Unmanned Systems, Vol. 12, No. 2 (2024) 341–358

DOI: 10.1142/S2301385024410152

UNMANNED SYSTEMS
https://www.worldscientific.com/worldscinet/us

Defense for Advanced Persistent Threat with Inadvertent and Malicious Insider Threats

Ziqin Chen[*], Guanpu Chen[†], Yiguang Hong[*,‡]

[*]*Department of Control Science and Engineering and Shanghai Research Institute for Intelligent Autonomous Systems, Tongji University, Shanghai, P. R. China*

[†]*School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology, Stockholm, Sweden*

In this paper, we propose a game theory framework to solve advanced persistent threat problems, especially considering two types of insider threats: malicious and inadvertent. Within this framework, we establish a unified three-player game model and derive Nash equilibria in response to different types of insider threats. By analyzing these Nash equilibria, we provide quantitative solutions to advanced persistent threat problems pertaining to insider threats. Furthermore, we have conducted a comparative assessment of the optimal defense strategy and corresponding defender's costs between two types of insider threats. Interestingly, our findings advocate a more proactive defense strategy against inadvertent insider threats in contrast to malicious ones, despite the latter imposing a higher burden on the defender. Our theoretical results are substantiated by numerical results, which additionally include a detailed exploration of the conditions under which different insiders adopt risky strategies. These conditions can serve as guiding indicators for the defender when calibrating their monitoring intensities and devising defensive strategies.

Keywords: Security game; advanced persistent threat; insider threats; Nash equilibrium.

1. Introduction

Advanced Persistent Threat (APT), as a new type of cyberattack, has posed significant threats to cybersecurity [1–5]. Typically, APT is executed by well-resourced and well-organized entities and aims to persistently compromise sensitive information from target organizations [6, 7]. To mitigate APT attacks, numerous game-based approaches [8–11] have emerged to provide feasible defense strategies [12–18]. However, most of the existing game-based approaches merely consider defending against external attacks, often neglecting the presence of insider threats.

In fact, statistical results in [19] revealed that the damage caused by insider threats exceeds that inflicted by external attackers, mainly because insiders have privileged access to more sensitive resources than attackers. As such, both academia and industry have placed increasing attention on insider threats in recent years [20–25]. In particular, game-based approaches have been proposed to analyze mutual strategic behaviors between a defender and an insider [26–28]. However, two-player game models in these approaches cannot be directly applied to analyze the coupling relation among the defender, attacker, and insider in APT with insider threats (APT-I). In response to this dilemma, certain efforts have been undertaken in [29–32]. For example, [29] modeled the APT-I problem as a three-player timing game, whereby the defender strategically selects time points to invest defense resources, intending to minimize the APT-I impact at the lowest cost. Hu *et al.* [30] further captured the APTs' distinctive feature of prolonged attack periods with a two-layer game. Specifically, this two-layer game relies on a differential equation for the evolution

Received 17 August 2023; Revised 10 December 2023; Accepted 11 December 2023; Published 29 January 2024. This paper was recommended for publication in its revised form by Special Issue Editors: Jie Chen, Ben M. Chen and Jie Huang.
Email Address: ‡*yghong@iss.ac.cn*

of the fraction of the compromised organization, with the defense-attack interaction between the defender and the external attacker, as well as information trading among insiders, being modeled, respectively. However, the above-mentioned APT-I game-based approaches [29, 30] have not adequately considered the types of insider threats during defense process.

In the practical APT-I defense, there are generally two types of insiders: *malicious insiders* and *inadvertent insiders*. Specifically, malicious insiders collaborate with external attackers for personal, financial, or revenge reasons [22]. In this case, the competition between defenders and attackers, the competition between defenders and malicious insiders, and the cooperation between malicious insiders and attackers, need to be considered simultaneously in the APT-I game. This stands in stark contrast to the existing two-player APT game framework in [26–28], which lacks the cooperation between malicious insiders and attackers and serves as a special case in our setting, as confirmed in our theoretical analysis in Sec. 3.2. For *inadvertent insiders*, they act without any malicious intent. However, they may inadvertently cause harm or increase the likelihood of future harm to an organization's confidentiality, integrity, and availability [33–36]. For instance, employees might accidentally leak sensitive data on social media, lose work devices, or fall victim to phishing and other disguised malware attacks [22, 33, 34]. Due to the unintentional nature of inadvertent insiders, predicting their strategies is much more complicated than those of malicious insiders. Moreover, in the APT-I game involving inadvertent insiders, as opposed to those with malicious insiders, there is a lack of cooperation between attackers and inadvertent insiders. However, the strategies of inadvertent insiders are strongly intertwined with those of defenders, which in turn affects the attackers' strategies, consequently leading to different distributions of Nash equilibria compared to those involving malicious insiders. Therefore, the analysis of Nash equilibria in a three-player APT-I game for the two types of insiders is necessary. To the best of our knowledge, no results have been reported on the two types of insider threats in game-based approaches of the APT-I problem.

In this paper, we distinguish between two types of insider threats in the APT-I problem and establish a three player game framework that addresses three key questions: (i) What is the optimal defense strategy to solve the APT-I problem involving inadvertent insider threats or malicious threats? (ii) How do the optimal defense strategies and associated defense costs differ between the two types of insider threats mentioned above? Furthermore, (iii) What strategies should be used for feasible defense if the defender is uncertain about the type of insider threats? The contributions are summarized as follows:

- We establish a three-player game model for the APT-I problem that involves a defender, an attacker, and an insider, with the insider categorized as either malicious or inadvertent. Our proposed model extends the existing two-player game frameworks in [26–28, 37] and the three-player game frameworks that consider only malicious insiders in [29–32].
- We derive Nash equilibria for the proposed three-player game. The derived Nash equilibria serve as acceptable solutions to the APT-I problem with respect to two types of insider threats.
- In addition to providing feasible Nash equilibrium strategies for the defender, we provide practicable suggestions for the defender to achieve effective defense against APT attacks with different types of insider threats.
- The derived Nash equilibria are validated through numerical simulations and experiments. Moreover, we explore the differences in Nash equilibrium strategies between malicious insiders and inadvertent insiders under different levels of monitoring strength. The results indicate that the inadvertent insider is more likely to exhibit risky behaviors than the malicious insider.

The remainder of this paper is organized as follows. Section 2 introduces a three-player game model to solve the APT-I problem associated with two types of insider threats. Section 3 presents the corresponding Nash equilibria. Section 4 discusses Nash equilibrium strategies and the defender's costs under different types of insider threats. Section 5 conducts numerical simulations to verify the derived Nash equilibria. Finally, Sec. 6 concludes this paper.

2. Problem Formulation

Consider a scenario where an organization faces joint threats from an external attacker and an insider, as depicted in Fig. 1. The organization comprises a resource server, a defender, and an insider. The resource server, used for storing sensitive data, can be accessed by both the defender and the insider to meet business needs. The insider is classified as either malicious or inadvertent. A malicious insider may exploit its access to sell sensitive information or provide a backdoor for an attacker. If an attacker obtains sensitive information from a malicious insider, it can bypass detection systems like firewalls, authentication controls, and intrusion prevention systems, to rapidly infiltrate the organization and execute malicious activities such as monitoring sensitive operations, stealing private information, or

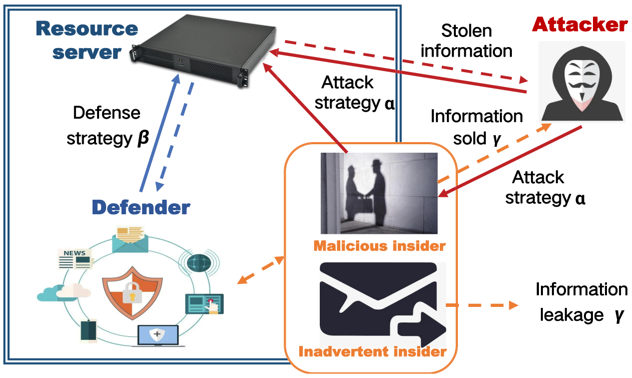


Fig. 1. The diagram of an APT-I model. The dashed line with a single arrow signifies the flow of private data from organization's resources to participants. A solid line with a single arrow represents a direct action of each participant. The blue double-lined frame symbolizes the secured detection system.

injecting ransomware. While an inadvertent insider has no incentive to assist an external attacker, it may unintentionally engage in risky behaviors that lead to information leakage. In summary, this paper is dedicated to addressing the following problem:

APT-I Problem: Consider an APT-affected organization with insider threats. How should the defender adopt optimal defense strategies to minimize the system's continuing losses in response to APT attacks with inadvertent or malicious insider threats?

Remark 2.1. Defense measures include user multi-factor authentication, network security monitoring, and workforce education [2, 35]. Defense strategies can be interpreted as the strength/frequency of the adoption of defense measures. However, defense strategies in most organizations, such as companies, are often constrained by limited computational resources. Therefore, the challenge of an APT-I problem lies in the efficient allocation of finite defense resources to effectively mitigate APT attacks coupled with insider threats.

To solve the APT-I problem, we construct a three-player game model to characterize compromised resources. Hereinafter, each participant in the scenario is referred to as a *player*, and every plausible action taken by a player is denoted as a *strategy*.

2.1. *The evolution model of resource states*

The organization's resource experiences dynamic changes due to the long-term presence of APT attacks with insider threats. The total system resource is normalized to the value of 1. Define $x(t) \in [0,1]$ as the fraction of compromised resources at time t, and thus $1 - x(t)$ denotes the fraction of resources under the defender's protection. The proportion of compromised resources evolves according to the following dynamic [30]:

$$\dot{x}(t) = \alpha(1 - x(t)) - \beta x(t), \tag{1}$$

where an attack strategy is represented by $\alpha \in (0,1]$ and a defense strategy is denoted by $\beta \in (0,1]$. At a given time t, $\alpha(1 - x(t))$ corresponds to the proportion of resources invaded by the attacker and $\beta x(t)$ signifies the fraction of resources recaptured by the defender.

Remark 2.2. Given that the resource state $x(t)$ is not observable in real-time by all players, it is impractical for players to make real-time strategies. In light of this limitations, we employ nonadaptive strategies, which imply that α, β, and γ are determined prior to the organization's deployment. Such nonadaptive strategies can be regarded as a preplanned attack, a defender's routine security assessment, and an insider's steady rate of information leakage. It is noteworthy that the nonadaptive strategy has been recommended as an optimal solution for the periodic APT response problem [29].

Based on the evolution model (1), the resource state at time t satisfies

$$x(t) = \frac{\alpha}{\alpha + \beta}(1 - e^{-(\alpha+\beta)t}), \tag{2}$$

which implies that at the onset (i.e. $x(0) = 0$), organization's resources are completely under the defender's protection. As time tends to infinity, the resource state converges to $\frac{\alpha}{\alpha+\beta}$ at an exponential rate of $e^{-(\alpha+\beta)t}$. This implies two key insights: (1) In the face of a prolonged attack initiated by an attacker, the proportion of compromised resources increases. Nevertheless, due to defense strategies adopted by the defender, complete compromise of organization's resources is prevented. (2) A high value of β leads to a smaller limit point $\frac{\alpha}{\alpha+\beta}$, suggesting that proactive defense strategies can reduce the proportion of compromised resources.

2.2. *The three-player APT-I game*

This subsection establishes a three-player game for the APT-I problem with two types of insider threats. To this end, we introduce the objective functions of each player in the APT-I problem.

Attacker: An external attacker aims to invade and occupy as many resources as possible over an extended period, while minimizing attack risks. Therefore, the attacker's cost function consists of three parts: (i) the risk of detection by a defender, which is reduced by a factor of $(1-\gamma)^2$, where $\gamma \in [0,1]$ is the amount of purchased information from a malicious insider; (ii) the cost of launching attacks, associated with attack strategies $\alpha \in (0,1]$; and (iii) the expense of compensating the malicious insider.

The attacker's average cost function over the time horizon $[0, \infty)$ is given as follows:

$$J_A(\alpha, \beta, \gamma) = \lim_{T \to \infty} \frac{1}{T} \int_0^T p_A(1-\gamma)^2(1-x(t))^2 + q_A\alpha^2(1-x(t))^2 + \gamma^2(1-x(t))^2 dt, \quad (3)$$

where $p_A \in (0,1)$ denotes a unit risk coefficient of being detected and $q_A > 0$ represents a weight of each attack cost.

Unlike the attacker's average cost function used in [30], where the terms $p_A(1-\gamma)^2(1-x(t))^2$ and $\gamma^2(1-x(t))^2$ are ignored, the effect of an insider for the attacker has been considered in our formulation (3).

