7-2022

Strategic signaling for utility control in audit games

Jianan Chen
Purdue University

Qin Hu
Purdue University

Honglu Jiang
The University of Texas Rio Grande Valley

Recommended Citation

Chen, Jianan, Qin Hu, and Honglu Jiang. "Strategic signaling for utility control in audit games." Computers & Security 118 (2022): 102721. https://doi.org/10.1016/j.cose.2022.102721

Strategic Signaling for Utility Control in Audit Games

Jianan Chen, Qin Hu, and Honglu Jiang

***Abstract*—As an effective method to protect the daily access to sensitive data against malicious attacks, the audit mechanism has been widely deployed in various practical fields. In order to examine security vulnerabilities and prevent the leakage of sensitive data in a timely manner, the database logging system usually employs an online signaling scheme to issue an alert when suspicious access is detected. Defenders can audit alerts to reduce potential damage. This interaction process between a defender and an attacker can be modeled as an audit game. In previous studies, it was found that sending real-time signals in the audit game to warn visitors can improve the benefits of the defender. However, the previous approaches usually assume perfect information of the attacker, or simply concentrate on the utility of the defender. In this paper, we introduce a brand-new zero-determinant (ZD) strategy to study the sequential audit game with online signaling, which empowers the defender to unilaterally control the utility of visitors when accessing sensitive data. In addition, an optimization scheme based on the ZD strategy is designed to effectively maximize the utility difference between the defender and the attacker. Extensive simulation results show that our proposed scheme enhances the security management and control capabilities of the defender to better handle different access requests and safeguard the system security in a cost-efficient manner.**

***Index Terms*—Audit game, zero-determinant strategy, utility control, signaling, game theory**

I. Introduction

Since the databases of modern organizations store a large amount of private information, such as personal health and commercial secrets, their sensitivity and economic value make the databases prominent targets of malicious attacks or illegal invasions. Therefore, audit mechanisms are widely deployed, which utilize a combination of manual operations and automated methods to detect and deter attackers. Currently, the audit mechanism has become a typical method employed by many organizations with a large amount of sensitive information, such as hospitals, banks, and search engine companies, to prevent information security attacks [1].

Despite the extensive employment of audit mechanisms, information leakage and illegal transactions caused by various attacks are still widespread according to a recent report [2]. This concern can be even worse as some internal malicious users can abuse their authority to launch attacks. These vicious attacks from inside are less likely to be audited because they have certain privileges. To deal with these problems, modern databases are usually equipped with alarm functions in the audit mechanism to notify visitors and defenders of the potential risks during access to critical information [3], [4]. These alerts, which will be sent to defenders, are triggered by some specific access requests meeting predefined rules. In some audit mechanisms, users (or attackers) are granted with access permissions by defenders. And these granted permissions will be recorded in the log so that defenders can retrospectively check for any potential abuse or attack.

Currently, researchers usually model the above audit process between the defender and the attacker as an audit game [5]–[7]. To further enhance the timeliness in this process, other researchers introduce a signaling scheme working in an online manner. Whenever an access request triggers an alarm, the auditor will send a signal to the visitor to remind him/her that the requested data are sensitive. The behavior of sending a signal can be real-time with manual operations, or it can be automatic according to offline-setting rules. Although signaling does not substantially defend against attacks, it can help defenders discover security vulnerabilities promptly and prevent attackers from making more severe damages. In addition, the signaling step can interfere with attackers by strategically disclosing noisy information. The effectiveness of signaling has been proved in [8], and there are several studies [5], [9], [10] based on the Stackelberg game providing auditors with better strategic guidance in defending the database. In the industry, multiple medical centers and online service websites have deployed signaling schemes to protect sensitive data [11].

However, there exist two major shortcomings of the current research on signaling-based audit games. First, the widely employed Stackelberg game model usually assumes perfect information of attackers, which can be unrealistic since attackers may adopt various strategies in practice [10], [12]. Second, the existing studies focus more on the defender's interest without considering the attacker's utility, implying that the higher interest of the defender corresponds to the lower utility of the attacker [3], [6], [13], which may not hold for all types of attacks.

In this paper, we model the interactions between the defender and the attacker as a sequential game, where the attacker can observe the action of the defender regarding sending signals. In this sequential game, the defender acting first will be at a disadvantage, since the attacker can make more beneficial choices after witnessing the defender's behavior, leading to enormous losses for the defender in the long run. To solve this problem, given that the defender cannot fully detect the attacker's strategy, a brand-novel approach

Jianan Chen and Qin Hu (Corresponding Author) are with the Department of Computer and Information Science, Indiana University - Purdue University Indianapolis, IN, USA. Email: jc144@iu.edu, qinhu@iu.edu

Honglu Jiang is with the Department of Informatics and Engineering Systems, The University of Texas Rio Grande Valley, Brownsville, TX, USA. Email: honglu.jiang@utrgv.edu

This work is partly supported by the US NSF under grant CNS-2105004.

is employed to allow the defender to play against various attackers flexibly. More specifically, no matter what strategy the attacker employs, the defender can always deliberately set a feasible strategy of signaling and auditing to control the damages brought by the attack. Furthermore, compared with the existing methods, our proposed strategy is more in line with the real audit environment where the defender may not be able to predict the specific strategy adopted by an attacker. To achieve these goals, we employ the zero-determinant (ZD) strategy [14] to analyze the sequential audit game, which empowers the defender to unilaterally manage the utility of the attacker and even the utility difference between the defender and the attacker. By this means, we can address the issues of the existing studies, where the perfect information of the attacker is not required, but the interest of the attacker is explicitly considered and restricted.

Our main contributions can be summarized as follows:

- Considering that the audit action of the defender might be deterministic or probabilistic, we propose two different sequential games to model the interactions between the defender and the attacker, which describes the audit game in a more comprehensive manner.
- To unilaterally control the attacker's utility, we introduce a strategy guide for the defender with the help of the extended ZD strategy, which enables the defender to set up defense strategies for a low utility of the attacker in an effective way. Besides, we reveal the critical strategy variable in utility control for the defender by analyzing the controlling gradients and value ranges.
- For the cost-efficiency of utility control, we design an optimization scheme based on the ZD strategy to maximize the utility difference between the defender and the attacker, instead of controlling the utility of the attacker solely.
- Through comparing with classic strategies, we evaluate the effectiveness of our proposed ZD strategy-based schemes, where the defender adopting the ZD strategy can efficiently control the utility of the attacker using various strategies, and further maximize the utility difference between the defender and the attacker.

