf{H})}{P(\mathbf{H})P(A|\mathbf{H}) + P(\mathbf{M})P(A|\mathbf{M}) + P(\mathbf{L})P(A|\mathbf{L})}. \tag{3}$$

These relationships should hold for all information sets, and some information sets can never be reached under the strategy given in the game. (i.e., off-equilibrium paths). Meanwhile, the second condition requires two players to choose the optimal responses in all information sets, based on a given belief and the opponent's strategy. Having defined the concept of the necessary solution, then we identify the possibility of the PBEs.

1) Pure-strategy PBE

Theorem 1: There is no pure-strategy PBE for the proposed one-shot signaling game.

TABLE 2. The Players' Payoff Matrix

Type of attack	Type of defense		
	Normal service	Fake honeypot	Honeypot
Attack	$\alpha A_r - \beta A_c, -\alpha D_p$	$\beta A_r - \beta A_c, -\alpha D_p - F_c$	$-\beta A_p - \beta A_c, \beta H_r - H_c$
Anti-honeypot	$-\delta I_c, 0$	$I_g - \delta I_c, -F_p - F_c$	$\gamma I_r - \delta I_c, -\gamma H_p - H_c$
Disguised attack	$\alpha A_r - \beta A_c - E_c, -\alpha D_p - E_c$	$\alpha A_r - \beta A_c - E_c, -\alpha D_p - F_c - E_c$	$-\beta A_p - \beta A_c - E_c, \beta H_r - H_c + E_r$

TABLE 3. The List of Pure Strategies

Type of player	Profile	Label	Profile	Label	Profile	Label	Profile	Label
Attacker	(A, A, A)	σ_1	(A, A, D)	σ_8	(A, A, I)	σ_{15}	(I, D, A)	σ_{22}
	(A, D, A)	σ_2	(A, D, D)	σ_9	(A, D, I)	σ_{16}	(I, I, A)	σ_{23}
	(A, I, A)	σ_3	(A, I, D)	σ_{10}	(A, I, I)	σ_{17}	(I, D, D)	σ_{24}
	(D, A, A)	σ_4	(D, A, D)	σ_{11}	(D, A, I)	σ_{18}	(I, I, D)	σ_{25}
	(D, D, A)	σ_5	(D, D, D)	σ_{12}	(D, D, I)	σ_{19}	(I, D, I)	σ_{26}
	(D, I, A)	σ_6	(D, I, D)	σ_{13}	(D, I, I)	σ_{20}	(I, I, I)	σ_{27}
	(I, A, A)	σ_7	(I, A, D)	σ_{14}	(I, A, I)	σ_{21}	——	——
ICPS defender	(F, F, F)	τ_1	(F, F, H)	τ_8	(F, F, N)	τ_{15}	(N, H, F)	τ_{22}
	(F, H, F)	τ_2	(F, H, H)	τ_9	(F, H, N)	τ_{16}	(N, N, H)	τ_{23}
	(F, N, H)	τ_3	(F, N, F)	τ_{10}	(F, N, N)	τ_{17}	(N, H, H)	τ_{24}
	(H, F, F)	τ_4	(H, F, H)	τ_{11}	(H, F, N)	τ_{18}	(N, N, F)	τ_{25}
	(H, H, F)	τ_5	(H, H, H)	τ_{12}	(H, H, N)	τ_{19}	(N, H, N)	τ_{26}
	(H, N, H)	τ_6	(H, N, F)	τ_{13}	(H, N, N)	τ_{20}	(N, N, N)	τ_{27}
	(N, F, F)	τ_7	(N, F, H)	τ_{14}	(N, F, N)	τ_{21}	——	——

Proof: After exhaustively examining all strategy profiles, we conclude that there is no pure-strategy PBE in this game. The detailed proof process is as follows:

First, we discuss the pure strategy Nash Equilibrium under a certain type of ICPS attacker. The pure strategy Nash Equilibrium is obtained by using the streak plate method. We fix the attack action of the ICPS attacker as disguised attack, general attack and honeypot recognition respectively, and get the maximum of the ICPS defender's benefit, i.e., when we fix the attacker's action as Attack(disguise), we can get the ICPS defender's maximum benefit $\beta H_r - H_c + E_r$ ($\beta H_r - H_c + E_r > -\alpha D_p - E_c$ as well as $\beta H_r - H_c + E_r > -\alpha D_p - F_c - E_c$). Then we fixed the ICPS defender's defense action as normal service, fake honeypot, and honeypot respectively, to get the maximum value of attack action. The maximums are bolded.

$$A = \begin{bmatrix} -\alpha D_p & -\alpha D_p - F_c & \boldsymbol{\beta H_r - H_c} \\ \mathbf{0} & -F_p - F_c & -\gamma H_p - H_c \\ -\alpha D_p - E_c & -\alpha D_p - F_c - E_c & \boldsymbol{\beta H_r - H_c + E_r} \end{bmatrix}, \quad (4)$$

$$D= \begin{bmatrix} \boldsymbol{\alpha A_r - \beta A_e} & \boldsymbol{\beta A_r - \beta A_c} & -\beta A_p - \beta A_c \\ -\delta I_c & I_g - \delta I_c & \boldsymbol{\gamma I_r - \delta I_c} \\ \alpha A_r - \beta A_c - E_c \alpha A_r - \beta A_c - E_c - \beta A_p - \beta A_c - E_c & & \end{bmatrix}. \quad (5)$$