Remark 2.3. In an APT-I game, the attacker is generally well-funded and highly-motivated, with its primary objectives often including espionage, control, or maintaining prolonged access. The strategic focus of an attacker is predominantly on evading detection rather than on immediate financial gains. Therefore, here we consider the attacker's average cost instead of its profit.

Defender: A defender's primary objective is to minimize the damage caused by both an external attacker and an insider. Its cost function consists of three parts: (i) the loss caused by compromised resources; (ii) the cost associated with launching defenses, which correlates with defense strategies $\beta \in (0,1]$; and (iii) the damage inflicted by insider threats. In the time horizon $[0, \infty)$, the defender's average cost function is given as follows:

$$J_D(\alpha, \beta, \gamma) = \lim_{T \to \infty} \frac{1}{T} \int_0^T p_D(1-\gamma)^2 x^2(t) + q_D\beta^2 x^2(t) + \gamma^2 x^2(t) dt, \quad (4)$$

where $p_D \in (0,1)$ denotes a unit cost coefficient for compromised resources and $q_D > 0$ represents the weight of each defensive cost. Notably, the damage from compromised resources $p_D(1-\gamma)^2 x^2(t)$ is reduced by a factor of $(1-\gamma)^2$ since the cost brought about by an insider $\gamma^2 x^2(t)$ is already considered in the last term on the right-hand side of (4).

Remark 2.4. According to Eq. (4), the defender's average cost function J_D exhibits a positive correlation with the fraction of compromised resources $x(t)$. Hence, minimizing the compromised resources in the organization is equivalent to finding the best response strategy β^* that minimizes J_D.

Malicious insider: The malicious insider's objective is to maximize his profit, which is determined by three factors: (i) the benefit acquired from secured resources; (ii) the financial gain from selling information to an attacker; and iii) the negative risk of being caught by a defender. Specifically, the profit function over the time horizon $[0, \infty)$ is described as follows:

$$J_I(\alpha, \beta, \gamma) = \lim_{T \to \infty} \frac{1}{T} \int_0^T p_I(1-x(t))^2 + \gamma^2(1-x(t))^2 - \left(q_I\gamma + \frac{1}{2}\gamma^2\right) dt, \quad (5)$$

where $p_I \in (0,1)$ represents the proportion of resources owned by an insider and $q_I \geq 0$ denotes the penalty coefficient.

The insider's profit function (5) introduces a risk term $-(q_I\gamma + \frac{1}{2}\gamma^2)$, which implies that the malicious insider suffers a loss when engaging in risky behaviors. This stands against the profit design for an insider in [29], where the risk term is omitted, implying that the malicious insider can abuse his privileges without bearing any cost.

Inadvertent insider: Since the costs of risky behaviors adopted by an inadvertent insider are typically shouldered by the organization rather than the insider itself, this creates no deterrence for such an insider to abstain from risky behaviors or to consider the potential risks brought bout by his actions and behaviors [33–35]. To encourage the inadvertent insider to manage its own risk and deter it from engaging in risky behaviors, we propose a risk budget mechanism applicable to all participating players, including inadvertent insiders. This mechanism can take the same form as (5) and includes three different components: (i) A player who exhibits cautious behaviors can be rewarded by the organization, as characterized by $p_I(1-x(t))^2$; (ii) A player engaging in risky behaviors may face penalties, characterized by $-(q_I\gamma + \frac{1}{2}\gamma^2)$; (iii) In addition, players' risky behaviors can also bring some benefits, such as gaining entertainment or relieving stress, which are depicted by $\gamma^2(1-x(t))^2$. Under this risk budget mechanism, all players will evaluate their own risks before adopting risky behaviors [35]. Therefore, this mechanism can not only encourage the inadvertent insider to behave responsibly but also offload the risk from the organization.

Remark 2.5. The introduced risk budget mechanism can mitigate potential organizational losses/risks caused by the unconscious risky behaviors of inadvertent insiders to a certain degree. More specifically, the risk budget mechanism incorporates the potential losses to inadvertent insiders, which in turn improves their risk awareness and security consciousness. Moreover, by assigning the risk budget mechanism to each player, the organization can limit its risky actions or access scope, thereby reducing the impact of insiders' risky behaviors on organization. Last but not least, this risk budget mechanism allows the organization to monitor and provide feedback on players' risky behaviors. If J_I exceeds some preset J_I', the organization can promptly adopt security measures, such as reinforcing risk management and training.

It is worth noting that the optimal strategies of all players in the APT-I game with inadvertent insiders are not the same as those in the APT-I game with malicious insiders, even if the form of objective functions is similar. This is because there is no direct cooperation between the inadvertent insider and an external attacker. The lack of such cooperation implies that the influence of an inadvertent insider on an attacker is implicit, leading to a fundamental difference between two types of insiders in the APT-I game.

Definition 2.6 (Nash Equilibrium). A strategy pair $(\alpha^*, \beta^*, \gamma^*)$ is defined as a Nash equilibrium if

$$\begin{aligned} J_A(\alpha^*, \beta^*, \gamma^*) &\leq J_A(\alpha, \beta^*, \gamma^*), \\ J_D(\alpha^*, \beta^*, \gamma^*) &\leq J_D(\alpha^*, \beta, \gamma^*), \\ J_I(\alpha^*, \beta^*, \gamma^*) &\geq J_I(\alpha^*, \beta^*, \gamma). \end{aligned}$$

A Nash equilibrium provides a prediction for attacker's and insider's strategies, helping the defender to determine the optimal countermeasures against the APT attack and insider threats. The APT-I problem can be formulated as a unified three-player game as follows:

APT-I Game: Consider three players: an attacker with an attack strategy α, a defender with a defense strategy β, and an insider (either inadvertent or the malicious) with a strategy γ. The goal is to find Nash equilibria $(\alpha^*, \beta^*, \gamma^*)$ that can solve the following three optimization problems simultaneously:

$$\begin{cases} \alpha^* = \min\limits_{\alpha} J_A(\alpha, \beta^*, \gamma^*), \\ \beta^* = \min\limits_{\beta} J_D(\alpha^*, \beta, \gamma^*), \\ \gamma^* = \max\limits_{\gamma} J_I(\alpha^*, \beta^*, \gamma), \end{cases} \tag{6}$$

where the objective functions J_A, J_D, and J_I are given in (3)–(5), respectively.

Note that in the worst-case scenario, the attacker knows the accurate form of $J_A(\alpha, \beta, \gamma)$, and aims to minimize it. In this sense, Nash equilibrium strategies β^* are optimal for the organization's defense, at least in the worst-case scenario. Therefore, if $(\alpha^*, \beta^*, \gamma^*)$ is a Nash equilibrium in an APT-I game, β^* is deemed an acceptable solution to the APT-I problem.

3. Nash Equilibrium Analysis

In this section, we compute Nash equilibria for APT-I game under two types of insiders in the following four scenarios:

- The defender is aware of insider threats:
  (A) A malicious insider exists in the organization;
  (B) An inadvertent insider exists in the organization.
- The defender is unaware of insider threats:
  (C) A malicious insider exists in the organization;
  (D) An inadvertent insider exists in the organization.

3.1. *The defender is aware of insider threats*

In Scenarios (A) and (B), the defender has access to insider's strategies, as these strategies are contingent upon the insider's privileges and accesses, all of which are known to the defender.

In Scenario (A), the competition between a defender and both an attacker and a malicious insider, as well as the cooperation between an attacker and a malicious insider is included in the APT-I game. Considering players' objective functions given in (3)–(5), the best response strategy of each player is derived as follows:

Lemma 3.1. *Considering an APT-I game with a known malicious insider, the best response strategies for the defender, attacker, and malicious insider satisfy*

$$\alpha^* = \begin{cases} \dfrac{p_A(1-\gamma)^2 + \gamma^2}{q_A \cdot \beta}, & \dfrac{p_A(1-\gamma)^2 + \gamma^2}{q_A \cdot \beta} < 1, \\ 1, & \dfrac{p_A(1-\gamma)^2 + \gamma^2}{q_A \cdot \beta} \geq 1. \end{cases} \tag{7}$$

$$\beta^* = \begin{cases} \dfrac{p_D(1-\gamma)^2 + \gamma^2}{q_D \cdot \alpha}, & \dfrac{p_D(1-\gamma)^2 + \gamma^2}{q_D \cdot \alpha} < 1, \\ 1, & \dfrac{p_D(1-\gamma)^2 + \gamma^2}{q_D \cdot \alpha} \geq 1. \end{cases} \tag{8}$$

$$\gamma^* = \begin{cases} 1, & \left(\dfrac{\beta}{\alpha+\beta}\right)^2 - q_I > \dfrac{1}{2}, \\ 1 \text{ or } 0, & \left(\dfrac{\beta}{\alpha+\beta}\right)^2 - q_I = \dfrac{1}{2}, \\ 0, & \left(\dfrac{\beta}{\alpha+\beta}\right)^2 - q_I < \dfrac{1}{2}. \end{cases} \tag{9}$$

Proof. See Appendix A. □

Lemma 3.1 implies that the best response strategy of each player is affected by the strategies of all other players. According to the best response strategies of players in (7)–(9), we can derive the effective Nash equilibrium strategy for each player, which will be presented in Theorem 3.5. In particular, the best response strategy of the insider in (9) is either 1 or 0 under the condition $(\frac{\beta}{\alpha+\beta})^2 - q_I = \frac{1}{2}$. The choice of which will be determined by the derived Nash equilibrium.

Remark 3.2. Note that $\arg\min_{\gamma\in[0,1]} J_I(\alpha, \beta, \gamma) \subseteq \{0, 1\}$ results in $\gamma^* \in \{0, 1\}$, suggesting that the malicious insider can either sell all of information or none at all.

In Scenario (B), since the inadvertent insider has no intention of selling information to the attacker, there is no cooperation between an attacker and an inadvertent insider. Therefore, the attacker's objective function becomes $J_A(\alpha, \beta, 0)$. With this understanding, the best response strategy for each player is derived as follows:

Lemma 3.3. *Considering an APT-I game with a known inadvertent insider, the best response strategies for the defender, attacker, and inadvertent insider satisfy*

$$\alpha^* = \begin{cases} \dfrac{p_A}{q_A \cdot \beta}, & \dfrac{p_A}{q_A \cdot \beta} < 1, \\ 1, & \dfrac{p_A}{q_A \cdot \beta} \geq 1. \end{cases} \tag{10}$$

$$\beta^* = \begin{cases} \dfrac{p_D(1-\gamma)^2 + \gamma^2}{q_D \cdot \alpha}, & \dfrac{p_D(1-\gamma)^2 + \gamma^2}{q_D \cdot \alpha} < 1, \\ 1, & \dfrac{p_D(1-\gamma)^2 + \gamma^2}{q_D \cdot \alpha} \geq 1. \end{cases} \tag{11}$$

$$\gamma^* = \begin{cases} 1, & \left(\dfrac{\beta}{\alpha+\beta}\right)^2 - q_I > \dfrac{1}{2}, \\ 1 \text{ or } 0, & \left(\dfrac{\beta}{\alpha+\beta}\right)^2 - q_I = \dfrac{1}{2}, \\ 0, & \left(\dfrac{\beta}{\alpha+\beta}\right)^2 - q_I < \dfrac{1}{2}. \end{cases} \tag{12}$$

Proof. The lemma can be obtained following the same line of reasoning of Lemma 3.1. □

Lemma 3.3 implies that the best response strategy of the inadvertent insider influences that of the defender, which in turn affects the attacker's best response strategy.

Remark 3.4. From (9) and (12), it can be seen that when the penalty coefficient $q_I > (\frac{\beta}{\alpha+\beta})^2 - \frac{1}{2}$, the insider prefers to choose risk-averse strategy, i.e. $\gamma^* = 0$. This implies that a large risk coefficient can prevent the risky behaviors of both malicious and inadvertent insiders.

For the sake of notations simplicity, we denote $r_A = \frac{p_A}{q_A}$, $r_D = \frac{p_D}{q_D}$, and

$$\varepsilon = \frac{1}{\sqrt{\frac{1}{r_D}\left(\frac{1}{\sqrt{1/2+q_I}} - 1\right)}}.$$

By using (7)–(9) and (10)–(12), we summarize the effective Nash equilibrium for the APT-I game with two types of known insiders in Theorem 3.5.