The remainder of this paper is organized as follows. We introduce the most related work in Section II. Two game models are presented in Section III. Section IV displays how the defender uses the ZD strategy to unilaterally control the attacker's utility. Section V proposes an optimization scheme to control the utility difference between the defender and the attacker. Experimental evaluation is reported in Section VI and the whole paper is concluded in Section VII.

II. Related Work

Most of the research on audit games focus on three aspects: dealing with different types of alarms, adapting to actual database scenarios, and optimizing the expected utility of the defender.

In order to solve the challenge of handling different types of alarms, Yan et al. proposed a game-theoretic audit method which first determines the priority of different alarms, and then assigns distinct amounts of resources to alarms with resource upper limits [7], [15]. Schlenker et al. proposed a method to distribute appropriate alerts to security analysts for different fields [16]. In [8], based on the two-stage security game framework, Xu et al. studied this problem by solving an optimization problem of Stacklberg equilibrium with a developed scalable approach.

Regarding the extension to the real-world scenario, Blocki et al. generalized the audit game model to account for multiple audit resources where each resource is restricted to audit a subset of potential violations [17]. Korzhyk et al. designed a polynomial time algorithm for security games with multiple resources [18]. Schlenker et al. used an approach based on game theory to address alerts [16], which can be well extended to different database security applications. Kiral et al. analyzed the inherent role conflicts of internal audit in risk management using signal game model [19].

Optimizing the expected utility of auditors can bring direct economic benefits to the database, where the related research can be divided into two categories: classic security game based and two-stage security game based. Blocki et al. first modeled the audit problem between an auditor and an auditee as a classic security game [17]. In this case, the auditor takes a strategic action with the goal of learning an optimized resource allocation strategy to optimize the auditor's expected utility. However, other research [10] claimed that the scalability of this framework is limited since the methods in [6], [17] regarded alerts as targets that could be attacked, which are not easy to apply to database. Xu et al. proposed a two-stage security game framework to overcome this challenge [8], where the characteristic is that the defender will leak his own information and send a signal in the second stage, which can protect the target with a better performance. A subsequent work [9] extended the advantages of signaling to Stackelberg games. This shows that the signal can also enhance the defense performance in the security game to a certain extent.

Our work is more related to optimizing the expected utility of the defender, which is usually modeled as Stackelberg games in previous studies. It is worth noting that the Stackelberg game requires complete information, which is difficult to achieve in a real audit environment. In the face of unknown strategy attacks, defenders need to respond more efficiently, which inspires this paper. Besides, previous research pay more attention to the utility of the defender, but lacked research on attackers' behaviors. We use the ZD strategy in this paper to allow the defender to have more control over the attacker's utility with unknown strategies, which has no requirement on the information completeness of audit games.

III. Game Models

We consider the interaction process occuring between an attacker and a defender, starting with the attacker issuing an access request for a certain type of data. Access to different types of data will trigger different types of alerts. After one type of alert verifies the access permission which does not necessarily ensure security, but allows the visitor to enter the database, the defender receives the alarm and chooses whether

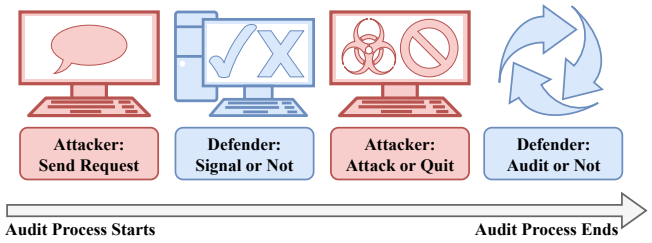


Fig. 1. The interaction process between the attacker and the defender.

to send a signal for real-time notification. The content of the prompt can be like if the attacker continues to visit, it may be reviewed. At this point, when receiving a prompt, the attacker clearly knows that the defender has sent a signal. Next, the attacker can further choose to continue access (and carry out illegal activities) or exit directly according to whether he receives the signal. After performing this operation, the defender will decide whether to audit based on whether there is a signal sent.

As shown in Fig. 1, the attacker first sends a request, and then the defender chooses whether to send a signal according to his request. Next, the attacker decides whether to continue or not based on the signaling behavior of the defender. The actions of both parties are carried out strictly in order, and the previous actions of the other party can be observed. Therefore, we define the interaction process between the attacker and defender as a sequential game.

Since the attacker can access the database multiple times or different units of the database, the defender interacts with the same attacker in multiple rounds, leading to an iterative sequential game. Participants of this kind of non-zero-sum iterative sequential game may get into trouble because of the existence of dominant strategies. In practical, this is not conducive to defenders. Nash equilibrium reveals the dominant strategies of both parties in this type of game. Therefore, we study the Nash equilibrium that may exist in this game, hoping to adopt a reasonable strategy to control the attacker's utility.

The defender will choose whether to audit or not according to the situation of sending signals after the attacker's action. The relationship between signaling and auditing can be probabilistic, where the defender audits with a certain probability. Or it could be deterministic, where the defender only audits after sending a signal. In the following context, in order to study the defender's strategy more comprehensively, we establish two models, the deterministic model and the probabilistic model.

A. Deterministic Model

In the deterministic model, the correlation between the defender's signaling and auditing is simple: for the alert of type η, if the defender sends a signal for the attacker's request, she[1] will definitely audit the request; otherwise she will not. We denote the action of the defender as $d \in \{0, 1\}$, where 0 represents that the defender chooses not to send a signal to the current request or audit it, while 1 indicates that the defender sends a signal to the current request and audits it. The attacker's action is denoted as $a \in \{0, 1\}$, where 0 refers to attack and 1 refers to quit without further attacks. Thus, there are four possible states of the game between the defender and the attacker, i.e., $da = (00, 01, 10, 11)$.