We set the values in ICPS defender's payoff matrix D to d_{ij}, while the values in ICPS attacker's payoff matrix A are set to a_{ij}, where $i, j = 1, 2, 3$. Pure strategy exists only if d_{ij} and a_{ij} are both marked. Therefore, we can see from Eqs. (4) and (5) that this game doesn't have a pure strategy PBE. ■

2) Mixed-strategy PBE

In this section, we solve the mixed-strategy PBE in this game. First, we define two tuples $\bar{\omega} = (\rho_1, \rho_2, \rho_3)$ and $\bar{\upsilon} = o_1, o_2, o_3$. $\bar{\omega}$ is set to indicates a ICPS attacker plays his/her actions with the probability ρ_1, ρ_2, and ρ_3. Type-**H** ICPS attacker always plays **D**, type-**L** always plays **I**, while type-**M** chooses **A**, **I**, and **D** with probability ρ_1, ρ_2 and ρ_3 respectively. By observing ICPS attacker's actions **I** and **A**, the ICPS defender usually react as **N** and **H** respectively, while randomly chooses **N**, **F**, and **H** with probability o_1, o_2 and o_3 by observing **D**. Here, $\rho_1 + \rho_2 + \rho_3 = 1$ and $o_1 + o_2 + o_3 = 1$.

Theorem 2: There is a mixed-strategy PBE($\bar{\sigma}, \bar{\tau}$) in this one-shot signaling game with beliefs $(\bar{\mu}, \bar{\lambda}, \bar{\varphi})$, where $\bar{\sigma} = (D, \bar{\omega}, I)$, $\bar{\tau} = (\bar{\upsilon}, H, N)$ with $\bar{\omega} = (\rho_1^*, \rho_2^*, \rho_3^*)$ and $\bar{\upsilon} = (o_1^*, o_2^*, o_3^*)$.

The detailed proof for Theorem 2 is shown in the **Appendix**.

Remark 1: It can be seen that when the ICPS attacker tends to use anti-honeypot actions, the ICPS defender can't benefit from deploying honeypots for the identification action. According to this, the ICPS defender is likely to use the normal system against the ICPS attacker. In Section V, the remark is proved by the simulation experiment.

IV. REPEATED GAME

A. GAME MODEL AND EQUILIBRIA ANALYSIS

The one-shot signaling game captures only one encounter between the ICPS defender and the ICPS attacker. In other words, the attackers don't know the specific network topology behind the firewall, the only information may be known is the types of defense network entities, such as normal host, honeypot, and fake honeypot. Relatively speaking, the ICPS defenders don't know the type of attack action which would be chosen by the ICPS attacker, but he/she can prepare honeypots to trap the ICPS attacker, or use fake honeypots to deceive the ICPS attacker [31].

We take the one-shot signaling game as a round of the entire game, and in the long term, ICPS defenders may face plenty of similar independent interactions. This situation can be modeled as a game that repeats indefinitely over time. In game theory, this is called the game of "multistage game with observed action and incomplete information". Hence, we assume that the cost, penalty, and revenue of the model don't change over each round. In order to better divide the periods of repeated games, we introduce the concept of time slice. The whole process is regarded as a series of time slices, and each time slice represents a signal game. In each time slot, the nature combined with attackers and ICPS defenders detects the current network state, judges the capability value of the current ICPS attacker, and then plays a new round of signaling game according to this. What's more, the transition of network state is random. Each slice of time can be viewed as a static game with incomplete information. However, in the whole process of attack and defense, the action of both sides during the current time slice will affect the network state of the subsequent time slice, and then affect the direction of the branches of the game tree, which is considered as a dynamic process. It is worth noting that during the time slice shift, the player selects a strategy based on the observation of the opponent's action.

In the calculation of equilibrium revenue of repeated games [32], we introduce four variables to divide the corresponding abilities of P1 players (α, β, γ, and δ), which has been mentioned in Section III-B. Formally, we define T (time slice) as the index of stages, and i as the action taken by player i at stage T. In a other word, i denotes the action signals and specific actions in this game, e.g., A, D, or I for P1–ICPS attacker, or H, F, or N for P2–ICPS defender. Hence, the game's history at the beginning of stage T is encompassed in $h_t = (a^0, a^1, ..., a^{t-1})$ and each $a^j = (a_1^j, a_2^j)$ means the joint observed actions taken by players at stage j.

```
Algorithm 1: Attacker's Payoff Calculation Algorithm.
Input: $P|(a_1^i, d_1^j), (a_2^i, d_2^j), (a_3^i, d_3^j)$, $a_1^I$, $d_1^N$, $a_2^I$, $d_2^F$, $l_c$,
       $l_g$, $l_r$, $\delta_x$, $\alpha_x$, $\beta_x$, $\gamma_x$, $A_r$, $A_c$, $E_c$.
Output: E.
Initialization:
 a). Initialize the payoff of the attacker by $E \leftarrow 0$;
 b). Initialize the game round index by $t \leftarrow 1$.
Procedure:
 In every game round $t$, the attacker and the defender
 choose their own actions, respectively;
while $a_1^i = a_1^I$, $d_1^j = d_1^N$ do
    $\mathrm{E} \leftarrow \mathrm{E} + (-\delta_x l_c)$;
    $t \leftarrow t + 1$;
end
if $a_2^i = a_2^I$, $d_2^j = d_2^F$ then
    $\mathrm{E} \leftarrow \mathrm{E} + (l_g - \delta_x l_c + \alpha_x A_r - \beta_x A_c)$.
else
    $\mathrm{E} \leftarrow \mathrm{E} + (\gamma_x l_r - \delta_x l_c + \alpha_x A_r - \beta_x A_c - E_c)$.
end
return E.
```