Theorem 3.5. *When the defender is aware of insider threats, Nash equilibria (corresponding to $\gamma^* = 1$) for the APT-I game with a malicious insider (Scenario (A)) are summarized as follows:*

$$\begin{cases} \left(\dfrac{r_D}{p_D \beta_A^*}, \beta_A^*, 1\right), & \text{if } \dfrac{r_A}{p_A} = \dfrac{r_D}{p_D} \leq 1 \quad \text{and} \\ \quad q_I \leq \left(\dfrac{1}{\frac{r_A}{p_A}+1}\right)^2 - \dfrac{1}{2}, \\ \left(\dfrac{r_A}{p_A}, 1, 1\right), & \text{if } \dfrac{r_A}{p_A} \leq 1, \quad \dfrac{r_A}{p_A} < \dfrac{r_D}{p_D}, \quad \text{and} \\ \quad q_I \leq \left(\dfrac{1}{\frac{r_A}{p_A}+1}\right)^2 - \dfrac{1}{2}, \end{cases}$$

where $\beta_A^* \in [\varepsilon\sqrt{p_D}, 1]$. Nash equilibria (corresponding to $\gamma^* = 1$) for the APT-I game with an inadvertent insider (Scenario (B)) are given as follows:

$$\begin{cases} \left(\dfrac{r_D}{p_D \beta_B^*}, \beta_B^*, 1\right), & \text{if } r_A = \dfrac{r_D}{p_D} \leq 1 \quad \text{and} \\ \quad q_I \leq \left(\dfrac{1}{r_A+1}\right)^2 - \dfrac{1}{2}, \\ (r_A, 1, 1), & \text{if } r_A \leq 1, \quad r_A < \dfrac{r_D}{p_D}, \quad \text{and} \\ \quad q_I \leq \left(\dfrac{1}{r_A+1}\right)^2 - \dfrac{1}{2}, \end{cases}$$

where $\beta_B^* \in [\varepsilon\sqrt{p_D}, 1]$. Moreover, Nash equilibria (corresponding to $\gamma^* = 0$) for the APT-I game are given by

$$\begin{cases} \left(\dfrac{r_D}{\beta^*}, \beta^*, 0\right), & \text{if } r_A = r_D \leq 1 \quad \text{and} \\ \quad q_I > \left(\dfrac{1}{r_A+1}\right)^2 - \dfrac{1}{2}, \\ \text{where } \beta^* \in [r_D, 1]; \\ \left(\dfrac{r_D}{\beta^*}, \beta^*, 0\right), & \text{if } r_A = r_D \leq 1 \quad \text{and} \\ \quad q_I \leq \left(\dfrac{1}{r_A+1}\right)^2 - \dfrac{1}{2}, \\ \text{where } \beta^* \in [r_D, \epsilon], \\ (r_A, 1, 0), & \text{if } r_A \leq 1, \quad r_A < r_D, \quad \text{and} \\ \quad q_I \leq \left(\dfrac{1}{r_A+1}\right)^2 - \dfrac{1}{2}, \\ (1, r_D, 0), & \text{if } r_D \leq 1, \quad r_D < r_A, \\ (1, 1, 0), & \text{if } r_A > 1, \quad r_D > 1. \end{cases} \tag{13}$$

Proof. See Appendix B. □

The Nash equilibria (corresponding to $\gamma* = 1$) in Theorem 3.5 are summarized in Table 1, which includes two kinds of Nash equilibria. The first kind belongs to a continuous set and the second one is a singular point. The Nash equilibria (corresponding to $\gamma* = 0$) in Theorem 3.5 are summarized in Table 2.

Table 1. Different Nash equilibria in Scenarios (A) and (B).

The defender is aware of insider threats						
Types	Malicious insider (Scenario (A))			Inadvertent insider (Scenario (B))		
	System configurations		Nash equilibria	System configurations		Nash equilibria
First	$\frac{r_A}{p_A} = \frac{r_D}{p_D} \leq 1$	$q_I \leq (\frac{1}{\frac{r_A}{p_A}+1})^2 - \frac{1}{2}$	$\left(\frac{r_D}{p_D \beta_A^*}, \beta_A^*, 1\right)$ with $\beta_A^* \in [\varepsilon\sqrt{p_D}, 1]$	$r_A = \frac{r_D}{p_D} \leq 1$	$q_I \leq (\frac{1}{r_A+1})^2 - \frac{1}{2}$	$\left(\frac{r_D}{p_D \beta_B^*}, \beta_B^*, 1\right)$ with $\beta_B^* \in [\varepsilon\sqrt{p_D}, 1]$
Second	$\frac{r_A}{p_A} \leq 1,\ \frac{r_A}{p_A} < \frac{r_D}{p_D}$	$q_I \leq (\frac{1}{\frac{r_A}{p_A}+1})^2 - \frac{1}{2}$	$\left(\frac{r_A}{p_A}, 1, 1\right)$	$r_A \leq 1,\ r_A < \frac{r_D}{p_D}$	$q_I \leq (\frac{1}{r_A+1})^2 - \frac{1}{2}$	$(r_A, 1, 1)$

Table 5 implies that the defender's Nash equilibrium strategies β^* in response to malicious insider threats are not consistently identical to those relative to inadvertent insider threats. Therefore, adopting different defense strategies for responding to different types of insider threats enhances the specificity and effectiveness of APT-I defenses.

3.2. *The defender is unaware of insider threats*

In Scenarios (C) and (D), the defender is unaware of any strategies of the insider, and thus the objective function of the defender becomes $J_D(\alpha, \beta, 0)$. While the defender lacks information about insiders, the Nash equilibrium strategy is not consistent in response to different types of insider threats. This is because the insider's strategy affects the attacker's strategy, which further influences the defender's strategies.

In Scenario (C), the best response strategies of all three players are determined by (3), $J_D(\alpha, \beta, 0)$, and (5), which are given as follows:

Lemma 3.6. *Considering an APT-I game with a unknown malicious insider, the best response strategies for the defender, attacker, and malicious insider satisfy*

$$\alpha^* = \begin{cases} \dfrac{p_A(1-\gamma)^2+\gamma^2}{q_A \cdot \beta}, & \dfrac{p_A(1-\gamma)^2+\gamma^2}{q_A \cdot \beta} < 1, \\ 1, & \dfrac{p_A(1-\gamma)^2+\gamma^2}{q_A \cdot \beta} \geq 1. \end{cases} \tag{14}$$

$$\beta^* = \begin{cases} \dfrac{p_D}{q_D \cdot \alpha}, & \dfrac{p_D}{q_D \alpha} < 1, \\ 1, & \dfrac{p_D}{q_D \alpha} \geq 1. \end{cases} \tag{15}$$

$$\gamma^* = \begin{cases} 1, & \left(\dfrac{\beta}{\alpha+\beta}\right)^2 - q_I > \dfrac{1}{2}, \\ 1 \text{ or } 0, & \left(\dfrac{\beta}{\alpha+\beta}\right)^2 - q_I = \dfrac{1}{2}, \\ 0, & \left(\dfrac{\beta}{\alpha+\beta}\right)^2 - q_I < \dfrac{1}{2}. \end{cases} \tag{16}$$

Proof. The lemma can be obtained following the same line of reasoning of Lemma 3.1. □

From (14)–(16), the malicious insider's strategy influences the attacker's best response strategy, which further influences the defender's best response strategy.

In scenario (D), $J_A(\alpha, \beta, 0)$, $J_D(\alpha, \beta, 0)$, and (5) determine the best response strategies for three players:

Lemma 3.7. *Considering an APT-I game with a unknown inadvertent insider, the best response strategies for the defender, attacker, and inadvertent insider satisfy*

$$\alpha^* = \begin{cases} \dfrac{p_A}{q_A \cdot \beta} & \dfrac{p_A}{q_A \cdot \beta} \leq 1, \\ 1 & \dfrac{p_A}{q_A \cdot \beta} > 1. \end{cases} \tag{17}$$

$$\beta^* = \begin{cases} \dfrac{p_D}{q_D \cdot \alpha} & \dfrac{p_D}{q_D \cdot \alpha} \leq 1, \\ 1 & \dfrac{p_D}{q_D \cdot \alpha} > 1. \end{cases} \tag{18}$$

$$\gamma^* = \begin{cases} 1, & \left(\dfrac{\beta}{\alpha+\beta}\right)^2 - q_I > \dfrac{1}{2}, \\ 1 \text{ or } 0, & \left(\dfrac{\beta}{\alpha+\beta}\right)^2 - q_I = \dfrac{1}{2}, \\ 0, & \left(\dfrac{\beta}{\alpha+\beta}\right)^2 - q_I < \dfrac{1}{2}. \end{cases} \tag{19}$$

Proof. The lemma can be obtained following the same line of reasoning of Lemma 3.1. □

It can be seen that the best response strategies of players are consistent with those in two-player static APT game [30], which is indeed a special case for our setting.

According to (14)–(16) and (17)–(19), we present effective Nash equilibria of the APT-I game with two types of unknown insiders in Theorem 3.8:

Theorem 3.8. *When the defender is unaware of insider threats, the Nash equilibria* (*corresponding to* $\gamma^* = 1$) *for the*

Table 2. Different Nash equilibria in Scenarios (C) and (D).

The defender is unaware of insider threats						
Types	Malicious insider (Scenario (C))			Inadvertent insider (Scenario (D))		
	System configurations		Nash equilibria	System configurations		Nash equilibria
First	$\frac{r_A}{p_A} = r_D \leq 1$	$q_I \leq (\frac{1}{\frac{r_A}{p_A}+1})^2 - \frac{1}{2}$	$\left(\frac{r_D}{\beta_C^*}, \beta_C^*, 1\right)$ with $\beta_C^* \in [\varepsilon, 1]$	$r_A = r_D \leq 1$	$q_I \leq (\frac{1}{r_A+1})^2 - \frac{1}{2}$	$\left(\frac{r_D}{\beta_D^*}, \beta_D^*, 1\right)$, with $\beta_D^* \in [\varepsilon, 1]$.
Second	$\frac{r_A}{p_A} \leq 1,\ \frac{r_A}{p_A} < r_D$	$q_I \leq (\frac{1}{\frac{r_A}{p_A}+1})^2 - \frac{1}{2}$	$\left(\frac{r_A}{p_A}, 1, 1\right)$	$r_A \leq 1,\ r_A < r_D$	$q_I \leq (\frac{1}{r_A+1})^2 - \frac{1}{2}$	$(r_A, 1, 1)$

APT-I game with a malicious insider (Scenario (C)) are summarized as follows:

$$\begin{cases} \left(\dfrac{r_D}{\beta_C^*}, \beta_C^*, 1\right), \quad \text{if } \dfrac{r_A}{p_A} = r_D \leq 1 \quad \text{and} \\ \quad q_I \leq \left(\dfrac{1}{\frac{r_A}{p_A}+1}\right)^2 - \dfrac{1}{2}, \\ \left(\dfrac{r_A}{p_A}, 1, 1\right), \quad \text{if } \dfrac{r_A}{p_A} \leq 1, \quad \dfrac{r_A}{p_A} < r_D, \quad \text{and} \\ \quad q_I \leq \left(\dfrac{1}{\frac{r_A}{p_A}+1}\right)^2 - \dfrac{1}{2}, \end{cases}$$

where $\beta_C^* \in [\varepsilon, 1]$. Nash equilibria (corresponding to $\gamma^* = 1$) for APT-I game with an inadvertent insider (Scenario (D)) are given as follows:

$$\begin{cases} \left(\dfrac{r_D}{\beta_D^*}, \beta_D^*, 1\right), \quad \text{if } r_A = r_D \leq 1 \quad \text{and} \\ \quad q_I \leq \left(\dfrac{1}{r_A+1}\right)^2 - \dfrac{1}{2}, \\ (r_A, 1, 1), \quad \text{if } r_A \leq 1, \quad r_A < r_D, \quad \text{and} \\ \quad q_I \leq \left(\dfrac{1}{r_A+1}\right)^2 - \dfrac{1}{2}, \end{cases}$$

where $\beta_D^* \in [\varepsilon, 1]$. Moreover, Nash equilibria (corresponding to $\gamma^* = 0$) for APT-I game are the same as those in (13) of Theorem 3.5.

Proof. See Appendix C. □

The Nash equilibria (corresponding to $\gamma * = 1$) in Theorem 3.8 are summarized in Table 2, in which β_C^* is not consistently identical to β_D^*. This indicates that even when the defender does not know the existence of insiders, the Nash equilibrium strategy of the defender differs for different types of insider threats. The Nash equilibria (corresponding to $\gamma * = 0$) in Theorem 3.5 are summarized in Table 2.

The Nash equilibrium strategies $\beta_j^*,\ j \in \{A, B, C, D\}$ for the defender in Tables 1 and 2 are recommended as acceptable solutions to the APT-I problem when the insider's Nash equilibrium strategy is $\gamma^* = 1$.

When $\gamma^* = 0$, the three-player APT-I game can be simplified to a two-player APT game. In this case, the Nash equilibria are identical across Scenarios (A)–(D). Therefore, the Nash equilibrium strategies β^* in Table 2 are suggested as acceptable solutions to the APT-I problem with $\gamma^* = 0$. This result aligns with that in the APT game of [30].