We can depict the sequential interaction process between the defender and the attacker in one round using a game tree as shown in Fig. 2. In the game tree, the payoffs in four states can be calculated as follows: i) for $da = 00$, as the defender chooses not to send a signal and the attacker doesn't attack, no one costs or acquires anything; ii) for $da = 01$, since the defender chooses not to send a signal but the attacker continues to attack, the defender suffers a loss t_d without auditing, while the attacker gains income r_a from a successful attack; iii) for $da = 10$, the defender sends a signal and audits but the attacker quits, so the defender spends c as the cost of auditing while the attacker acquires nothing; iv) when $da = 11$, meaning that the defender sends a signal and audits while the attacker deploys malicious attack, the defender suffers a loss t_m plus the cost of audit c, where t_m denotes the loss of being attacked but auditing timely; as for the attacker, the audit operation brings the attacker a decrease of s_a on income r_a, where s_a refers to the loss of the attacker being audited. Subsequently, we can define the payoff vectors of the defender (D) and the attacker (A) as:

$$\mathbf{U}_D^{\eta} = (0, -t_d, -c, -c - t_m),$$
$$\mathbf{U}_A^{\eta} = (0, r_a, 0, r_a - s_a).$$

It should be noted that t_d, c, t_m, r_a, and s_a are all positive. In particular, for the attacker, once the attack is successful without being caught, the benefit is large since the attacker can obtain valuable information or destroy the database. While for the defender, timely auditing after the attack or taking other repair measures, such as rollback, can only reduce the defender's loss. For the defender, auditing the attack can bring more benefit, i.e., the loss of non-auditing is larger than that of auditing. Therefore, we assume $t_d > t_m + c$. From the defender's point of view, she can gain from the historical data about the attacker's income r_a and the loss caused by the audit s_a. These two values, r_a and s_a, help the defender to control the attacker's utility in future games.

From the perspective of the attacker being the last player to perform action, the action with the greatest benefit is 1, so he makes this choice no matter what the situation is. Then, if the attacker's best action is to attack, from the defender's point of view, the most profitable action is 1, and this choice should be made no matter what the circumstance is. Thus, the Nash equilibrium of this game is $da = 11$.

B. Probabilistic Model

Different from the deterministic model, we now consider a situation closer to the reality, that the defender does not have to be fully deterministic with only auditing after sending the signal. Sometimes, out of some strategic considerations, the defender will not audit after sending the signal, or audit unexpectedly without sending a signal. In this case, we assume

[1]For the sake of distinction, we use "she" to refer to the defender and "he" to refer to the attacker.

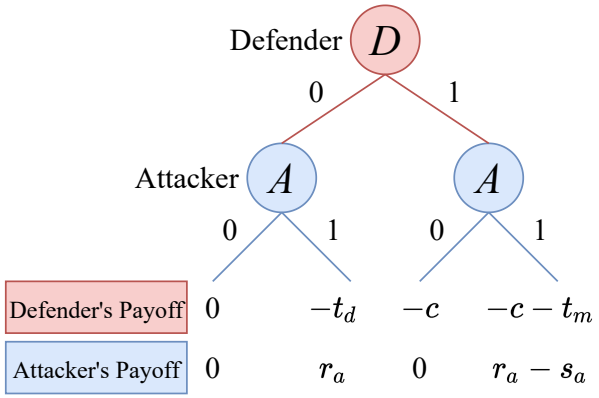


Fig. 2. The game tree of the deterministic model.

that there is a probability between the defender's signaling and auditing behavior, leading to the probabilistic model.

In the probabilistic model, we assume that if the defender sends a signal, the auditing will be done with the probability of τ; otherwise, she audits with the probability of δ, where $\tau > \delta$, as it is natural to be more inclined to audit when sending a signal.

Similar to the deterministic model, the probabilistic model also produces four possible states of the game between the defender and the attacker: $da = (00, 01, 10, 11)$. The payoffs of four states are calculated as follows: i) for $da = 00$, as the defender chooses not to send the signal and the attacker doesn't attack, the defender emerges an audit cost of c with the probability of δ while the attacker acquires nothing; ii) for $da = 01$, the defender chooses not to send the signal but the attacker attacks, the defender's loss consists of three parts: the audit cost, denoted as c, with the probability of δ, the loss of being attacked without audited, denoted as t_d, with the probability of $1-\delta$, and the loss of being attacked but audited sooner, denoted as t_m, with the probability of δ. Attacker gains income r_a minus punishment s_a from the audit with the probability of δ; iii) for $da = 10$, the defender sends a signal and audits with the probability of τ but the attacker quits, so the defender spends c as the cost of auditing with the probability of τ and the attacker acquires nothing; iv) for $da = 11$, denoting that the defender sends a signal and the attacker attacks. The defender's loss consists of three parts: the audit cost, denoted as c, with the probability of τ, the loss of being attacked without audited, denoted as t_d, with a probability of $1-\tau$, the loss of being attacked but audited sooner, denoted as t_m, with the probability of τ. While the attacker gains income r_a minus punishment s_a from the audit with the probability of τ. Subsequently, the payoff vector of the defender is $\tilde{\mathbf{U}}_D^\eta = (-\delta c, -\delta c - (\delta t_m + (1-\delta)t_d), -\tau c, -\tau c - (\tau t_m + (1-\tau)t_d))$ and that for attacker is $\tilde{\mathbf{U}}_A^\eta = (0, r_a - \delta s_a, 0, r_a - \tau s_a)$. For the sake of notation simplicity, we omit η in the following expressions, using $\mathbf{U}_A$, $\mathbf{U}_D$, $\tilde{\mathbf{U}}_A$ and $\tilde{\mathbf{U}}_D$ instead of $\mathbf{U}_A^\eta$, $\mathbf{U}_D^\eta$, $\tilde{\mathbf{U}}_A^\eta$ and $\tilde{\mathbf{U}}_D^\eta$, respectively.

Other related restrictions are similar to those in the above subsection, but with an additional restriction $\tau > \delta$. Since the attacker acts secondly, he will choose 1 to make the largest profit. For the defender, we can also conclude that the benefit of choosing 1 is always greater. So the Nash equilibrium in the probabilistic model is still $da = 11$.