Every stage is evolved from the one-shot signaling game. We can learn that a priori distribution over ICPS attacker's types (θ_H, θ_M, and θ_L) which is known beforehand contributes heavily to the actual PBE payoffs. This situation doesn't comply with the unknown ICPS attacker. Therefore, the player's beliefs can't be perfectly estimated. Instead, at the beginning, the nature begins with an initial estimate $\theta_H^0 = P(H|h^0)$, then repeatedly update $\theta_H^t = P(H|h^t)$ after each time slice. Hence, we can get the posterior belief θ_H^{t+1} via Bayesian updates, i.e.,

$$\theta_1^{t+1} = \frac{\theta_1^t P(a_1^t|\mathbf{H}, h^t)}{\theta_1^t P(a_1^t|\mathbf{H}, h^t) + \theta_2^t P(a_1^t|\mathbf{M}, h^t) + \theta_3^t P(a_1^t|\mathbf{L}, h^t)}, \tag{6}$$

where a_1^t refers to the previous ICPS attacker (P1)'s action in stage t.

In real-world scenarios, the repeated games with multiple Nash equilibrium can design multiple strategies, the outcome is uncertain in the absence of communication between the two sides [33]. Hence, it is not reasonable for ICPS attackers to stick to one unfavorable pure strategy equilibrium, since there is no pure strategy equilibrium in this model. In this case, we focus on the mixed strategies application in the repeated game. According to the strategy modes, they can be divided into fixed strategy and trigger strategy. Generally, a mixed strategy means the path formed by the combination of pure Nash equilibrium in the original game is considered. Since we have no pure strategy equilibrium, trigger strategy equilibrium can be chosen [34].

The trigger strategy is to choose a certain strategy at the beginning, and adapts as per the opponent player's strategy in the game. Hence, we set the repeated game strategy of the ICPS attacker as below (see also in Algorithm 1):

1) At the beginning of the game, the ICPS attacker chooses anti-honeypots (I) to detect the defense network. If the ICPS defender responds by a normal service (N), then the second phase continues to cooperate (the ICPS attacker still selects anti-honeypots, and the ICPS defender still selects normal service).
2) If the ICPS defender responds in the form of fake honeypots to the collaboration (the second phase), then

TABLE 4. Comparison of Research Approaches

Reference	Game type	Game process	Model expandability	Equilibrium solution	Performances
Ref. [21]	Incomplete information/ Dynamic	Multi-stage	Average	None	Poor
Ref. [23]	Incomplete information/ Dynamic	Single-stage	Better	Detailed	Medium
Ref. [35]	Incomplete information/ Static	Single-stage	Average	Simple	Poor
Ref. [36]	Complete information/ Static	Multi-Stage	Better	Detailed	Medium
This study	Incomplete information/ Dynamic	Multi-stage	Good	Detailed	Good

we choose attack actions as the penalty of the non-cooperation strategy of the ICPS defender in the third phase.

3) From another aspect, if the ICPS defender responds in the form of honeypots to the collaboration (the second phase), then the disguising attack actions are adopted by the ICPS attacker in the third phase.
4) The cooperation of the first stage can last for $\{1,\ldots,T\}$ time slices. Once the ICPS defender chooses not to cooperate (in the form of honeypots or fake honeypots), the mechanism will be triggered, the second stage and the third stage will only last for one time slice.
5) After the third phase of the game (combating phase), the whole game will be ended. Then, all the payoffs will be calculated.

Theorem 3: In a repeated game, as T increases, the ICPS attacker's revenue of once attack decreases gradually, and the higher the capability of an ICPS attacker, the smaller the value of a single return, and the faster the yield curve falls.

Proof: We define the attack-defense routes as $P|(a_1^i, d_1^j), (a_2^i, d_2^j), (a_3^i, d_3^j)$, where a_k^i and d_k^j $(k = 1, 2, 3)$ respectively denotes the ICPS attacker and ICPS defender's action in the k-th phase. As mentioned above, in the first phase of the repeated game, $a_1^i := I$ and $d_1^j := N$. Assuming that we set the game to repeat round $T + 1$, the triggering occurs in T and the combating occurs in $T + 1$, we can get the ICPS attacker's payoff of the repeated game as (7), shown as follows:

$$\begin{cases} \mathrm{E}\left[p_1 |\left((I,N),(I,F),(A,N)\right)\right] \\ \quad = -\delta_x l_c(T-1) + l_g - \delta_x l_c + \alpha_x A_r - \beta_x A_c, \\ \mathrm{E}\left[p_1 |\left((I,N),(I,H),(D,N)\right)\right] \\ \quad = -\delta_x l_c(T-1) + \gamma_x l_r - \delta_x l_c + \alpha_x A_r - \beta_x A_c - E_c. \end{cases} \tag{7}$$

Consider x as the ICPS attacker's ability level, set $x = H$ when the ICPS attacker's revenue is lower than $\mathrm{E}(u_1)\rho_1^*$, set $x = M$ when the ICPS attacker's revenue is lower than $\mathrm{E}(u_1)\rho_2^*$, and set $x = L$ when the ICPS attacker's revenue is lower than $\mathrm{E}(u_1)\rho_3^*$. The threshold is derived from the calculation of the one-shot signaling game.