As shown in Table 2, the Nash equilibrium strategies α^* and β^* are dependent on the system parameters r_A and r_D. More specifically, if $r_A = r_D \leq 1$, then $\alpha^* \cdot \beta^* = r_A = r_D$. If $r_A < r_D$, the defender expands its defense strategy to $\beta^* = 1$, which implies a greater concern for the cost of uncontrolled resources relative to the attacker. Conversely, if $r_D < r_A$, the attacker expends its strategy to $\alpha^* = 1$ such that it can compromise additional system's resources. If $r_D > 1$ and $r_A > 1$, both the defender and the attacker employ their maximum strategies.

Remark 3.9. We observe that $\gamma^* = 0$ always holds under the system configuration $r_D \leq 1,\ r_D < r_A$ or $r_A > 1,\ r_D > 1$. This is because, under such configuration, $\alpha^* = 1$ always holds, leading to a reduction in the percentage of secure resources $1 - x(t)$ based on (2). From the insider's objective function (5), a low percentage of secure resources means that the profit term $p_I(1 - x(t))^2 + \gamma^2(1 - x(t))^2$ fails to compensate for the risk term $q_I\gamma + \frac{1}{2}\gamma^2$. This leaves the insider with no incentive to engage in risky behaviors,

Table 3. The Nash equilibria in Scenarios (A)–(D) when $\gamma^* = 0$.

System configurations		Nash equilibria
$r_A = r_D \leq 1$	$q_I > (\frac{1}{r_A+1})^2 - \frac{1}{2}$	$\left(\frac{r_D}{\beta^*}, \beta^*, 0\right),\ \beta^* \in [r_D, 1]$
	$q_I \leq (\frac{1}{r_A+1})^2 - \frac{1}{2}$	$\left(\frac{r_D}{\beta^*}, \beta^*, 0\right),\ \beta^* \in [r_D, \varepsilon]$
$r_A \leq 1, r_A < r_D$	$q_I \geq (\frac{1}{r_A+1})^2 - \frac{1}{2}$	$(r_A, 1, 0)$
$r_D \leq 1, r_D < r_A$	—	$(1, r_D, 0)$
$r_A > 1, r_D > 1$	—	$(1, 1, 0)$

February 20, 2024 9:49:10am WSPC/284-US 2441015 ISSN: 2301-3850

i.e. $\gamma^* = 0$ always holds. Therefore, under the system configuration $r_D \le 1,\ r_D < r_A$ or $r_A > 1,\ r_D > 1$, the insider threats can be ignored by the defender. In addition, a high risk coefficient $q_I > (\frac{1}{r_A+1})^2 - \frac{1}{2}$ can also suppress the risk behaviors of insiders.

According to Tables 1–2, the defender can adopt the following defense measures to mitigate its costs: (i) Decrease the weight of the defense action q_D to satisfy either $r_A < r_D$ or $r_D > 1$, which ensures $\beta^* = 1$ and $\alpha^* = r_A$. (ii) Enhance detection capabilities to satisfy $q_I > (\frac{1}{r_A+1})^2 - \frac{1}{2}$, which ensures $\gamma^* = 0$.

4. Discussions and Suggestions

4.1. *Discussions*

In this subsection, we characterize the difference between two types of insider threats in terms of the Nash equilibrium strategy β^* and the cost $J_D(\alpha^*, \beta^*, 1)$ for the defender. Our results show that compared with malicious insider threats, inadvertent insider threats result in a larger value of β^* but a smaller value of J_D.

Comparisons on Nash equilibrium strategies β^*:

For the sake of analysis, we summarize all effective Nash equilibrium strategies under eight system configurations in Table 4.

Table 4 implies that the value of β^* for defending inadvertent insider threats is always larger than that for defending malicious insider threats. Therefore, the defender should employ more active defense strategies (such as increasing the frequency of double user identification, enhancing network security monitoring, and implementing robust employee training programs [2, 35]) to address the APT-I problem with inadvertent insider threats compared with malicious insider threats.

Comparisons on defender's costs $J_D(\alpha^*, \beta^*, 1)$:

(1) *The defender is aware of insider threats*

Given $J_D(\alpha^*, \beta^*, \gamma^*)$, we compute the defender's average cost as follows:

$$J_D(\alpha^*, \beta^*, 1) = (1 + q_D(\beta^*)^2)\left(\frac{\alpha^*}{\alpha^* + \beta^*}\right)^2 = \frac{1}{1 + q_D(\beta^*)^2}, \tag{20}$$

where $\alpha^* \cdot \beta^* = \frac{r_D}{p_D}$ and $\gamma^* = 1$ are obtained from Table 1.

(2)*The defender is unaware of insider threats*

Given $J_D(\alpha^*, \beta^*, 0)$, we compute the defender's average cost as follows:

$$J_D(\alpha^*, \beta^*, 0) = (p_D + q_D(\beta^*)^2)\left(\frac{\alpha^*}{\alpha^* + \beta^*}\right)^2 = \frac{p_D^2}{p_D + q_D(\beta^*)^2}, \tag{21}$$

where $\alpha^* \cdot \beta^* = r_D$ are obtained from Table 2.

According to Table 4, malicious insider threats always increase the value of α^* and decrease the value of β^*. Combining this relationship with (20) and (21), we can see that malicious insider threats impose higher costs on the defender compared to inadvertent insider threats.

4.2. *Suggestions*

The Nash equilibrium strategies β^* in Tables 1–2 are suggested as acceptable solutions to the APT-I problem. According to the theoretical analysis in Secs. 3 and 4.1, we present some practicable suggestions for the defender to mitigate the APT-I problem with two types of insider threats.

- The defender should employ more active defense strategies against inadvertent threats as compared to

Table 4. Nash equilibrium strategies under different system configurations and two types of insiders.

Configurations	Insiders	α^*	β^*	γ^*	Configurations	Insiders	α^*	β^*	γ^*
$\frac{r_A}{p_A} = \frac{r_D}{p_D} \le 1$ and	Inadvertent	r_A	1	1	$\frac{r_A}{p_A} \le 1,\ \frac{r_A}{p_A} < \frac{r_D}{p_D}$ and	Inadvertent	r_A	1	1
$q_I \le (\frac{1}{\frac{r_A}{p_A}+1})^2 - \frac{1}{2}$	Malicious	$[\frac{r_D}{p_D}, \frac{r_D}{\varepsilon\sqrt{p_D^3}}]$ $\uparrow$	$[\varepsilon\sqrt{p_D}, 1]$ $\downarrow$	0	$q_I \le (\frac{1}{\frac{r_A}{p_A}+1})^2 - \frac{1}{2}$	Malicious	$\frac{r_A}{p_A}$ $\uparrow$	1	1
$r_A = \frac{r_D}{p_D} \le 1$ and	Inadvertent	$[\frac{r_D}{p_D}, \frac{r_D}{\varepsilon\sqrt{p_D^3}}]$	$[\varepsilon\sqrt{p_D}, 1]$	1	$r_A \le 1,\ r_A < \frac{r_D}{p_D} \le 1$ and	Inadvertent	r_A	1	1
$q_I \le (\frac{1}{r_A+1})^2 - \frac{1}{2}$	Malicious	1 $\uparrow$	r_D $\downarrow$	0	$q_I \le (\frac{1}{r_A+1})^2 - \frac{1}{2}$	Malicious	$\frac{r_A}{p_A}$ $\uparrow$	1	1
$\frac{r_A}{p_A} = r_D \le 1$ and	Inadvertent	r_A	1	1	$\frac{r_A}{p_A} \le 1,\ \frac{r_A}{p_A} < r_D$ and	Inadvertent	r_A	1	1
$q_I \le (\frac{1}{\frac{r_A}{p_A}+1})^2 - \frac{1}{2}$	Malicious	$[r_D, \frac{r_D}{\varepsilon}]$ $\uparrow$	$[\varepsilon, 1]$ $\downarrow$	1	$q_I \le (\frac{1}{\frac{r_A}{p_A}+1})^2 - \frac{1}{2}$	Malicious	$\frac{r_A}{p_A}$ $\uparrow$	1	1
$r_A = r_D \le 1$ and	Inadvertent	$[r_D, \frac{r_D}{\varepsilon}]$	$[\varepsilon, 1]$	1	$r_A \le 1,\ r_A < r_D$ and	Inadvertent	r_A	1	1
$q_I \le (\frac{1}{r_A+1})^2 - \frac{1}{2}$	Malicious	$[\frac{r_D}{\varepsilon}, 1]$ $\uparrow$	$[r_D, \varepsilon]$ $\downarrow$	0	$q_I \le (\frac{1}{r_A+1})^2 - \frac{1}{2}$	Malicious	$\frac{r_A}{p_A}$ $\uparrow$	1	1

February 20, 2024 9:49:11am WSPC/284-US 2441015 ISSN: 2301-3850 2nd Reading

Table 5. The system configurations of Tables 1 and 2.

Scenarios	Kinds	q_A	Configurations	NEs
A	First	4.55	$\frac{r_A}{p_A} = \frac{r_D}{p_D} = 0.22 \leq 1$	(0.26, 0.84, 1)
	Second	7.14	$\frac{r_A}{p_A} = 0.14 < \frac{r_D}{p_D} = 0.22$	(0.14, 1, 1)
B	First	4.32	$r_A = \frac{r_D}{p_D} = 0.22 \leq 1$	(0.25, 0.89, 1)
	Second	7.14	$r_A = 0.13 < \frac{r_D}{p_D} = 0.22$	(0.13, 1, 1)
C	First	5	$\frac{r_A}{p_A} = r_D = 0.2 \leq 1$	(0.26, 0.76, 1)
	Second	6.67	$\frac{r_A}{p_A} = 0.15 < r_D = 0.2$	(0.15, 1, 1)
D	First	4.75	$r_A = r_D = 0.2 \leq 1$	(0.25, 0.8, 1)
	Second	6.67	$r_A = 0.14 < r_D = 0.2$	(0.14, 1, 1)

malicious ones. The active defense strategies include increasing the strength of security monitoring and the frequency of workforce education.

- When the defender is unaware of insider threats, it is advisable to maintain a high level of monitoring and defense.
- Increase the penalty coefficient to satisfy $q_I > (\frac{1}{r_A+1} - \frac{1}{2}$ and $\gamma^* = 0$. For inadvertent insider threats, the defender can enhance employee training and risk communication, enforce process discipline, and intensify punitive measures [35]. For malicious insiders, the defender can use deception techniques (e.g. Darknets and Honey nets [38]) to increase the malicious insiders' losses when selling information.
- The defender can prejudge whether the condition $r_D \leq 1$, $r_D < r_A$ or $r_D > 1,\ r_A > 1$ is met. If it is met, the defender can ignore insider threats (as $\gamma^* = 0$ always holds) and maintain the same defense strategy as that used in the two-player APT game.

5. Numerical Experiments

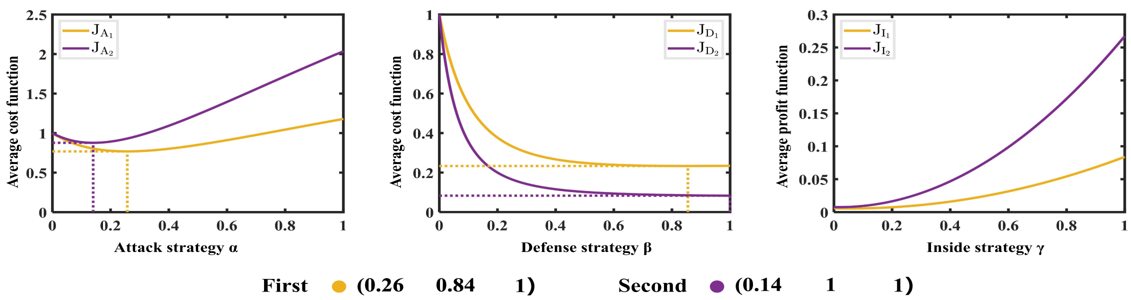
We first verify the Nash equilibria in Tables 1–3. Then, we validate the results in Sec. 4. Finally, we examine the insider's strategies under multiple different values of q_I.

5.1. *The Nash equilibrium verification*

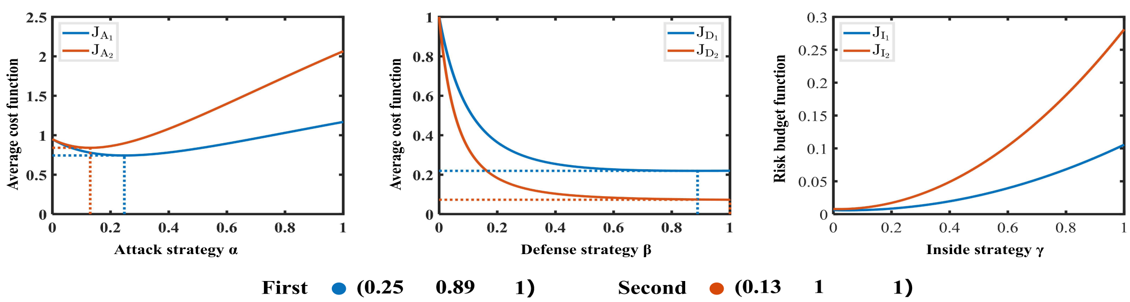
5.1.1. *Verification of Tables* 1 *and* 2

The system configurations are set as $p_A = 0.95$, $p_D = 0.9$, $q_D = 4.5$, $p_I = 0.1$, and $q_I = 0.01$. The values of q_A and theoretical Nash equilibria are given in Table 5.