IV. Utility Control of the Attacker using the Zero-Determinant Strategy

According to the analysis of Section III, we can see that there is a sequential Nash equilibrium in the game between the defender and the attacker, where the attacker's optimal strategy is to attack because the attack always brings him positive benefits, while the defender's optimal strategy is to send a signal and audit (with a higher probability in the probabilistic model) since auditing can effectively reduce the loss in both the deterministic model and the probabilistic model. In the long run, the defender consumes a lot of resources to send signals and conduct audits to play against potential attackers. However, considering that the defender's resource budget is generally limited, it is impossible to audit all requests including requests from non-attackers without restrictions. To solve this challenge, it becomes necessary to figure out an efficient strategy to audit requests, which can bring several benefits as follows. Firstly, this can effectively improve the audit efficiency and ensure the security of database information. Secondly, defender can also reduce the costs of signaling and auditing by sending signals strategically. In addition, reducing the number of signal prompts can improve the user experience for normal users.

In this section, we resort to the zero-determinant (ZD) strategy for achieving the above goals. Previous studies have proved that the ZD strategy ensures a linear relationship between the incomes of two players in the iterative game by setting an appropriate mixed strategy for one player, and even unilaterally set the opponent's expected income. This suggests us to propose a strategy to help the defender control the attacker's utility and prevent the database from excessive damages. Nonetheless, the classic ZD strategy studies the simultaneous game between two parties without knowing each other's actions. Therefore, we need to expand the ZD strategy to our sequential games.

As mentioned in [14], a long-memory player has no priority against a short-memory player in an iterated game. Therefore, we assume that the defender has only one round of memory. The defender's mixed strategy in a round is the conditional probability of choosing the strategy 0 based on all possible states of the previous round. As for the attacker, he has only one round of memory as well. His mixed strategy in a round is the conditional probability of choosing the strategy 0 based on all possible states of the previous round.

Definition IV.1. (The defender's mixed strategy $\mathbf{p}$). The mixed strategy of defender is denoted as $\mathbf{p} = (p_1, p_2, p_3, p_4)$, with each element being the probability of the defender to choose 0 when the outcome state of the previous round is $da = (00, 01, 10, 11)$.

Thus, $1 - p_i$ $(i \in \{1, 2, 3, 4\})$ denotes the probability of the defender to choose 1 when the outcome state of the previous round is $da = (00, 01, 10, 11)$.

Definition IV.2. (The attacker's mixed strategy $\mathbf{q}$). The mixed strategy of the attacker is denoted as $\mathbf{q} = (q_1, q_2)$, with each element being the probability of the attacker to choose 0 when the defender's action in the current round is $d = (0, 1)$.

Respectively, $1-q_1$ and $1-q_2$ denote the probability of the attacker to choose 1 when the defender's action in this round is $d = (0, 1)$.

Based on the above definitions, $\mathbf{p}$ and $\mathbf{q}$ can compose a Markov matrix denoting the state transition between two consecutive rounds, which can be expressed as:

$$\mathbf{M} = \begin{bmatrix} p_1q_1 & p_1(1-q_1) & (1-p_1)q_2 & (1-p_1)(1-q_2) \\ p_2q_1 & p_2(1-q_1) & (1-p_2)q_2 & (1-p_2)(1-q_2) \\ p_3q_1 & p_3(1-q_1) & (1-p_3)q_2 & (1-p_3)(1-q_2) \\ p_4q_1 & p_4(1-q_1) & (1-p_4)q_2 & (1-p_4)(1-q_2) \end{bmatrix}.$$

Each element in $\mathbf{M}$ is the transition probability from the state in the last round to that in the current round. Taking the first row of $\mathbf{M}$ as an example, four elements denote the transition probabilities from state $da = 00$ at the last round to the four possible states $da = 00, 01, 10, 11$ in the current round. The other three rows, similarly, correspond to the states $da = 01, 10, 11$ in the last round.

We can easily calculate that $\mathbf{M}' \equiv \mathbf{M} - \mathbf{I}$ is singular with the determinant value of zero. Besides, the stationary vector of $\mathbf{M}$, denoted as $\mathbf{v}$, satisfies $\mathbf{v}^T\mathbf{M} = \mathbf{v}^T$ which equals $\mathbf{v}^T\mathbf{M}' = 0$. Applying Cramer's rule on matrix $\mathbf{M}'$, we can get:

$$Adj(\mathbf{M}')\mathbf{M}' = \det(\mathbf{M}')\mathbf{I} = 0,$$

where $Adj(\mathbf{M}')$ denotes the adjugate matrix of $\mathbf{M}'$. Thus, we can conclude that every row of $Adj(\mathbf{M}')$ is proportional to $\mathbf{v}$. The determinant of $\mathbf{M}'$ is unchanged if we add the first column of $\mathbf{M}'$ into the second and third columns. Thus, we can calculate the dot product of an arbitrary four-element vector $\mathbf{f} = (f_1, f_2, f_3, f_4)$ and the stationary vector $\mathbf{v}$ as follows:

$$\mathbf{v} \cdot \mathbf{f} \equiv D(\mathbf{p}, \mathbf{q}, \mathbf{f})$$

$$= \det \begin{bmatrix} p_1q_1 - 1 & p_1 - 1 & (1-p_1)q_2 + p_1q_1 - 1 & f_1 \\ p_2q_1 & p_2 - 1 & (1-p_2)q_2 + p_2q_1 & f_2 \\ p_3q_1 & p_3 & (1-p_3)q_2 + p_3q_1 - 1 & f_3 \\ p_4q_1 & p_4 & (1-p_4)q_2 + p_4q_1 & f_4 \end{bmatrix}, \tag{1}$$

where the second column is under the control of the defender. Combining payoff vectors of the defender and the attacker, their respective utilities in the stationary state are:

$$u_a = \frac{\mathbf{v} \cdot \mathbf{U}_A}{\mathbf{v} \cdot \mathbf{1}} = \frac{D(\mathbf{p}, \mathbf{q}, \mathbf{U}_A)}{D(\mathbf{p}, \mathbf{q}, \mathbf{1})},$$

$$u_d = \frac{\mathbf{v} \cdot \mathbf{U}_D}{\mathbf{v} \cdot \mathbf{1}} = \frac{D(\mathbf{p}, \mathbf{q}, \mathbf{U}_D)}{D(\mathbf{p}, \mathbf{q}, \mathbf{1})}.$$