On the contrary, the ICPS attacker's payoff in the repeated game can be expressed as (8), which is shown as follows:

$$\begin{cases} \mathrm{E}\left[p_2 |\left((N,I),(F,I),(N,A)\right)\right] \\ \quad = -F_p - F_c - \alpha_x D_p, \\ \mathrm{E}\left[p_2 |\left((N,I),(H,I),(N,D)\right)\right] \\ \quad = \beta_x H_r - H_c + E_r - \alpha_x D_p - E_c. \end{cases} \tag{8}$$

Obviously, from the formulation we have drawn, if $l_g > \gamma_x l_r - E_c$, the combination of attack and defense tactics $(I, N), (I, F), (A, N)$ is more efficient, else $(I, N), (I, H), (D, N)$ would be more profitable. ■

TABLE 5. The Payoff Matrix of the Considered Attack-Defense Game

Attacker	ICPS defender		
	Normal service	Fake honeypot	Honeypot
Attack	(48, -48)	(48, -58)	(-36, 20)
Anti-honeypot	(-4, 0)	(16, -50)	(20, -52)
Attack(disguise)	(38, -38)	(38, -48)	(-46, 30)

In this section, we make a quantitative comparison between the non-cooperative game in the second stage and the antagonistic game in the third stage, to find that the revenue values of l_g, $\gamma_x l_r$, E_c, etc., affect the final outcome of the entire game. Taking these factors as part of the slope, we can obviously infer that the higher the ICPS attacker's capability is, the higher the cost of launching an attack, and the higher the benefit of the attack. However, with the increase of rounds, the attacker's gain rate will be slower and slower. At the same time, the method proposed in this paper is compared with other studies, which is shown in Table 4. Game process refers to whether the dynamic game model has the ability to analyze the multi-stage attack and defense process. The equilibrium solution refers to whether the literature has the method to calculate the equilibrium solution. Because dynamic multi-stage games are often more difficult than static games, the lack of a detailed solution undermines the practicality. Based on this, we can see that the method we proposed is more in line with the real network environment, and more practical. The next section will verify the rationality and inference of the model.

V. EVALUATION

In this section, we evaluate the ICPS attacker's and the ICPS defender's strategies in terms of their payoffs in the one-shot signaling and repeated game, respectively. First, we consider the offensive and defensive payoffs of the one-shot signaling game, and establish a payoff matrix for this game (see Table 5). The relevant payoff parameters (shown in Table 1) are set as follows: $A_r = 130, A_c = 10, A_p = 80, I_r = 60, I_c = 10, I_g = 20, D_p = 120, H_r = 100, H_p = 80, H_c = 20, F_p = 40, F_c = 10, E_c = 10, E_r = 10,$ and in high capability $\alpha = \beta = \gamma = \delta = 1$, in medium capability $\alpha = \beta = \gamma = \delta = 0.7$, in low capability $\alpha = \beta = \gamma = \delta = 0.4$.

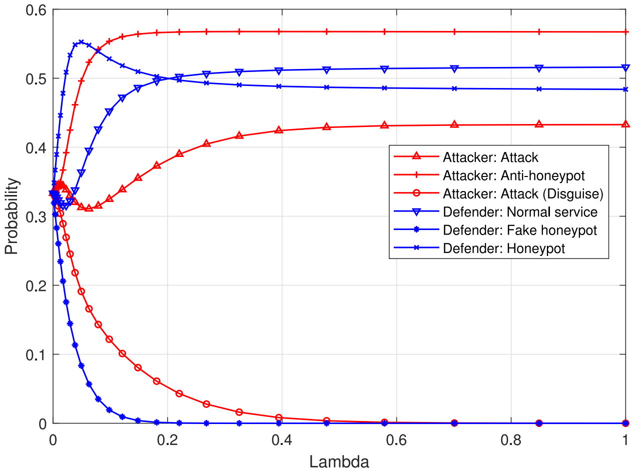


FIGURE 4. **One-shot signaling game results.**

Based on the payoff matrix, we use Gambit[1] to calculate the Nash Equilibrium of the one-shot signaling game.

Figure 4 plots the selection probabilities of all strategies, color-coded by player, as a function of the precision parameter lambda, where we can see that the probability of each strategy converges to the Nash Equilibrium. The results show that in a one-shot signaling game, in order to maximize the profits, the ICPS attacker may abandon the strictly weak strategy (here refers to disguised attack), and tend to choose anti-honeypot. While for the ICPS defender, the best defense strategy against anti-honeypot is to directly provide normal system service. The result is consistent with Remark 1.

The numerical results of the ICPS attacker's payoffs in a repeated game are presented to verify our the proposed model. In this group of experiments, except for the values of $\alpha, \beta, \gamma, \delta$, all the other parameters are the same as that for the one-shot game model. A parameter setting for a test case is defined as a three-tuple: Test case $i := \{a, b, c\}$, where i refers to the index of the test case and a, b, c, respectively, represents the factor setting (note that we set $\alpha = \beta = \gamma = \delta$) of a low capability, medium capability, and high capability ICPS attacker. Here, we consider four test cases, i.e., Test case 1 :={0.2, 0.3, 0.4}, Test case 2 :={0.3, 0.5, 0.7}, Test case 3 :={0.4, 0.7, 1.0}, and Test case 4 :={0.4, 0.9, 1.0}.

According to the repeated strategy, these parameters are used for each repetition of the game. Furthermore, when the revenue of the ICPS attacker is below a certain threshold, the level of the ICPS attacker's capability will be adjusted automatically to maintain the overall revenue in a balanced state. Although the parameters are generically given, we believe that the presented numerical examples are still useful in illustrating the model's behaviors.