Figure 2 depicts the average objective function for each player under the system configurations given in Table 1.



(a) The APT-I game with a known malicious insider (Scenario (A))



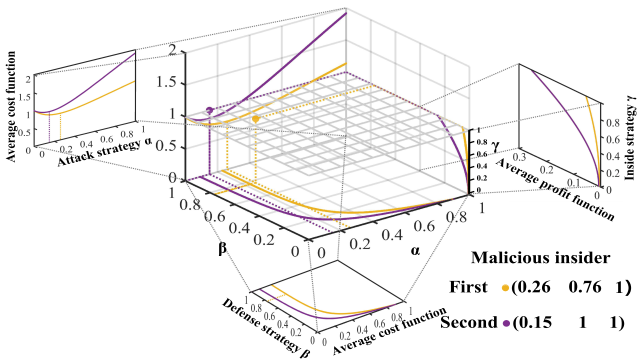
(b) The APT-I game with a known inadvertent insider (Scenario (B))

Fig. 2. Verification of Table 1. In Fig. 2(a), the yellow lines are used to verify the first kind of Nash equilibria under Scenario (A) in Table 5. The purple lines are used to verify the second kind of Nash equilibria under Scenario (A) in Table 5. In Fig. 2(b), the blue lines are used to verify the first kind of Nash equilibria under Scenario (B) in Table 5. The red lines are used to verify the second kind of Nash equilibria under Scenario (B) in Table 5.

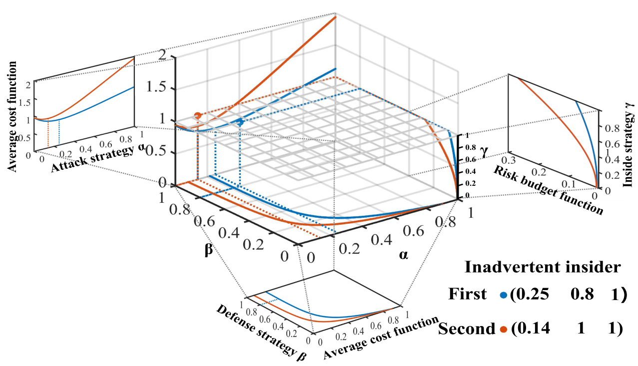
February 20, 2024 9:49:28am WSPC/284-US 2441015 ISSN: 2301-3850 2nd Reading

In Fig. 2(a), the Nash equilibrium $(0.26, 0.84, 1)$ aligns with $(\frac{r_D}{p_D\beta^*}, \beta^*, 1)$, where $\beta^* \in [\varepsilon\sqrt{p_D}, 1]$ and $\varepsilon\sqrt{p_D} = 0.67$. The Nash equilibrium $(0.14, 1, 1)$ aligns with $(\frac{r_A}{p_A}, 1, 1)$. In Fig. 2(b), the Nash equilibrium $(0.25, 0.89, 1)$ is consistent with $(\frac{r_D}{p_D\beta^*}, \beta^*, 1)$, where $\beta^* \in [\varepsilon\sqrt{p_D}, 1]$ and $\varepsilon\sqrt{p_D} = 0.67$. The Nash equilibrium $(0.13, 1, 1)$ is consistent with $(r_A, 1, 1)$.

Figure 3 shows the average objective function for each player under the system configurations in Table 2. In Fig. 3(a), the Nash equilibrium $(0.26, 0.76, 1)$ aligns with $(\frac{r_D}{\beta^*}, \beta^*, 1)$, where $\beta^* \in [\varepsilon, 1]$ and $\varepsilon = 0.71$. The Nash equilibrium $(0.15, 1, 1)$ aligns with $(\frac{r_A}{p_A}, 1, 1)$. In Fig. 3(b), the Nash equilibrium $(0.25, 0.8, 1)$ is consistent with $(\frac{r_D}{\beta^*}, \beta^*, 1)$ when $\beta^* \in [\varepsilon, 1]$ and $\varepsilon = 0.71$. The Nash equilibrium $(0.14, 1, 1)$ is consistent with $(r_A, 1, 1)$.



(a) The APT-I game with an unknown malicious insider (Scenario (C))



(b) The APT-I game with an unknown inadvertent insider (Scenario (D))

Fig. 3. Verification of Table 2. In Fig. 2(a), the yellow lines are used to verify the first kind of Nash equilibria under Scenario (C) in Table 5. The purple lines are used to verify the second kind of Nash equilibria under Scenario (C) in Table 5. In Fig. 2(b), the blue lines are used to verify the first kind of Nash equilibria under Scenario (D) in Table 5. The red lines are used to verify the second kind of Nash equilibria under Scenario (D) in Table 5.

Table 6. The system configurations of Table 2.

q_A	q_D	System configurations		NEs
4.75	4.5	$r_A = r_D = 0.2 \le 1$	$q_I = 0.3$	(0.9, 0.33, 0)
			$q_I = 0.01$	(0.6, 0.5, 0)
6.67	4.5	$r_A = 0.14 < r_D = 0.2$	$q_I = 0.3$	(0.225, 1, 0)
1.9	4.5	$r_D = 0.2 < r_A = 0.5$	$q_I = 0.01$	(1, 0.3, 0)
0.5	0.3	$r_A = 1.9,\ r_D = 3$	$q_I = 0.01$	(1, 1, 0)

Therefore, the minimums of J_D and J_A, and the maximum of J_I in Figs. 2 and 3, correspond with theoretical Nash equilibria listed in Table 5.

5.1.2. *Verification of Table* 2

The system configurations are set as $p_A = 0.95$, $p_D = 0.9$, and $p_I = 0.1$. The remaining system configurations and theoretical Nash equilibria are established in Table 6.

Figure 4 validates Nash equilibria in Table 2, and Fig. 4 also demonstrates that the insider always achieves the largest profit when $\gamma^* = 0$.

5.2. *Discussion validation*

Table 7 directly shows that β^* associated with the malicious threat is never greater than β^* associated with the inadvertent threat.

Figure 5 depicts the defender's average costs J_D under different β^* between malicious insider threats (Scenario (A) or Scenario (C)) and inadvertent insider threats (Scenario (B) or Scenario (D)). The results indicate that malicious insider threats impose a higher cost on the defender compared to inadvertent insider threats.

Furthermore, we also compare two types of insider threats in terms of the attacker's average costs and the insider's average profits. The results are depicted in Fig. 6, which shows that the malicious insider increases the attacker's costs but also incurs greater risk than the inadvertent insider.

5.3. *Risk coefficient examination*

We set a series of risk coefficients, $q_I^k = 0.1 + 0.01 * k$, $k = 0, \ldots, 14$ to examine the insider's Nash equilibrium strategies γ^*. The system configurations are set as $p_A = p_D = 0.8$, $q_A = 4$, and $p_I = 0.1$. The rest of parameters and theoretical Nash equilibria are listed in Table 8.

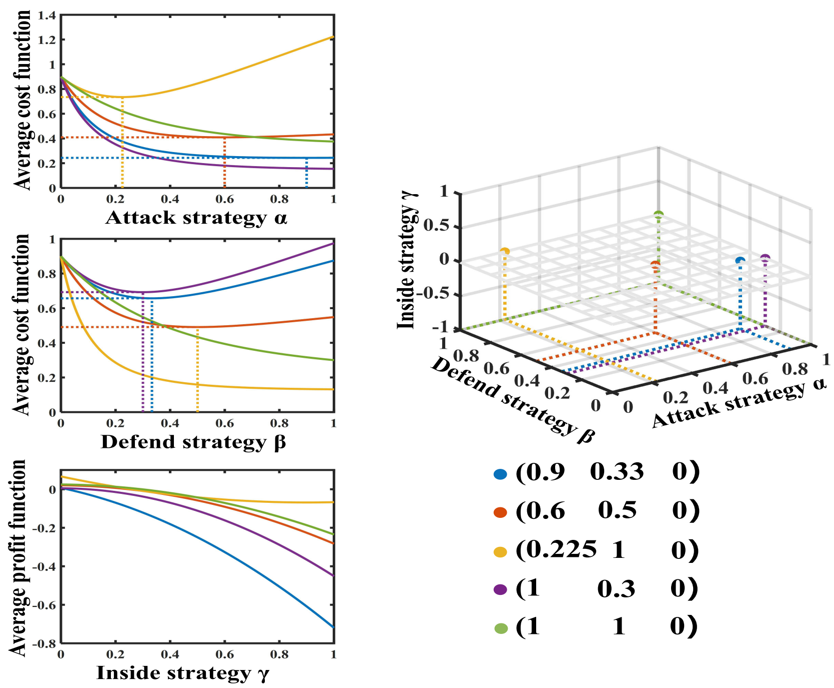
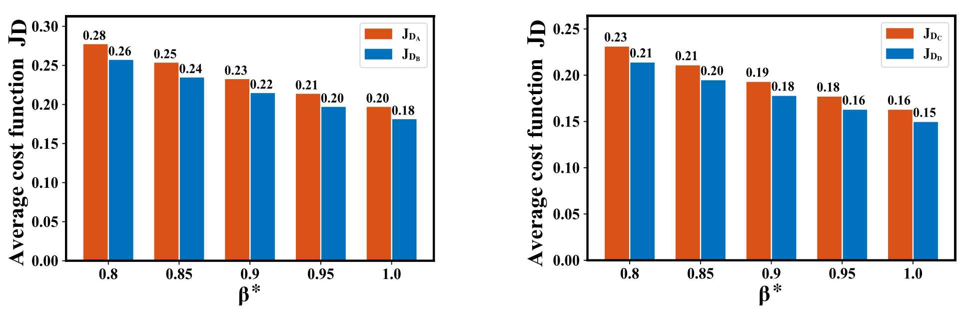


Fig. 4. Verification of Table 2 with $\gamma^* = 0$.

Table 7. The variations of NE strategies under different system configurations.

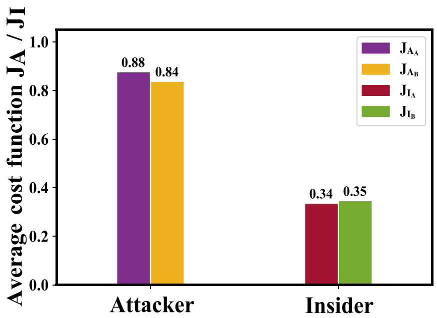
Configurations	Insiders	α^*	β^*	γ^*	Configurations	Insiders	α^*	β^*	γ^*
$\frac{r_A}{p_A} = \frac{r_D}{p_D} = 0.22 \le 1$ and	Inadvertent	0.21	1	1	$\frac{r_A}{p_A} = 0.14 < \frac{r_D}{p_D} = 0.22$ and	Inadvertent	0.13	1	1
$q_I = 0.01 < 0.17$	Malicious	$[0.22, 0.33]$ $\uparrow$	$[0.67, 1]$ $\downarrow$	0	$q_I = 0.01 < 0.27$	Malicious	0.14 $\uparrow$	1	1
$r_A = \frac{r_D}{p_D} = 0.22 \le 1$ and	Inadvertent	$[0.22, 0.33]$	$[0.67, 1]$	1	$r_A = 0.13 < \frac{r_D}{p_D} = 0.22$ and	Inadvertent	0.13	1	1
$q_I = 0.01 < 0.17$	Malicious	1 $\uparrow$	0.2 $\downarrow$	0	$q_I = 0.01 < 0.28$	Malicious	0.14 $\uparrow$	1	1
$\frac{r_A}{p_A} = r_D = 0.2 \le 1$ and	Inadvertent	0.19	1	1	$\frac{r_A}{p_A} = 0.15 < r_D = 0.2$ and	Inadvertent	0.14	1	1
$q_I = 0.01 < 0.19$	Malicious	$[0.2, 0.28]$ $\uparrow$	$[0.71, 1]$ $\downarrow$	1	$q_I = 0.01 < 0.26$	Malicious	0.15 $\uparrow$	1	1
$r_A = r_D = 0.2 \le 1$ and	Inadvertent	$[0.2, 0.28]$	$[0.71, 1]$	1	$r_A = 0.14 < r_D = 0.2$ and	Inadvertent	0.14	1	1
$q_I = 0.01 < 0.19$	Malicious	$[0.28, 1]$ $\uparrow$	$[0.2, 0.71]$ $\downarrow$	0	$q_I = 0.01 < 0.27$	Malicious	0.15 $\uparrow$	1	1



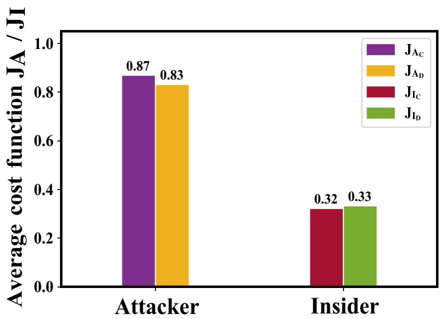
(a) Comparisons of J_D between Scenarios (A) and (B) (b) Comparisons of J_D between Scenarios (C) and (D)

Fig. 5. Comparisons of the defender's average costs under various β^* between two types of insider threats. The red bars represent the values of J_D associated with malicious insider threats, and the blue bars represent those related to inadvertent insider threats.