The above equations show that the utility of the attacker and that of the defender depend linearly on their corresponding payoff vectors. Thus, their linear combination of utilities will be calculated as:

$$\alpha u_a + \beta u_d + \gamma = \frac{D(\mathbf{p}, \mathbf{q}, \alpha\mathbf{U}_A + \beta\mathbf{U}_D + \gamma\mathbf{1})}{D(\mathbf{p}, \mathbf{q}, \mathbf{1})}, \tag{2}$$

with α, β, γ being constant parameters. It brings us many good attributes, allowing the defender to have a chance to make the determinant $D(\mathbf{p}, \mathbf{q}, \alpha\mathbf{U}_A + \beta\mathbf{U}_D + \gamma\mathbf{1})$ vanish. In fact, when the defender chooses a strategy that satisfies $\hat{\mathbf{p}} = \alpha\mathbf{U}_A + \beta\mathbf{U}_D + \gamma\mathbf{1}$, where $\hat{\mathbf{p}}$ denotes the second column of $D(\mathbf{p}, \mathbf{q}, \mathbf{f})$, the second column and the forth column of $D(\mathbf{p}, \mathbf{q}, \alpha\mathbf{U}_A + \beta\mathbf{U}_D + \gamma\mathbf{1})$ can be the same, then (2) changes to:

$$\alpha u_a + \beta u_d + \gamma = 0. \tag{3}$$

Thus, a linear relationship between u_a and u_d is enforced. The ZD strategy, however, is not feasible in all cases, which depends on whether the range of $\mathbf{p}$ is [0,1].

We can deploy the ZD strategy in the deterministic model and the probabilistic model, which provides the defender with a powerful approach to unilaterally control the attacker's utility.

A. Deterministic Model

In this part, we start with the basic deterministic model to find a strategy for the defender to control the attacker's utility. Generally, we analyze the relationship between the defender's strategy and the attacker's utility to get an appropriate strategy, and then find the most efficient variable to control the attacker's income, where the maximum and minimum utility of the attacker are analyzed as well to help the defender to assess potential risks.

From (3), we can see that the defender only needs to play a fixed strategy satisfying $\hat{\mathbf{p}} = \alpha\mathbf{U}_A + \gamma\mathbf{1}$ (setting $\beta = 0$) to set the attacker's utility. In this case, we can solve the below equation group:

$$\begin{cases} p_1 - 1 = \gamma, \\ p_2 - 1 = \alpha r_a + \gamma, \\ p_3 = \gamma, \\ p_4 = \alpha(r_a - s_a) + \gamma, \end{cases} \tag{4}$$

where p_1 and p_4 can be used to represent the remaining variables to get the expression of u_a:

$$u_a = -\frac{\gamma}{\alpha} = \frac{1-p_1}{p_4 + 1 - p_1} \cdot (r_a - s_a). \tag{5}$$

This expression implies that if the defender adopts a strategy satisfying $\hat{\mathbf{p}} = \alpha\mathbf{U}_A + \gamma\mathbf{1}$, the utility of the attacker can be determined by the defender. Then, we can analyze the features of u_a. Firstly, the value range of u_a is $[0, r_a - s_a]$; secondly, in (5), p_1 and p_4 are variables that are unilaterally controlled by the defender, so we need to further study the extent of their influences on u_a. By this means, we can reveal that which variable is more effective to safeguard the system security to the greatest extent. Therefore, we first take the partial derivative of u_a with respect to p_1,

$$\frac{\partial u_a}{\partial p_1} = \frac{-p_4}{(p_4 + 1 - p_1)^2} \cdot (r_a - s_a), \tag{6}$$

where the derivative function decreases monotonically in $p_1 \in [0, 1]$. Further, we have:

$$\overline{u}_a = u_a | (p_1 = 0) = \frac{1}{p_4} \cdot (r_a - s_a),$$

$$\underline{u}_a = u_a|(p_1 = 1) = 0,$$

where $\overline{u}_a$ denotes the maximum value of u_a and $\underline{u}_a$ denotes the minimum value of u_a. This shows that if the defender only changes the value of p_1 in the strategy, the attacker's utility will be a certain value within the range of $[0, \frac{r_a - s_a}{p_4}]$.

Similarly, we take the partial derivative of p_4,

$$\frac{\partial u_a}{\partial p_4} = \frac{p_1 - 1}{(p_4 + 1 - p_1)^2} \cdot (r_a - s_a).$$

It can be seen that the derivative function decreases monotonically in $p_4 \in [0, 1]$ and we have:

$$\overline{u}_a = u_a|(p_4 = 0) = (r_a - s_a),$$

$$\underline{u}_a = u_a|(p_4 = 1) = \frac{1 - p_1}{2 - p_1} \cdot (r_a - s_a).$$

This shows that if the defender only changes the value of p_4 in the strategy, the attacker's utility could be a certain value within the range of $[\frac{1-p_1}{2-p_1} \cdot (r_a - s_a), r_a - s_a]$.

To control the attacker's utility more efficiently, we study which variable is more effective. In other words, when the increments of p_1 and p_4 are the same, which one of them causes a larger loss of the attacker's utility. Comparing the partial derivatives of two variables, we have:

$$\frac{\partial u_a}{\partial p_1} - \frac{\partial u_a}{\partial p_4} = \frac{1 - p_1 - p_4}{(p_4 + 1 - p_1)^2} \cdot (r_a - s_a).$$

It is clear that, when $1 - p_1 - p_4 > 0$, the partial derivative of p_1 is greater than that of p_4. Since they are all negative, it is more effective for the defender to control attacker's utility by changing p_4. While when $1 - p_1 - p_4 < 0$, the partial derivative of p_4 is greater than that of p_1. At this time, it is more effective for the defender to control attacker's utility by changing p_1.

Besides, p_1 and p_4 also have impacts on the value range of u_a. Regarding p_1 as the only variable, $u_a \in [0, \frac{r_a - s_a}{p_4}]$, with the range size of $\frac{r_a - s_a}{p_4}$. Regarding p_4 as the only variable, $u_a \in [\frac{1-p_1}{2-p_1} \cdot (r_a - s_a), r_a - s_a]$, with the range size of $\frac{r_a - s_a}{2 - p_1}$. The above two sizes of range present the relationship of $\frac{r_a - s_a}{2-p_1} \leq \frac{r_a - s_a}{p_4}$, since $2 - p_1$ is in the range of $[1, 2]$ and p_4 is in $[0, 1]$, which means p_1 has a greater impact on the control range of u_a. Comparing the lower bounds of the above ranges, we have $0 \leq \frac{1-p_1}{2-p_1} \cdot (r_a - s_a)$, while for the upper bounds, we have $\frac{r_a - s_a}{p_4} \leq r_a - s_a$. Thus, if the defender tries to control u_a at a low level, it is more effective to change p_1.