We constructed two strategy paths for repeated games, as shown in Fig. 5. Fig. 5(a) represents the strategy: in the first stage of the cooperative game, the ICPS attacker takes the anti-honeypot to scan and the ICPS defender takes the normal service to respond (this stage lasts twelve time slices). In the second stage of the non-cooperative game, the ICPS attacker still takes the anti-honeypots, but the defender responds in fake honeypots. in the third stage of the combating game, the ICPS attacker uses the direct attack to attack the normal service of the defender.

Fig. 5(b) represents the strategy: in the first stage of the cooperative game, the ICPS attacker takes the anti-honeypot to scan and the ICPS defender takes the normal service to respond (this stage lasts twelve time slices). In the second stage of the non-cooperative game, the ICPS attacker still takes the anti-honeypots, but the ICPS defender responds in honeypots. In the third stage of the combating game, the ICPS attacker fights the normal service of the ICPS defender with a disguised attack.

From the experiments, we can verify the inference of the article before. As the number of T increases, the ICPS attacker's revenue will gradually decrease, which is also in line with the real network environment. From the point of view of resource consumption and deployment, the ICPS defender's resource will decrease with the attack going on, while the ICPS attacker's consumption continues to increase. As is evident in the Fig. 5, the higher the ICPS attacker's capability is, the faster the revenue declines. We can add a threshold to control the ICPS attacker's ability to stabilize the payoff within a certain range, but the effect is small and can not change the overall trend of attack revenue. In conclusion, a visible network attack is a war of attrition, a certain degree of the game can bring considerable benefits, but the long-term offensive and defensive battle, will bring harm to both sides.

VI. CONCLUSION

In this paper, a realistic attack-defense model has been proposed in ICPS and we also proposed a novel hybrid game model in order to more realistically capture the real-world interactions between cyber attackers and cyber defenders. Using simulations, we have demonstrated how an optimal attack strategy can be obtained for attackers with different capabilities, using the Nash equilibrium in our game model.

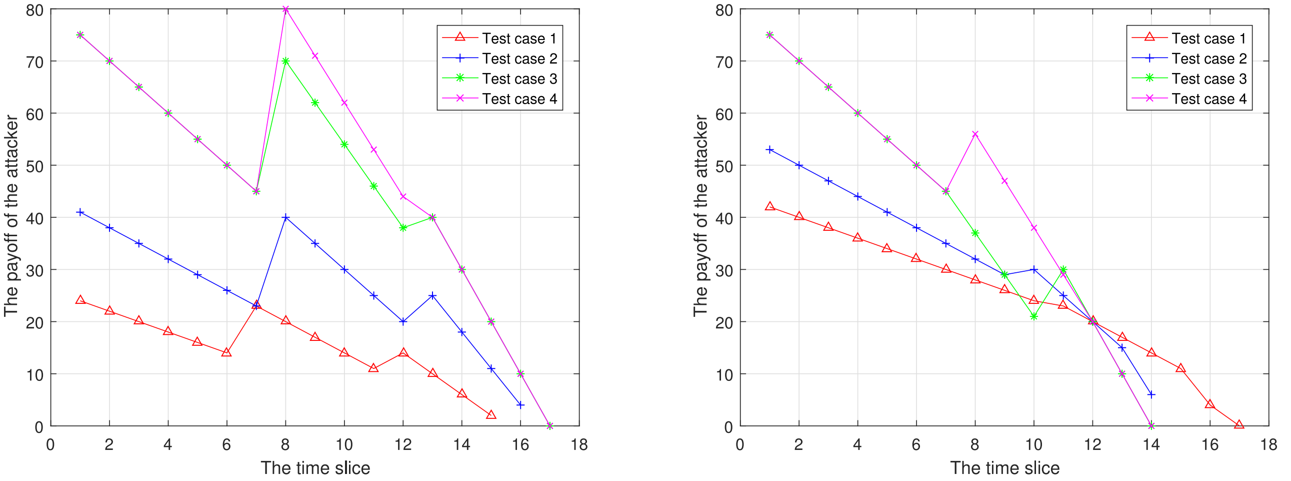
Future research includes extending the evaluation of the proposed game model to systems in our domains such as smart grids and intelligent transportation systems.

APPENDIX

A. PROOF FOR THEOREM 2

Proof: We conclude that there is a mixed-strategy PBE in the one-shot signaling game. In this paper, we show the partial proof process of a mixed strategy PBE under a certain attacker type. The whole process is very complicated. We omit the remainder of the proof process for brevity. The partial proof process is as follows: we discuss the mixed-strategy PBE in type-**M** attacker. Assume Player 1's (attacker) mixed strategy $\bar{\omega} = (\rho_1, \rho_2, \rho_3)$, where ρ_1, ρ_2, and ρ_3 respectively corresponds to the attacker's attack action, anti-honeypot action

[1] www.gambit-project.org



(a) The defender with a fake honeypot

(b) The defender with a honeypot

FIGURE 5. The attacker's payoff in a repeated game with the ICPS defender.