February 20, 2024 9:50:14am WSPC/284-US 2441015 ISSN: 2301-3850 2nd Reading



(a) Comparisons of J_A and J_I in Scenarios (A) and (B)



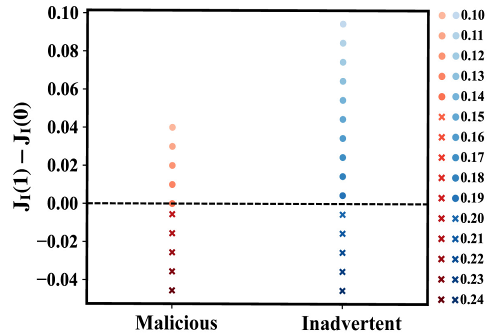
(b) Comparisons of J_A and J_I in Scenarios (C) and (D)

Fig. 6. Comparisons of the attacker's average costs and the insider's average profits between two types of insider threats. The purple bars represent the values of J_A associated with malicious insider threats, while the yellow bars represent those associated with inadvertent insider threats. The red bars represent the values of J_I related to malicious insider threats, and the green bars represent those related to inadvertent insider threats.

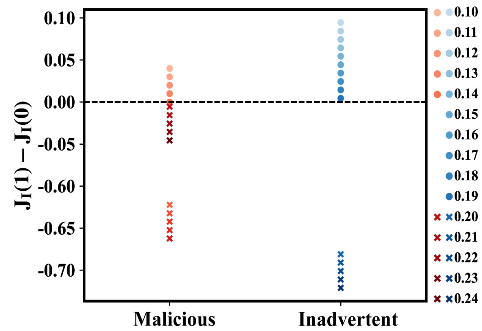
Figure 7 implies that the inadvertent insider is more likely to choose $\gamma^* = 1$ than the malicious insider is. Therefore, the defender should adopt more active monitoring effort to enlarge q_I in response to inadvertent insider threats than malicious insider threats.

Table 8. NE strategies γ^* under different q_I.

Scenarios	q_D	r_D	q_I	NEs
A	4	0.2	$q_I \leq 0.14$	(0.25, 1, 1)
			$0.14 < q_I < 0.19$	(1, 0.2, 0)
			$q_I \geq 0.19$	(0.2, 1, 0)
B	5	0.16	$q_I \leq 0.19$	(0.2, 1, 1)
			$q_I > 0.19$	(1, 0.16, 0)
C	3.2	0.25	$q_I \leq 0.14$	(0.25, 1, 1)
			$0.14 < q_I < 0.19$	None
			$q_I \geq 0.19$	(0.2, 1, 0)
D	4	0.2	$q_I \leq 0.19$	(0.2, 1, 1)
			$q_I > 0.19$	(0.2, 1, 0)



(a) $J_I(1) - J_I(0)$ in Scenarios (A) and (B)



(b) $J_I(1) - J_I(0)$ in Scenarios (C) and (D)

Fig. 7. The Nash equilibrium strategies γ^* under different q_I. When $J_I(1) - J_I(0) \geq 0$, $\gamma^* = 1$, otherwise, $\gamma^* = 0$. The red points represent Nash equilibrium strategies γ^* of the malicious insider and the blue points represent those of the inadvertent insider.

6. Conclusion

In this paper, we proposed a three-player APT-I game model to characterize the coupling relation among the defender, the attacker and the insider in the problem of advanced persistent threat with insider threats. The proposed APT-I game model is applicable to both malicious insider threats and inadvertent insider threats. Through rigorous theoretical analysis, we derived the effective Nash equilibrium for the proposed three-player APT-I game, which serves as an acceptable solution to the problem of advanced persistent threat with insider threats. Moreover, by comparing the defender's Nash equilibrium strategies and the defender's average costs between malicious insider threats and inadvertent insider threats, we provide practicable suggestions for the defender to effectively mitigate APT attacks with different insider threats. Finally, the numerical simulations and experiments verify the derived Nash equilibria. Future work will include dynamic games and Bayesian games for solving the APT-I problem.

Appendix A. Proof of Lemma 3.1

By substituting (2) into (3)–(5), we obtain

$$\begin{cases} J_A(\alpha,\beta,\gamma) = (p_A(1-\gamma)^2 + q_A\alpha^2 + \gamma^2)\left(\dfrac{\beta}{\alpha+\beta}\right)^2, \\ J_D(\alpha,\beta,\gamma) = (p_D(1-\gamma)^2 + q_D\beta^2 + \gamma^2)\left(\dfrac{\alpha}{\alpha+\beta}\right)^2, \\ J_I(\alpha,\beta,\gamma) = (p_I + \gamma^2)\left(\dfrac{\beta}{\alpha+\beta}\right)^2 - \left(q_I\gamma + \dfrac{1}{2}\gamma^2\right). \end{cases}$$

By taking the derivative of $J_A(\alpha,\beta^*,\gamma^*)$, we have

$$\frac{dJ_A(\alpha,\beta^*,\gamma^*)}{d\alpha} = \frac{2(\beta^*)^2}{(\alpha+\beta^*)^3}[q_A\alpha\beta^* - p_A(1-\gamma^*)^2 - (\gamma^*)^2].$$

When $\alpha = 0$, it yields

$$\left.\frac{dJ_A(\alpha,\beta^*,\gamma^*)}{d\alpha}\right|_{\alpha=0} = -\frac{2}{\beta^*}[p_A(1-\gamma^*)^2 + (\gamma^*)^2] < 0,$$

which implies that $J_A(\alpha,\beta^*,\gamma^*)$ is decreasing at the initial attack strategy. Given $\alpha\in(0,1]$, if $\frac{dJ_A}{d\alpha}$ remains negative, then $J_A(\alpha,\beta^*,\gamma^*)$ reaches its minimum value at $\alpha^*=1$. If $\frac{dJ_A}{d\alpha}$ strikes the horizontal axis once and only once at $\bar\alpha = \frac{p_A(1-\gamma^*)^2+(\gamma^*)^2}{q_A\beta^*}$, then the minimum point of $J_A(\alpha,\beta^*,\gamma^*)$ is $\alpha^*=\bar\alpha$ when $\bar\alpha<1$, or $\alpha^*=1$ when $\bar\alpha\geq 1$.

Following a similar argument to the above analysis, we obtain that the derivative of $J_D(\alpha^*,\beta,\gamma^*)$ satisfies

$$\frac{dJ_D(\alpha^*,\beta,\gamma^*)}{d\beta} = \frac{2(\alpha^*)^2}{(\alpha^*+\beta)^3}[q_D\alpha^*\beta - p_D(1-\gamma^*)^2 - (\gamma^*)^2].$$

When $\beta = 0$, it yields

$$\left.\frac{dJ_D(\alpha^*,\beta,\gamma^*)}{d\beta}\right|_{\beta=0} = -\frac{2}{\alpha^*}[p_D(1-\gamma^*)^2 + (\gamma^*)^2] < 0.$$

Therefore, when $\bar\beta = \frac{p_D(1-\gamma^*)^2+(\gamma^*)^2}{q_D\alpha^*} < 1$, the minimum value of $J_D(\alpha^*,\beta,\gamma^*)$ is achieved at $\beta^*=\bar\beta$. Otherwise, the minimum point is $\beta^*=1$.

We proceed to characterize the best response strategy of the insider. The derivative of $J_I(\alpha^*,\beta^*,\gamma)$ satisfies

$$\frac{dJ_I(\alpha^*,\beta^*,\gamma)}{d\gamma} = 2\gamma\left(\frac{\beta^*}{\alpha^*+\beta^*}\right)^2 - q_I - \gamma.$$

The second derivative of $J_I(\alpha^*,\beta^*,\gamma)$ satisfies

$$\frac{d^2J_I(\alpha^*,\beta^*,\gamma)}{d^2\gamma} = 2\left(\frac{\beta^*}{\alpha^*+\beta^*}\right)^2 - 1,$$

which implies that if $2(\frac{\beta^*}{\alpha^*+\beta^*})^2 - 1 \geq 0$, then $J_I(\alpha^*,\beta^*,\gamma)$ is convex, otherwise, it is concave. Moreover, when $\gamma=0$, we have

$$\left.\frac{dJ_I(\alpha^*,\beta^*,\gamma)}{d\gamma}\right|_{\gamma=0} = -q_I \leq 0,$$

which implies that the maximum point of $J_I(\alpha^*,\beta^*,\gamma)$ is either $\gamma^*=0$ or $\gamma^*=1$. The relationship between $J_I(\alpha^*,\beta^*,0)$ and $J_I(\alpha^*,\beta^*,1)$ satisfies

$$J_I(\alpha^*,\beta^*,1) = J_I(\alpha^*,\beta^*,0) + \left(\frac{\beta^*}{\alpha^*+\beta^*}\right)^2 - \frac{1}{2} - q_I.$$

Hence, when $(\frac{\beta^*}{\alpha^*+\beta^*})^2 - q_I < \frac{1}{2}$, the maximum value of $J_I(\alpha^*,\beta^*,\gamma)$ is achieved at $\gamma^*=0$. When $(\frac{\beta^*}{\alpha^*+\beta^*})^2 - q_I > \frac{1}{2}$, we have $\gamma^*=1$. When $(\frac{\beta^*}{\alpha^*+\beta^*})^2 - q_I = \frac{1}{2}$, the maximum point is either $\gamma^*=1$ or $\gamma^*=0$.

Appendix B. Proof of Theorem 3.5

(1) *APT-I game with a known malicious insider*

According to the optimal response strategies in (7)–(9), there exist twelve potential Nash equilibria in the APT-I game. We characterize each of them as follows:

Case 1: $\mathrm{NE}_1 = (\frac{r_A}{\beta^*}, \frac{r_D}{\alpha^*}, 0)$.

The existence of NE_1 is dependent on system configurations r_A and r_D. When $r_A \neq r_D$, NE_1 does not exit. When $r_A = r_D$, we have

$$\frac{r_A}{\beta^*} \leq 1, \quad \frac{r_D}{\alpha^*} \leq 1, \quad \text{and} \quad \left(\frac{\beta^*}{\alpha^*+\beta^*}\right)^2 - q_I \leq \frac{1}{2}.$$

Since $\alpha^* = \frac{r_A}{\beta^*}$ is always valid, we obtain

$$1 \leq \frac{1}{\beta^*} \leq \frac{1}{r_A} \quad \text{and} \quad \frac{1}{\beta^*} \geq \frac{1}{\varepsilon}. \tag{B.1}$$

Given $q_I \geq 0$, $r_D = r_A \leq 1$, and $\varepsilon > r_A$, there are two cases:

- If $q_I > (\frac{1}{r_A+1})^2 - \frac{1}{2}$, then $\frac{1}{\varepsilon} < 1$, and further $\mathrm{NE}_1 = (\frac{r_D}{\beta^*}, \beta^*, 0)$ with $\beta^* \in [r_D, 1]$.
- If $q_I \leq (\frac{1}{r_A+1})^2 - \frac{1}{2}$, then $\frac{1}{\varepsilon} \geq 1$, and further $\mathrm{NE}_1 = (\frac{r_D}{\beta^*}, \beta^*, 0)$ with $\beta^* \in [r_D, \varepsilon]$.

Case 2: $\mathrm{NE}_2 = (\alpha^*,\beta^*,\gamma^*) = (r_A, 1, 0)$.

When $r_A \geq r_D$, the Nash equilibrium NE_2 does not exist. When $r_A < r_D$, we have

$$r_A \leq 1, \quad r_A < r_D, \quad \text{and} \quad \left(\frac{1}{r_A+1}\right)^2 - q_I \leq \frac{1}{2}. \tag{B.2}$$

Therefore, when $r_A \leq 1$, $r_A < r_D$ and $q_I \geq (\frac{1}{r_A+1})^2 - \frac{1}{2}$, $\mathrm{NE}_2 = (r_A, 1, 0)$ holds.