According to the analysis above, we can conclude that when $p_1 < 1 - p_4$, p_1 has a greater impact on the value of u_a; when $p_1 > 1 - p_4$, p_4 has a greater impact on the value of u_a. In order to deploy defense strategies more effectively, the defender should pay attention to the relationship between the $p_1 + p_4$ and 1. And if the defender can only change one variable, changing p_1 can be more conducive to limit the attacker's utility.

B. Probabilistic Model

Similarly, we can analyze the probabilistic model. It should be noted that the two newly added variables τ and δ in the probabilistic model are unilaterally controlled by the defender, because they are used to determine the probability of auditing after signaling. Although τ and δ are different in definition from the strategy vector $\mathbf{p}$, their property of being controlled by the defender implies that they are also worthy of being studied. Solving the equation group like (4), the expression of $\tilde{u}_a$ in the probabilistic model becomes:

$$\tilde{u}_a = -\frac{\gamma}{\alpha} = \frac{1 - p_1}{p_4 + 1 - p_1} \cdot (r_a - \tau s_a). \tag{7}$$

Clearly, the value range of $\tilde{u}_a$ is $[0, r_a - \tau s_a]$. Further, in order to allow the defender to control the attacker's utility $\tilde{u}_a$ more efficiently, we study the influence of the four variables $p1, p4, \tau$ and δ controlled by the defender on $\tilde{u}_a$ from a mathematical perspective. Notice that only $p1, p4$ and τ appear in (7), so we ignore the effect of δ and take the partial derivative of $\tilde{u}_a$ with respect to p_1 firstly:

$$\frac{\partial \tilde{u}_a}{\partial p_1} = \frac{-p_4}{(p_4 + 1 - p_1)^2} \cdot (r_a - \tau s_a). \tag{8}$$

From (8), the derivative function decreases monotonically in $p_1 \in [0, 1]$. If we regard p_1 as the only variable, then we have:

$$\overline{\tilde{u}}_a = \tilde{u}_a|(p_1 = 0) = \frac{1}{p_4} \cdot (r_a - \tau s_a),$$

$$\underline{\tilde{u}}_a = \tilde{u}_a|(p_1 = 1) = 0,$$

where $\overline{\tilde{u}}_a$ denotes the maximum value of $\tilde{u}_a$, while $\underline{\tilde{u}}_a$ denotes the minimum value of $\tilde{u}_a$. It can be seen that if the defender only changes the value of p_1 in the strategy, the attacker's utility will be a certain value within the range of $[0, \frac{r_a - \tau s_a}{p_4}]$.

Similarly, taking the derivative of p_4, we have:

$$\frac{\partial \tilde{u}_a}{\partial p_4} = \frac{p_1 - 1}{(p_4 + 1 - p_1)^2} \cdot (r_a - \tau s_a),$$

where the derivative function decreases monotonically in $p_4 \in [0, 1]$. Regarding p_4 as a variable, we have:

$$\overline{\tilde{u}}_a = \tilde{u}_a|(p_4 = 0) = r_a - \tau s_a,$$

$$\underline{\tilde{u}}_a = \tilde{u}_a|(p_4 = 1) = \frac{1 - p_1}{2 - p_1} \cdot (r_a - \tau s_a),$$

which shows that if the defender only changes the value of p_4 in the strategy, the attacker's utility will be a certain value within the range of $[\frac{1-p_1}{2-p_1} \cdot (r_a - \tau s_a), r_a - \tau s_a]$.

In the probabilistic model, the effect of p_1 and p_4 are similar to that in the deterministic model. By comparing the partial derivatives of two variables:

$$\frac{\partial u_a}{\partial p_1} - \frac{\partial u_a}{\partial p_4} = \frac{1 - p_1 - p_4}{(p_4 + 1 - p_1)^2} \cdot (r_a - \tau s_a),$$

we can draw the same conclusion with that in the deterministic model: when $p_1 < 1 - p_4$, p_1 has a greater impact on the control of the value of $\tilde{u}_a$; when $p_1 > 1 - p_4$, p_4 is more effective to control $\tilde{u}_a$. Thus, p_1 has a greater impact on the value range of $\tilde{u}_a$ as well as on controlling $\tilde{u}_a$ at a low level.

Meanwhile, p_1 and p_4 have impacts on the value range of $\tilde{u}_a$. Regard p_1 as the only variable, $\tilde{u}_a \in [0, \frac{r_a - \tau s_a}{p_4}]$, with the range of $\frac{r_a - \tau s_a}{p_4}$. Regard p_4 as the only variable, $\tilde{u}_a \in [\frac{1-p_1}{2-p_1} \cdot (r_a - \tau s_a), r_a - \tau s_a]$, with the range of $\frac{r_a - \tau s_a}{2 - p_1}$. As for the size of range, we have $\frac{r_a - \tau s_a}{2-p_1} \leq \frac{r_a - \tau s_a}{p_4}$ as $2 - p_1 \in [1, 2]$ and

$p_4 \in [0,1]$. Comparing the lower bounds of the above ranges, we have $0 \leq \frac{1-p_1}{2-p_1} \cdot (r_a - \tau s_a)$, while for the upper bounds, we have $\frac{r_a - \tau s_a}{p_4} \leq r_a - \tau s_a$, so p_1 has greater influence on controlling value of $\tilde{u}_a$.