and disguised attack action. Player 2's (ICPS defender) mix strategy is $\bar{\nu} = (o_1, o_2, o_3)$, where o_1, o_2, and o_3 respectively corresponds to the defender's normal service action, fake honeypot action and honeypot action. Once the payoff parameters are set, the game is likely to has strict weak strategies, that is, the corresponding value of ρ or o is 0, which should be abandoned. Here the case where there is no strict weak strategy is discussed. We can calculate the attacker's payoff using the payoffs matrix, which is given by:

$$\begin{aligned} E(u_1) = {} & \rho_1 \left[o_1 (\alpha A_r - \beta A_c) + o_2 (\alpha A_r - \beta A_c) + o_3 \left(-\beta A_p \right.\right. \\ & \left.\left. -\beta A_c)\right] + \rho_2 \left[-o_1 \delta I_c + o_2 \left(I_g - \delta I_p\right) + o_3 (\gamma I_r \right. \\ & \left. -\delta I_c)\right] + \rho_3 [o_1 (\alpha A_r - \beta A_c - E_c) + o_2 (\alpha A_r \\ & - \beta A_c - E_c) + o_3 \left(-\beta A_p - \beta A_c - E_c)\right] \\ = {} & \rho_1 \left[o_1 (\alpha A_r - \beta A_c + \delta I_c) + o_2 \left(\alpha A_r - \beta A_c - I_g \right.\right. \\ & \left. +\delta I_c) + o_3 \left(-\beta A_p - \beta A_c - \gamma I_r + \delta I_c)\right]\right. \\ & + \rho_3 [o_1 (\delta I_c + \alpha A_r - \beta A_c - E_c) + o_2 (\alpha A_r \\ & \left. -\beta A_c - E_c - I_g + \delta I_p\right) + o_3 \left(\delta I_c - \gamma I_r - \beta A_p \right. \\ & -\beta A_c - E_c)] + o_1 (-\delta I_c) + o_2 \left(I_g - \delta I_p\right) \\ & + o_3 (\gamma I_r - \delta I_c) . \end{aligned} \tag{9}$$

Then we calculate the first partial derivative of $E(u_1)$ with respect to ρ_1, ρ_2 and set them as 0s.

$$\begin{cases} \dfrac{\partial E(u_1)}{\partial \rho_1} = o_1 (\alpha A_r - \beta A_c + \delta I_c) + o_2 \left(\alpha A_r - \beta A_c - I_g \right. \\ \qquad \left. + \delta I_p\right) + o_3 (-\beta A_s - \beta A_c - \gamma I_r + \delta I_c) = 0, \\ \dfrac{\partial E(u_1)}{\partial \rho_3} = o_1 (\alpha A_r - \beta A_c - E_c + \delta I_c) + o_2 (\alpha A_r - \beta A_c \\ \qquad \left. - E_c - I_g + \delta I_p\right) + o_3 (-\beta A_s - \beta A_c - E_c \\ \qquad - \gamma I_r + \delta I_c) = 0. \end{cases} \tag{10}$$

Let o_1, o_2, and o_3 be o_1^*, o_2^* and o_3^* if the upper condition is satisfied. Similarly, We can get the defender's payoff using the payoffs matrix, i.e.,

$$\begin{aligned} E(u_2) = {} & o_1 \left[-\rho_1 \alpha D_p + \rho_3 \left(-\alpha D_p - E_c\right)\right] + o_2 \left[\rho_1 \left(-\alpha D_p \right.\right. \\ & \left. -F_c) + \rho_2 \left(F_p - F_c\right) + \rho_3 \left(-\alpha D_p - F_c - E_c\right)\right] \\ & + o_3 \left[\rho_1 (\beta H_r - H_c) + \rho_2 \left(-\gamma H_p - H_c\right) \right. \\ & \left. + \rho_3 (\beta H_r - H_c + E_c)\right] , \\ = {} & o_2 \left[\rho_1 (-F_c) + \rho_2 \left(F_p - F_c\right) + \rho_3 (-F_c)\right] \\ & + o_3 [\rho_1 \left(\beta H_r - H_c + \alpha D_p\right) + \rho_2 \left(-\gamma H_p - H_c\right) \\ & + \rho_3 (\beta H_r - H_c + E_c + \alpha D_p + E_c)] - \rho_1 \alpha D_p \\ & + \rho_3 \left(-\alpha D_p - E_c\right) . \end{aligned} \tag{11}$$

Then we calculate the first partial derivative of $E(u_2)$ with respect to o_2 and o_3 and set them as 0s:

$$\begin{cases} \dfrac{\partial E(u_2)}{\partial o_2} = \rho_1 (-F_c) + \rho_2 \left(F_p - F_c\right) + \rho_3 (-F_c) = 0, \\ \dfrac{\partial E(u_2)}{\partial o_3} = \rho_1 \left(\beta H_r - H_c + \alpha D_p\right) + \rho_2 \left(-\gamma H_p - H_c\right) \\ \qquad + \rho_3 \left(\beta H_r - H_c + E_c + \alpha D_p + E_c\right) = 0. \end{cases} \tag{12}$$

Let ρ_1, ρ_2 and ρ_3 be ρ_1^*, ρ_2^* and ρ_3^* if the upper condition is satisfied. Accordingly, the one-shot game has a mixed-strategy PBE$(\bar{\omega}, \bar{\nu})$ with $\bar{\omega} = (\rho_1^*, \rho_2^*, \rho_3^*)$ and $\bar{\nu} = (o_1^*, o_2^*, o_3^*)$. ■

REFERENCES

[1] G. Marjan, "Dew computing architecture for cyber-physical systems and IoT," *Internet of Things*, vol. 11, Sep. 2020, Art. no. 100186.

[2] S. Pan, T. H. Morris, U. Adhikari, and V. Madani, "Causal event graphs cyber-physical system intrusion detection system," in *Proc. Annu. Cyber Secur. Inf. Intell. Res. Workshop*, Oak Ridge, TN, USA, Jan. 08-10, 2013, pp. 1–4.

[3] W. Yan, Y. Xue, X. Li, and J. Weng, "Integrated simulation and emulation platform for cyber-physical system security experimentation," in *Proc. Int. Conf. High Confidence Netw. Syst.*, Beijing, China, Apr. 17-18, 2012, pp. 81–88.