Case 3: $\mathrm{NE}_3 = (\alpha^*,\beta^*,\gamma^*) = (1, r_D, 0)$.

When $r_A \leq r_D$, NE_3 does not exist. When $r_A > r_D$, we have

$$r_D \leq 1, \; r_D < r_A \quad \text{and} \quad \left(\frac{p_D}{p_D+q_D}\right)^2 - q_I \leq \frac{1}{2}.$$

Since $p_D \leq q_D$ yields $q_I \geq (\frac{p_D}{p_D+q_D})^2 - \frac{1}{2}$, $\mathrm{NE}_3 = (1, r_D, 0)$ exists when $r_D \leq 1$ and $r_D < r_A$.

Case 4: $\mathrm{NE}_4 = (\alpha^*, \beta^*, \gamma^*) = (1, 1, 0)$.

When $r_A \leq 1$ or $r_D \leq 1$, NE_4 does not exist. When $r_A > 1$ and $r_D > 1$, $\mathrm{NE}_4 = (1, 1, 0)$ exists.

Case 5: $\mathrm{NE}_5 = (\frac{r_A}{p_A\beta^*}, \frac{r_D}{p_D\alpha^*}, 1)$.

When $\frac{r_A}{p_A} \neq \frac{r_D}{p_D}$, NE_5 does not exist. When $\frac{r_A}{p_A} = \frac{r_D}{p_D}$, we obtain

$$\frac{r_D}{p_D\beta^*} \leq 1, \ \frac{r_D}{p_D\alpha^*} \leq 1, \quad \text{and} \quad \left(\frac{\beta^*}{\alpha^* + \beta^*}\right)^2 - q_I \geq \frac{1}{2}. \tag{B.3}$$

Substituting $\alpha^* = \frac{r_D}{p_D\beta^*}$ into (B.3) yields

$$1 \leq \frac{1}{\beta^*} \leq \frac{p_D}{r_D}, \ \frac{1}{\beta^*} \leq \frac{1}{\varepsilon\sqrt{p_D}}, \quad \text{and}$$

$$q_I \leq \left(\frac{1}{\frac{r_D}{p_D(\beta^*)^2} + 1}\right)^2 - \frac{1}{2}.$$

Based on $q_I \geq 0$, we have $\frac{1}{\varepsilon\sqrt{p_D}} < \frac{p_D}{r_D}$, which involves the following two cases:

- If $q_I > (\frac{1}{\frac{r_D}{p_D}+1})^2 - \frac{1}{2}$, then $\frac{1}{\varepsilon\sqrt{p_D}} < 1$, which implies that NE_5 does not exist.
- If $q_I \leq (\frac{1}{\frac{r_D}{p_D}+1})^2 - \frac{1}{2}$, then $\frac{1}{\varepsilon\sqrt{p_D}} \geq 1$, and further $\mathrm{NE}_5 = (\frac{r_D}{p_D\beta^*}, \beta^*, 1)$ with $\beta^* \in [\varepsilon\sqrt{p_D}, 1]$.

Case 6: $\mathrm{NE}_6 = (\frac{p_A(1-\gamma^*)^2 + (\gamma^*)^2}{q_A\beta^*}, \frac{p_D(1-\gamma^*)^2 + (\gamma^*)^2}{q_D\beta^*}, \gamma^*)$ with $\gamma^* = 1$ or 0.

The existence of NE_6 requires that inequalities (B.1) and (B.3) hold simultaneously. However, $p_D \neq 1$ and $p_A \neq 1$ imply that NE_6 does not exist.

Case 7: $\mathrm{NE}_7 = (\alpha^*, \beta^*, \gamma^*) = (\frac{r_A}{p_A}, 1, 1)$.

When $\frac{r_A}{p_A} \geq \frac{r_D}{p_D}$, NE_7 does not exist. When $\frac{r_A}{p_A} < \frac{r_D}{p_D}$, we have

$$\frac{r_A}{p_A} \leq 1, \ \frac{r_A}{p_A} < \frac{r_D}{p_D}, \quad \text{and} \quad \left(\frac{q_A}{1 + q_A}\right)^2 - q_I \geq \frac{1}{2}. \tag{B.4}$$

Therefore, when $\frac{r_A}{p_A} \leq 1$, $\frac{r_A}{p_A} < \frac{r_D}{p_D}$, and $q_I \leq (\frac{1}{\frac{r_A}{p_A}+1})^2 - \frac{1}{2}$, $\mathrm{NE}_7 = (\frac{r_A}{p_A}, 1, 1)$ exists.

Case 8: $\mathrm{NE}_8 = (\frac{p_A(1-\gamma^*)^2 + (\gamma^*)^2}{q_A\beta^*}, 1, \gamma^*)$ with $\gamma^* = 0$ or 1.

The existence of NE_8 requires inequalities (B.2) and (B.4) hold simultaneously. However, $p_D \neq 1$ and $p_A \neq 1$ imply that NE_8 does not exist.

Case 9: $\mathrm{NE}_9 = (\alpha^*, \beta^*, \gamma^*) = (1, r_D, 1)$.

When $r_A \leq r_D$, NE_9 does not exist. When $r_A > r_D$, we have

$$r_D \leq 1, \ r_D < r_A, \quad \text{and} \quad \left(\frac{p_D}{p_D + q_D}\right)^2 - q_I \geq \frac{1}{2}.$$

Since $p_D \leq q_D$ implies $q_I \leq (\frac{p_D}{p_D+q_D})^2 - \frac{1}{2}$, NE_9 does not exist.

Case 10: $\mathrm{NE}_{10} = (1, r_D, \gamma^*)$ with $\gamma^* = 0$ or 1.

The inequality $q_I = (\frac{p_D}{p_D+q_D})^2 - \frac{1}{2} < 0$ implies that NE_{10} does not exist.

Case 11: $\mathrm{NE}_{11} = (\alpha^*, \beta^*, \gamma^*) = (1, 1, 1)$.

The inequality $q_I \leq -\frac{1}{4}$ implies that NE_{11} does not exist.

Case 12: $\mathrm{NE}_{12} = (1, 1, \gamma^*)$ with $\gamma^* = 0$ or 1.

The inequality $q_I = (\frac{1}{2})^2 - \frac{1}{2} < 0$ implies that NE_{12} does not exist.

(2) *APT-I game with a known inadvertent insider*

According to the best response strategies in (10)–(12), there exist 12 potential Nash equilibria in the APT-I game. Since Cases 1–4 and 9–12 can be obtained following the same line of reasoning as those in Appendix B(1), we omit them here. In addition, due to $p_D \neq 1$, the Nash equilibria in Cases 6 and 8 do not exist. The rest of cases are discussed as follows:

Case 5: $\mathrm{NE}_5 = (\frac{r_A}{\beta^*}, \frac{r_D}{p_D\alpha^*}, 1)$.

When $r_A \neq \frac{r_D}{p_D}$, NE_5 does not exist. When $r_A = \frac{r_D}{p_D}$, we have

$$\frac{r_D}{p_D\beta^*} \leq 1, \quad \frac{r_D}{p_D\alpha^*} \leq 1, \quad \text{and} \quad \left(\frac{\beta^*}{\alpha^* + \beta^*}\right)^2 - q_I \geq \frac{1}{2}.$$

Since the rest of the analysis is similar to the derivations of Case 5 in Appendix B(1), we omit them here and only present the result: when $r_A = \frac{r_D}{p_D} \leq 1$ and $q_I \leq (\frac{1}{r_A+1})^2 - \frac{1}{2}$, $\mathrm{NE}_5 = (\frac{r_D}{p_D\beta^*}, \beta^*, 1)$ exists, where β^* satisfies $\beta^* \in [\varepsilon\sqrt{p_D}, 1]$.

Case 7: $\mathrm{NE}_7 = (\alpha^*, \beta^*, \gamma^*) = (r_A, 1, 1)$.

When $r_A \geq \frac{r_D}{p_D}$, NE_7 does not exist. When $r_A < \frac{r_D}{p_D}$, we obtain

$$r_A \leq 1, \quad r_A < \frac{r_D}{p_D}, \quad \text{and} \quad \left(\frac{1}{r_A + 1}\right)^2 - q_I \geq \frac{1}{2}.$$

Therefore, when $r_A \leq 1, r_A < \frac{r_D}{p_D}$, and $q_I \leq (\frac{1}{r_A+1})^2 - \frac{1}{2}$, $\mathrm{NE}_7 = (r_A, 1, 1)$ exists.

Combining all the Cases given in Appendix B(1) with Cases 5 and 7 given in Appendix B(2), we prove Theorem 3.5.

Appendix C. Proof of Theorem 3.8

(1) *APT-I game with an unknown malicious insider*

Based on the best response strategies in (14)–(16), there are 12 possible Nash equilibria in the APT-I game. Since Cases 1–4 and 9–12 can be obtained following the same line of reasoning as those in Appendix B(1), we omit them here. In addition, due to $p_A \neq 1$, the Nash equilibria in Cases 6 and 8 do not exist. We proceed to discuss the rest of cases.

Case 5: $NE_5 = (\frac{r_A}{p_A\beta^*}, \frac{r_D}{\alpha^*}, 1)$.

When $\frac{r_A}{p_A} \neq r_D$, NE_5 does not exist. When $\frac{r_A}{p_A} = r_D$, we have

$$\frac{r_D}{\beta^*} \leq 1, \quad \frac{r_D}{\alpha^*} \leq 1 \quad \text{and} \quad \left(\frac{\beta^*}{\alpha^* + \beta^*}\right)^2 - q_I \geq \frac{1}{2}.$$

Given $\alpha^* = \frac{r_D}{\beta^*}$, we have

$$1 \leq \frac{1}{\beta^*} \leq \frac{1}{r_D} \quad \text{and} \quad \frac{1}{\beta^*} \leq \frac{1}{\varepsilon}.$$

By using $q_I \geq 0$ and $\varepsilon > r_D$, we consider the following two cases:

- When $q_I > (\frac{1}{r_D+1})^2 - \frac{1}{2}$, we have $\frac{1}{\varepsilon} < 1$, which implies that NE_5 does not exist.
- When $q_I \leq (\frac{1}{r_D+1})^2 - \frac{1}{2}$, we have $\frac{1}{\varepsilon} \geq 1$, which implies that $NE_5 = (\frac{r_D}{\beta^*}, \beta^*, 1)$ exists, where β^* satisfies $\beta^* \in [\varepsilon, 1]$.

Case 7: $NE_7 = (\alpha^*, \beta^*, \gamma^*) = (\frac{r_A}{p_A}, 1, 1)$.

When $\frac{r_A}{p_A} \geq r_D$, NE_7 does not exist. When $\frac{r_A}{p_A} < r_D$, we obtain

$$\frac{r_A}{p_A} \leq 1, \quad \frac{r_A}{p_A} < r_D, \quad \text{and} \quad \left(\frac{1}{\frac{r_A}{p_A} + 1}\right)^2 - q_I \geq \frac{1}{2}.$$

Therefore, when $\frac{r_A}{p_A} \leq 1$, $\frac{r_A}{p_A} < r_D$, and $q_I \leq (\frac{1}{\frac{r_A}{p_A}+1})^2 - \frac{1}{2}$, $NE_7 = (\frac{r_A}{p_A}, 1, 1)$ exists.

(2) *APT-I game with an unknown inadvertent insider*

Based on the best response strategies presented in (17)–(19), there exist 12 possible Nash equilibria in the APT-I game. Since Cases 1–4 and 9–12 can be obtained following the same line of reasoning as those in Appendix B(1), we omit them here. The rest of the cases are discussed as follows:

Case 5: $NE_5 = (\frac{r_A}{\beta^*}, \frac{r_D}{\alpha^*}, 1)$.

When $r_A \neq r_D$, NE_5 does not exist. When $r_A = r_D$, we have

$$\frac{r_D}{\beta^*} \leq 1, \quad \frac{r_D}{\alpha^*} \leq 1, \quad \text{and} \quad \left(\frac{\beta^*}{\alpha^* + \beta^*}\right)^2 - q_I \geq \frac{1}{2}. \tag{C.1}$$

Since the rest of the analysis is similar to the derivations of Case 5 in Appendix C(1), we omit them here and only present the result: when $r_A = r_D \leq 1$ and $q_I \leq (\frac{1}{r_D+1})^2 - \frac{1}{2}$, $NE_5 = (\frac{r_D}{\beta^*}, \beta^*, 1)$ exists, where β^* satisfies $\beta^* \in [\varepsilon, 1]$.