In addition, the influence of τ on $\tilde{u}_a$ is different from that of p_1 and p_4, as the partial derivatives of τ is:

$$\frac{\partial \tilde{u}_a}{\partial \tau} = \frac{s_a(p_1 - 1)}{(p_4 + 1 - p_1)},$$

which means the relationship between τ and $\tilde{u}_a$ is negative correlated since $p_1 \leq 1$. If we only regard τ as a variable, we have:

$$\overline{\tilde{u}}_a = \tilde{u}_a|(\tau = 0) = \frac{r_a(1-p_1)}{p_4 + 1 - p_1},$$

$$\underline{\tilde{u}}_a = \tilde{u}_a|(\tau = 1) = \frac{1-p_1}{p_4 + 1 - p_1} \cdot (r_a - s_a),$$

where $\overline{\tilde{u}}_a$ denotes the maximum value of $\tilde{u}_a$, while $\underline{\tilde{u}}_a$ denotes the minimum value of $\tilde{u}_a$. This shows that if the defender only changes the value of τ in the strategy, the attacker's utility will be a certain value within the range of $[\frac{(1-p_1)}{p_4+1-p_1} \cdot (r_a - s_a), \frac{r_a(1-p_1)}{p_4+1-p_1}]$. Regard τ as the only variable, $\tilde{u}_a \in [\frac{(1-p_1)}{p_4+1-p_1} \cdot (r_a - s_a), \frac{r_a(1-p_1)}{p_4+1-p_1}]$, whose range is $\frac{s_a(1-p_1)}{p_4+1-p_1}$.

V. Maximizing the Utility Difference using the Zero-Determinant Strategy

The ZD strategy demonstrates powerful control over the attacker's utility as mentioned in the previous section. Although controlling the attacker's utility sometimes leads to excellent performance, simply controlling the attacker's utility at a lower level may result in huge budget expenditures. Therefore, when necessary, we hope to design a strategy that considers both the utility of the defender and that of the attacker. Different from the defender's utility, the utility difference between the defender and the attacker is a relative value, and the study of utility difference is helpful for the defender to flexibly deal with the strategies of different attackers. Because this repeated game is not a zero-sum game, if the defender has the highest utility, the attacker could be likely to get a high utility as well, which can bring more damage to the database. In this section, we use the ZD strategy to find the maximum utility difference in defender's point of view.

Our main idea is to propose a set of signal and audit strategies for the defender to make $\tilde{u}_d - \tilde{u}_a$ the largest. It should be noted that although we proposed two models before, i.e., the deterministic model and the probabilistic model, in this section, we use the probabilistic model as an example to explore the utility difference control. The reason is that compared with the deterministic model, the variables τ and δ in the probabilistic model expand the action space of the defender, which is more flexible and comprehensive. In addition, it is easy to get similar conclusions in the probabilistic model and the deterministic model, via eliminating the influence of τ and δ by setting $\tau = 1$ and $\delta = 0$.

According to (3), by setting $\alpha = -1$ and $\beta = 1$, the utility difference between the defender and the attacker can be calculated as:

$$\tilde{u}_d - \tilde{u}_a = -\gamma.$$

Hence, the basic issue of maximizing the utility difference can be achieved by solving:

$$\begin{aligned} &\max\ -\gamma, \\ &s.t.\quad 0 \leq p_i \leq 1, \forall i \in \{1,2,3,4\}, \end{aligned}$$

which is equivalent to the following optimization problem with constraints:

$$\begin{aligned} &\min \gamma, \\ &s.t. \begin{cases} 0 \leq p_i \leq 1, \forall i \in \{1,2,3,4\}, \\ \hat{\mathbf{p}} = \phi(\tilde{\mathbf{U}}_D - \tilde{\mathbf{U}}_A + \gamma \mathbf{1}), \\ \phi \neq 0. \end{cases} \end{aligned}$$

Among them, $\hat{\mathbf{p}} = (p_1 - 1, p_2 - 1, p_3, p_4)$ is the second column in (1), which can be unilaterally determined by the defender's strategy. We denote $\tilde{U}_A^k$ and $\tilde{U}_D^k$ as the kth element in $\tilde{\mathbf{U}}_A$ and $\tilde{\mathbf{U}}_D$, respectively. Then we can solve the above optimization problem by considering the following two cases:

1) Case 1: $\phi > 0$. To meet the constraint $p_i \geq 0$, we can get the lower bound of γ as follows:

$$\begin{aligned} &\gamma_{min} = \max(\Lambda_k), \forall k \in \{1,2,3,4\}, \\ &\Lambda_k = \begin{cases} -\tilde{U}_D^k + \tilde{U}_A^k - \frac{1}{\phi}, & k = 1,2, \\ -\tilde{U}_D^k + \tilde{U}_A^k, & k = 3,4. \end{cases} \end{aligned}$$

To meet the constraint $p_i \leq 1$, we can get the upper bound of γ as follows:

$$\begin{aligned} &\gamma_{max} = \min(\Lambda_l), \forall l \in \{5,6,7,8\}, \\ &\Lambda_l = \Lambda_{k+4} \begin{cases} -\tilde{U}_D^k + \tilde{U}_A^k, & k = 1,2, \\ -\tilde{U}_D^k + \tilde{U}_A^k + \frac{1}{\phi}, & k = 3,4. \end{cases} \end{aligned}$$

Only if $\gamma_{min} \leq \gamma_{max}$ can γ has a feasible solution, which is equivalent to $\max(\Lambda_k) \leq \min(\Lambda_l), \forall k \in \{1,2,3,4\}, \forall l \in \{5,6,7,8\}$. If there exists $\phi > 0$ satisfying the above constraint, we can obtain the minimum value of γ as follow:

$$\begin{aligned} \gamma_{min} &= \max\{-\tilde{U}_D^1 + \tilde{U}_A^1 - \frac{1}{\phi}, -\tilde{U}_D^2 + \tilde{U}_A^2 - \frac{1}{\phi}, \\ &\qquad - \tilde{U}_D^3 + \tilde{U}_A^3, -\tilde{U}_D^4 + \tilde{U}_A^4\} \\ &= \max\{\delta c - \frac{1}{\phi}, \delta c + (\delta t_m + (1-\delta)t_d) + r_a - \delta s_a - \frac{1}{\phi}, \\ &\qquad \tau c, \tau c + (\tau t_m + (1-\tau)t_d) + r_a - \tau s_a\}. \end{aligned} \quad (9)$$