[4] S. Duan, Q. Zhang, and Y. Cai, "Research on industrial technology innovation strategic alliance based on alliance network: A case study based on three industrial alliances in zhejiang province," in *Proc. Int. Conf. Artif. Intell. Comput. Sci.*, Jul. 12-13, 2019, pp. 835–840.

[5] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, "DeepFed: Federated deep learning for intrusion detection in industrial cyber-physical systems," *IEEE Trans. Ind. Inform.*, Sep. 11, 2020, early access, doi: 10.1109/TII.2020.3023430.

[6] J. Pawlick, E. Colbert, and Q. Zhu, "A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy," *ACM Comput. Surv.*, vol. 52, no. 4, pp. 1–28, Aug. 2017.

[7] I. Kuwatly, M. Sraj, Z. Al Masri, and H. Artail, "A dynamic honeypot design for intrusion detection," in *Proc. IEEE/ACS Int. Conf. Pervasive Services*, Jul. 19-23, 2004, pp. 95–104.

[8] A. Belqruch and A. Maach, "SCADA security using SSH honeypot," in *Proc. Int. Conf. Netw. Inf. Syst. Secur.*, Mar. 27-28, 2019, pp. 1–5.

[9] J. R. Kondra, S. K. Bharti, S. K. Mishra, and K. S. Babu, "Honeypot-based intrusion detection system: A performance analysis," in *Proc. Int. Conf. Comput. Sustain. Global Development*, New Delhi, India, Mar. 16-18, 2016, pp. 2347–2351.

[10] H. Mohammadzadeh, M. Mansoori, and I. Welch, "Evaluation of fingerprinting techniques and a windows-based dynamic honeypot," in *Proc. Australasian Inf. Secur. Conf.*, Jan. 29–Feb. 1, 2013, pp. 59–66.

[11] N. C. Rowe, E. J. Custy, and B. T. Duong, "Defending cyberspace with fake honeypots," *J. Comput.*, vol. 2, no. 2, pp. 25–36, Apr. 2007.

[12] N. Rowe, B. Duong, and E. Custy, "Fake honeypots: A defensive tactic for cyberspace," in *Proc. IEEE Inf. Assurance Workshop*, Jun. 10-11, 2006, pp. 223–230.

[13] C. Kwon, W. Liu, and I. Hwang, "Security analysis for cyber-physical systems against stealthy deception attacks," in *Proc. Amer. Control Conf.*, Washington, DC, USA, Jun. 17-19, 2013, pp. 3344–3349.

[14] L. Xiao, D. Xu, N. B. Mandayam, and H. V. Poor, "Attacker-centric view of a detection game against advanced persistent threats," *IEEE Trans. Mob. Comput.*, vol. 17, no. 11, pp. 2512–2523, Nov. 2018.

[15] Q. D. La, T. Q. Quek, J. Lee, S. Jin, and H. Zhu, "Deceptive attack and defense game in honeypot-enabled networks for the Internet of Things," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 1025–1035, Dec. 2016.

[16] W. Li, Z. Su, K. Zhang, A. Benslimane, and D. Fang, "Defending malicious check-in using big data analysis of indoor positioning system: An access point selection approach," *IEEE Trans. Netw. Sci. Eng.*, Aug. 5, 2020, early access, doi: 10.1109/TNSE.2020.3014384.

[17] W. Li, Z. Su, R. Li, K. Zhang, and Q. Xu, "Abnormal crowd traffic detection with crowdsourcing-based RSS fingerprint position in heterogeneous communications networks," *IEEE Trans. Netw. Sci. Eng.*, Aug. 5, 2020, early access, doi: 10.1109/TNSE.2020.3014380.

[18] Z. Su, Y. Wang, Q. Xu, and N. Zhang, "LVBS: Lightweight vehicular blockchain for secure data sharing in disaster rescue," *IEEE Trans. Dependable Secur. Comput.*, early access, Mar. 13, 2020, doi: 10.1109/TDSC.2020.2980255.

[19] M. M. Pai, A. Roth, and J. Ullman, "An antifolk theorem for large repeated games," *ACM Trans. Econ. Comput.*, vol. 5, no. 2, pp. 1–20, Oct. 2016.

[20] N. Krawetz, "Anti-honeypot technology," *IEEE Secur. Priv*, vol. 2, no. 1, pp. 76–79, Jan. 2004.

[21] J. Lin, P. Liu, and J. Jing, "Using signaling games to model the multi-step attack-defense scenarios on confidentiality," in *Proc. Int. Conf. Decis. Game Theory Secur.*, Budapest, Hungary, Nov. 5-6, 2012, pp. 118–137.

[22] Q. D. La, T. Q. Quek, and J. Lee, "A game theoretic model for enabling honeypots in IoT networks," in *Proc. IEEE Int. Conf. Commun.*, May 23-27, 2016, pp. 1–6.

[23] K. Wang, S. Du, M. A. Maharjan, and Y. Sun, "Strategic honeypot game model for distributed denial of service attacks in the smart grid," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2474–2482, Feb. 2017.

[24] B. Edwards, A. Furnas, S. Forrest, and R. Axelrod, "Strategic aspects of cyberattack, attribution, and blame," *Proc. Nat. Acad. Sci. U.S.A.*, vol. 114, no. 11, pp. 2825–2830, Jan. 2017.

[25] J. Uitto, S. Rauti, S. Laurén, and V. Leppänen, "A survey on anti-honeypot and anti-introspection methods," in *Proc. World Conf. Inf. Syst. Technologies*, Apr. 11-13, 2017, pp. 125–134.