Case 6: $NE_6 = (\frac{r_A}{\beta^*}, \frac{r_D}{\alpha^*}, \gamma^*)$ with $\gamma^* = 1$ or 0.

The existence of NE_6 requires that inequalities (B.1) and (C.1) hold simultaneously. We have $NE_6 = (\frac{r_D}{\varepsilon}, \varepsilon, \gamma^*)$ with $\gamma^* = 1$ or 0 only when $r_A = r_D \leq 1$ and $q_I = (\frac{1}{r_D+1})^2 - \frac{1}{2}$, which is a special case of Cases 1 and 5, and thus can be included in Cases 1 and 5.

Case 7: $NE_7 = (\alpha^*, \beta^*, \gamma^*) = (r_A, 1, 1)$.

When $r_A \geq r_D$, NE_7 does not exist. When $r_A < r_D$, we have

$$r_A \leq 1, \quad r_A < r_D \quad \text{and} \quad \left(\frac{1}{r_A + 1}\right)^2 - q_I \geq \frac{1}{2}. \tag{C.2}$$

Therefore, when $r_A \leq 1$, $r_A < r_D$ and $q_I \leq (\frac{1}{r_A+1})^2 - \frac{1}{2}$, $NE_7 = (r_A, 1, 1)$ exists.

Case 8: $NE_8 = (r_A, 1, \gamma^*)$ with $\gamma^* = 0$ or 1.

The existence of NE_8 requires that inequalities (B.2) and (C.2) hold simultaneously. We have $NE_8 = (r_A, 1, \gamma^*)$ with $\gamma^* = 1$ or 0 only when $r_A \leq 1$, $r_A < r_D$, and $q_I = (\frac{1}{r_A+1})^2 - \frac{1}{2}$, which is a specific case of Cases 2 and 7, and thus can be included in Cases 2 and 7.

Combining Cases 5 and 7 in Appendix C(1) with Cases 5 and 7 in Appendix C(2) and Cases 1–4 and 9–12 in Appendix B(1), we prove Theorem 3.8.

Acknowledgments

This work was supported by the National Key Research and Development Program of China under grant 2022YFA1004700, the Natural Science Foundation of China under grant 62173250, and Shanghai Municipal Science and Technology Major Project under grant 2021SHZDZX0100.

ORCID

Ziqin Chen https://orcid.org/0000-0001-7836-6238
Guanpu Chen https://orcid.org/0000-0003-0698-7910
Yiguang Hong https://orcid.org/0000-0001-9505-8739

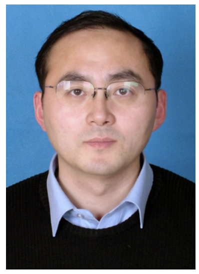
References

[1] C. Tankard, Advanced persistent threats and how to monitor and deter them, *Netw. Secur.* **2011**(8) (2011) 16–19.
[2] A. Lemay, J. Calvet, F. Menet and J. M. Fernandez, Survey of publicly available reports on advanced persistent threat actors, *Comput. Secur.* **72** (2018) 26–59.
[3] A. Alshamrani, S. Myneni, A. Chowdhary and D. Huang, A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities, *IEEE Commun. Surveys Tuts.* **21**(2) (2019) 1851–1877.
[4] T. Zhu, D. Ye, Z. Cheng, W. Zhou and S. Y. Philip, Learning games for defending advanced persistent threats in cyber systems, *IEEE Trans. Syst. Man Cybern. Syst.* **53**(4) (2022) 2410–2422.
[5] T. Halabi, O. A. Wahab, R. Al Mallah and M. Zulkernine, Protecting the internet of vehicles against advanced persistent threats: A Bayesian Stackelberg game, *IEEE Trans. Reliab.* **70**(3) (2021) 970–985.
[6] R. Langner, Stuxnet: Dissecting a cyberwarfare weapon, *IEEE Secur. Priv. Mag.* **9**(3) (2011) 49–51.
[7] C. Tankard, Advanced persistent threats and how to monitor and deter them, *Netw. Secur.* **2011**(8) (2011) 16–19.

[8] Z. Cheng, G. Chen and Y. Hong, Zero-determinant strategy in stochastic Stackelberg asymmetric security game, *Sci. Rep.* **13**(1) (2023) 11308.
[9] X. Li, Z. Peng, W. Zha and J. Chen, Construction of barrier in a three-player pursuit-evasion game, *Unmanned Syst.* **4**(1) (2016) 41–49.
[10] L. Liang, J. Wang and F. Deng, Targets-attackers-defenders game via pairwise outcomes, *Unmanned Syst.* **11**(2) (2023) 133–142.
[11] H. Fu and H. H.-T. Liu, Optimal solution of a target defense game with two defenders and a faster intrude, *Unmanned Syst.* **9**(3) (2021) 247–262.
[12] M. Van Dijk, A. Juels, A. Oprea and R. L. Rivest, Flipit: The game of stealthy takeover, *J. Cryptol.* **26**(4) (2013) 655–713.
[13] J. Chen and Q. Zhu, Security as a service for cloud-enabled internet of controlled things under advanced persistent threats: a contract design approach, *IEEE Trans. Inf. Forensics Secur.* **12**(11) (2017) 2736–2750.
[14] A. A. A. Abass, L. Xiao, N. B. Mandayam and Z. Gajic, Evolutionary game theoretic analysis of advanced persistent threats against cloud storage, *IEEE Access* **5** (2017) 8482–8491.
[15] J. Pawlick and Q. Zhu, Strategic trust in cloud-enabled cyber-physical systems with an application to glucose control, *IEEE Trans. Inf. Forensics Secur.* **12**(12) (2017) 2906–2919.
[16] S. Moothedath, D. Sahabandu, J. Allen, A. Clark, L. Bushnell, W. Lee and R. Poovendran, A game-theoretic approach for dynamic information flow tracking to detect multistage advanced persistent threats, *IEEE Trans. Autom. Control* **65**(12) (2020) 5248–5263.
[17] Z. Cheng, G. Chen and Y. Hong, Single-leader-multiple-followers Stackelberg security game with hypergame framework, *IEEE Trans. Inf. Forensics Secur.* **17** (2022) 954–969.
[18] Z. Cheng, G. Chen and Y. Hong, Misperception influence on zero-determinant strategies in iterated prisoner's dilemma, *Sci. Rep.* **12**(1) (2022) 5174.
[19] M. Kandias, V. Stavrou, N. Bozovic and D. Gritzalis, Proactive insider threat detection through social media: The youtube case, in *Proc. 12th ACM Workshop on Privacy in the Electronic Society* (ACM, 2013), pp. 261–266.
[20] I. Homoliak, F. Toffalini, J. Guarnizo, Y. Elovici and M. Ochoa, Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures, *ACM Comput. Surv.* **52**(2) (2019) 1–40.
[21] R. Kuheli and Sarkar, Assessing insider threats to information security using technical, behavioural and organisational measures, *Inf. Secur. Tech. Rep.* **15**(3) (2010) 112–133.
[22] J. R. Nurse, O. Buckley, P. A. Legg, M. Goldsmith, S. Creese, G. R. Wright and M. Whitty, Understanding insider threat: A framework for characterising attacks, in *Proc. IEEE Security and Privacy Workshops* (IEEE, 2014), pp. 214–228.
[23] I. J. Martinez-Moyano, E. Rich, S. Conrad, D. F. Andersen and T. R. Stewart, A behavioral theory of insider-threat risks: A system dynamics approach, *ACM Trans. Model. Comput. Simul.* **18**(2) (2008) 1–27.
[24] D. C. Le, N. Zincir-Heywood and M. I. Heywood, Analyzing data granularity levels for insider threat detection using machine learning, *IEEE Trans. Netw. Serv. Manag.* **17**(1) (2020) 30–44.
[25] S. Yuan and X. Wu, Deep learning for insider threat detection: Review, challenges and opportunities, *Comput. Secur.* **104** (2021) 102221.
[26] D. Liu, X. Wang and J. Camp, Game-theoretic modeling and analysis of insider threats, *Int. J. Crit. Infrastruct. Prot.* **1** (2008) 75–80.
[27] K. Tang, M. Zhao and M. Zhou, Cyber insider threats situation awareness using game theory and information fusion-based user behavior predicting algorithm, *J. Inf. Comput. Sci.* **8**(3) (2011) 529–545.
[28] C. Joshi, J. R. Aliaga and D. R. Insua, Insider threat modeling: An adversarial risk analysis approach, *IEEE Trans. Inf. Forensics Secur.* **16** (2020) 1131–1142.
[29] X. Feng, Z. Zheng, P. Hu, D. Cansever and P. Mohapatra, Stealthy attacks meets insider threats: A three-player game model, in *Proc. MILCOM IEEE Military Communications Conf.* (IEEE, 2015), pp. 25–30.
[30] P. Hu, H. Li, H. Fu, D. Cansever and P. Mohapatra, Dynamic defense strategy against advanced persistent threat with insiders, in *Proc. IEEE Conf. Computing, Communication and Security* (IEEE, 2015), pp. 747–755.
[31] Z. Liu and L. Wang, Flipit game model-based defense strategy against cyberattacks on scada systems considering insider assistance, *IEEE Trans. Inf. Forensics Secur.* **16** (2021) 2791–2804.
[32] Z. Liu and L. Wang, Defense strategy against load redistribution attacks on power systems considering insider threats, *IEEE Trans. Smart Grid* **12**(2) (2020) 1529–1540.
[33] F. L. Greitzer, J. R. Strozer, S. Cohen, A. P. Moore, D. Mundie and J. Cowley, Analysis of unintentional insider threats deriving from social engineering exploits, in *Proc. IEEE Security and Privacy Workshops* (IEEE, 2014), pp. 236–250.
[34] K. M. Carley and G. P. Morgan, Inadvertent leaks: exploration via agent-based dynamic network simulation, *Comput. Math. Org. Theory* **22**(3) (2016) 288–317.
[35] N. Khan, R. J. Houghton and S. Sharples, Understanding factors that influence unintentional insider threat: a framework to counteract unintentional risks, *Cogn. Technol. Work* **24**(3) (2022) 393–421.
[36] I. Homoliak, F. Toffalini, J. Guarnizo, Y. Elovici and M. Ochoa, Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures, *ACM Comput. Surv.* **52**(2) (2019) 1–40.
[37] W. Tian, M. Du, X. Ji, G. Liu, Y. Dai and Z. Han, Honeypot detection strategy against advanced persistent threats in industrial internet of things: A prospect theoretic game, *IEEE Int. Things J.* **8**(24) (2021) 17372–17381.
[38] N. Virvilis, B. Vanautgaerden and O. S. Serrano, Changing the game: The art of deceiving sophisticated attackers, in *Proc. 6th Int. Conf. IEEE Cyber Conflict* (IEEE, 2014), pp. 87–97.

Ziqin Chen received Ph.D. degree in Automation from the University of Science and Technology of China, Hefei, China, in 2020. She is currently Postdoctoral Associate at the Department of Electrical Computer and Engineering, Clemson University, USA. She was Postdoctoral Fellow at Tongji University, China, from 2020 to 2022. Her current research interests include game theory, distributed optimization, and differential privacy.

Guanpu Chen received B.Sc. degree from the University of Science and Technology of China, Hefei, China, in 2017, and Ph.D. degree from the Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, China, in 2022. He is currently Postdoctoral Researcher with the School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology, Stockholm, Sweden. He was Algorithm Scientist with JD Explore Academy, JD.com Inc, Beijing, in 2022. His research interests include distributed optimization, network games, and cybersecurity.



Yiguang Hong received B.S. and M.S. degrees from Peking University, Beijing, China, in 1987 and 1990, respectively, and Ph.D. degree from the Chinese Academy of Sciences (CAS), Beijing, China, in 1993. He is currently Professor with the Department of Control Science and Engineering and Shanghai Research Institute for Intelligent Autonomous Systems, Tongji University, Shanghai, China. Before October 2020, he was Professor with the Academy of Mathematics and Systems Science, CAS. His current research interests include nonlinear control, multiagent systems, distributed optimization and game, machine learning, and social networks.

Dr. Hong was the recipient of the Guan Zhaozhi Award at the Chinese Control Conference, the Young Author Prize of the IFAC World Congress, the Young Scientist Award of CAS, the Youth Award for Science and Technology of China, and the National Natural Science Prize of China. He was a Board of Governor of IEEE Control Systems Society. He serves as Editor-in-Chief for Control Theory and Technology. He also serves or served as Associate Editor for many journals, including the IEEE TRANSACTIONS ON AUTOMATIC CONTROL, IEEE TRANSACTIONS ON CONTROL OF NETWORK SYSTEMS, and IEEE Control Systems Magazine. He is IEEE Fellow, Fellow of Chinese Association for Artificial Intelligence and Chinese Association of Automation.