[26] C. Huang, E. Maiorana, J. Han, X. Zhang, and J. Liu, "Automatic identification of honeypot server using machine learning techniques," *Secur. Commun. Netw.*, vol. 2019, no. 5, pp. 1–8, Jul. 2019.

[27] D. Fudenberg and K. He, "Payoff information and learning in signaling games," *Games Econ. Behav.*, vol. 120, pp. 96–120, Dec. 2019.

[28] O. Baskov, "Equilibrium payoffs in repeated two-player zero-sum games of finite automata," *Int. J. Game Theory*, vol. 48, no. 8, pp. 423–431, Jun. 2018.

[29] T. Iimura and T. Watanabe, "Pure strategy equilibrium in finite weakly unilaterally competitive games," *Int. J. Game Theory*, vol. 45, pp. 719–729, Jun. 2015.

[30] Y. Han and Y. Deng, "A novel matrix game with payoffs of maxitive belief structure," *Int. J. Intell. Syst.*, vol. 34, no. 4, pp. 690–706, Nov. 2019.

[31] F. Forges, "Note on nash equilibria in infinitely repeated games with incomplete information," *Int. J. Game Theory*, vol. 13, no. 3, pp. 179–187, Sep. 1984.

[32] J. Moura and D. Hutchison, "Game theory for multi-access edge computing: Survey, use cases, and future trends," *IEEE Commun. Surv. Tut.*, vol. 21, no. 1, pp. 260–288, Aug. 2019.

[33] K. Wang, M. Du, D. Yang, C. Zhu, J. Shen, and Y. Zhang, "Game-theory-based active defense for intrusion detection in cyber-physical embedded systems," *ACM Trans. Embed. Comput. Syst.*, vol. 16, no. 18, pp. 1–21, Oct. 2016.

[34] Y. Zhao, X. He, and D. Zhou, "Optimal joint control and triggering strategies against denial of service attacks: A zero-sum game," *IET Control Theory Appl.*, vol. 11, pp. 2352–2360, May 2017.

[35] M. Zandebasiri *et al.*, "An incomplete information static game evaluating community-based forest management in zagros, iran," *Sustainability*, vol. 12, no. 5, 2020, Art. no. 1750.

[36] C. Ma, D. Yau, X. Lou, and N. Rao, "Markov game analysis for attack-defense of power networks under possible misinformation," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1676–1686, May 2013.

BEIBEI LI (Member, IEEE) received the B.E. degree (awarded Outstanding Graduate) in communication engineering from the Beijing University of Posts and Telecommunications, China, in 2014 and the Ph.D. degree (awarded Full Research Scholarship) from the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, in 2019. He is currently an Associate Professor with the College of Cybersecurity, Sichuan University, China. He was invited as a Visiting Researcher with the Faculty of Computer Science, University of New Brunswick, Canada, from March to August 2018 and also the research group of Networked Sensing and Control, College of Control Science and Engineering, Zhejiang University, China, from February to April 2019.

His research interests include several areas in security and privacy issues on cyber-physical systems (e.g., smart grids, industrial control systems, etc.), with a focus on intrusion detection techniques, artificial intelligence, and applied cryptography. His works have been published in IEEE Transactions on Information Forensics and Security, IEEE Transactions on Industrial Informatics, *ACM Transactions on Cyber-Physical Systems*, IEEE Internet of Things Journal, *IFAC Automatica, Information Sciences*, IEEE ICC, and IEEE GLOBECOM, etc. He is serving or has served as a Publicity Chair, Publication Co-Chair, or a TPC member for several international conferences, including IEEE ICC, IEEE GLOBECOM, IEEE ICNC, IEEE ATC, and WCSP, etc.

YUE XIAO is currently working toward the B.E. degree in cybersecurity at the College of Cybersecurity, Sichuan University, Chengdu, China. Her research interests include game theory, industrial cyber-physical system security, artificial intelligence, and intrusion detection technology. Her works have been published at the IEEE International Conference on Communications.

YAXIN SHI is currently working toward the B.E. degree in cybersecurity at the College of Cybersecurity, Sichuan University, Chengdu, China. Her main research interests include honeypots, game theory, cloud computing and big data security, and intrusion detection technology. Her works have been published at the IEEE Conference on Local Computer Networks.

QINGLEI KONG received the B.Eng. degree in communication engineering from the Harbin Institute of Technology, Harbin, China, in 2012, the M.Eng. degree in electronic and information engineering from the Shenzhen Graduate School, Harbin Institute of Technology, Shenzhen, China, in 2015, and the Ph.D. degree from the School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore, in 2018. She used to work at the Cyber Security Cluster, Institute for Infocomm Research, Singapore, and Tencent Security, Shenzhen, as a Research Scientist. She is currently working as a Postdoctoral Researcher with The Chinese University of Hong Kong (CUHK), Shenzhen. Her research interests include applied cryptography, blockchain, VANET, and game theory.

YUHAO WU is currently working toward the B.E. degree in cybersecurity at the College of Cybersecurity, Sichuan University, Chengdu, China. His research interests include cyber-physical system security, online social network security, and artificial intelligence. He has authored or coauthored several papers in IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS and International Conference on Web Information Systems Engineering, etc.

HAIYONG BAO received the Ph.D. degree in computer science from Shanghai Jiao Tong University, Shanghai, China, in 2006. Since March 2011, he has been an Associate Professor with the School of Computer Science and Information Engineering, Zhejiang Gongshang University, China. From June 2014 to May 2015, he was a Postdoctoral Fellow with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. His research interests include secure data aggregation, insider attack detection, and applied cryptography.