2) Case 2: $\phi < 0$. Similarly, when considering that $p_i \geq 0$, we have $\gamma_{min} = \max(\Lambda_l), \forall l \in \{5,6,7,8\}$; while when considering that $p_i \leq 1$, we have $\gamma_{max} = \min(\Lambda_k), \forall k \in \{1,2,3,4\}$. In addition, γ is feasible only when $\gamma_{min} \leq \gamma_{max}$, i.e., $\max(\Lambda_l) \leq \min(\Lambda_k), \forall k \in \{1,2,3,4\}, \forall l \in \{5,6,7,8\}$. Finally, we can get the following result:

$$\begin{aligned} \gamma_{min} &= \max\{-\tilde{U}_D^1 + \tilde{U}_A^1, -\tilde{U}_D^2 + \tilde{U}_A^2, \\ &\qquad - \tilde{U}_D^3 + \tilde{U}_A^3 + \frac{1}{\phi}, -\tilde{U}_D^4 + \tilde{U}_A^4 + \frac{1}{\phi}\} \\ &= \max\{\delta c, \delta c + (\delta t_m + (1-\delta)t_d) + r_a - \delta s_a, \\ &\qquad \tau c + \frac{1}{\phi}, \tau c + (\tau t_m + (1-\tau)t_d) + r_a - \tau s_a + \frac{1}{\phi}\}. \end{aligned} \quad (10)$$

In summary, by (9) and (10), the defender can unilaterally set the maximum value of $\tilde{u}_d - \tilde{u}_a$ with the ZD strategy $\mathbf{p}$

meeting $\hat{\mathbf{p}} = \phi(\tilde{\mathbf{U}}_D - \tilde{\mathbf{U}}_A + \gamma\mathbf{1})$, where each element of $\mathbf{p}$ can be calculated by:

$$p_i = \begin{cases} \tilde{U}_D^i - \tilde{U}_A^i + \gamma_{min} + 1, & i = 1, 2, \\ \tilde{U}_D^i - \tilde{U}_A^i + \gamma_{min}, & i = 3, 4. \end{cases}$$

Remark. For the deterministic model, we can have the optimization problem as:

$$\min \gamma, \quad s.t. \begin{cases} 0 \leq p_i \leq 1, \forall i \in \{1, 2, 3, 4\}, \\ \hat{\mathbf{p}} = \phi(\mathbf{U}_D - \mathbf{U}_A + \gamma\mathbf{1}), \\ \phi \neq 0, \end{cases}$$

which can be easily solved using the above conclusions. Specifically, we can derive the maximized utility difference as:

$$\gamma_{min} = \begin{cases} \max\{-U_D^1 + U_A^1 - \frac{1}{\phi}, -U_D^2 + U_A^2 - \frac{1}{\phi}, \\ \quad -U_D^3 + U_A^3, -U_D^4 + U_A^4\}, & \phi > 0, \\ \max\{-U_D^1 + U_A^1, -U_D^2 + U_A^2, -U_D^3 + U_A^3 + \frac{1}{\phi}, \\ \quad -U_D^4 + U_A^4 + \frac{1}{\phi}\}, & \phi < 0, \end{cases}$$

and $\mathbf{p}$ is given by

$$p_i = \begin{cases} U_D^i - U_A^i + \gamma_{min} + 1, & i = 1, 2, \\ U_D^i - U_A^i + \gamma_{min}, & i = 3, 4. \end{cases}$$

VI. Experimental Evaluation

In this section, we evaluate the performance of the ZD strategy for the defender based on simulation experiments. All experiments are implemented using Matlab R2020a on a laptop with 2.3 GHz Intel Core i5-8300H processor. Besides, for the common parameters of the deterministic model and probabilistic model, we set the following default values: the loss of non-auditing after being attacked $t_d = 8$, the loss of auditing after being attacked $t_m = 5$; the income of the successful attack $r_a = 10$, the loss of the attack being audited $s_a = 5$; the cost of auditing $c = 2$. Each experiment is repeated 50 times to get the average results for statistical confidence. We also conduct multiple experiments with different parameter settings, but all the experimental results are similar or have the same statistical significance. Therefore, in order to avoid redundancy, we omit them and report the most representative experimental results.

A. Unilateral Control of the Attacker's Utility using the ZD Strategy

We deploy simulation experiments to verify the effectiveness of the defender using the ZD strategy to unilaterally control the attacker's utility, as well as demonstrate how the defender controls the attacker's utility based on p_1 and p_4. Fig. 3 plots the attacker's utility changing with the defender's various strategy variables in the deterministic model. As mentioned in Section IV, p_1 and u_a are negatively correlated. The changing rate increases as p_1 increases. And p_4, is also negatively correlated with u_a while the rate of change decreases as p_4 increases. Fig. 4 presents that the probabilistic

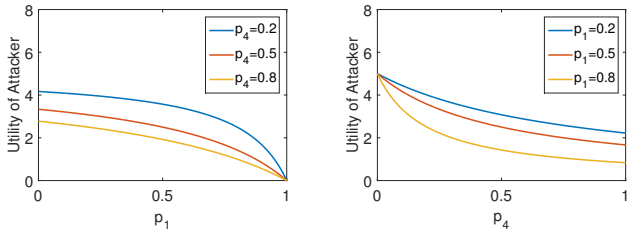


Fig. 3. The attacker's utility changes with different defender's strategy variables in the deterministic model.

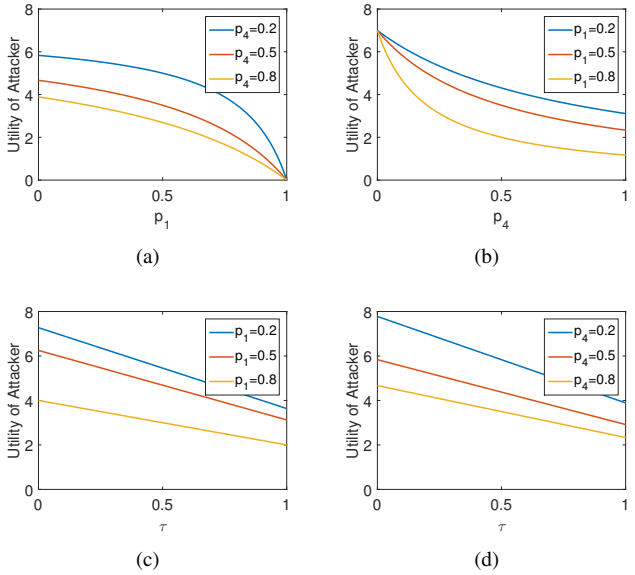


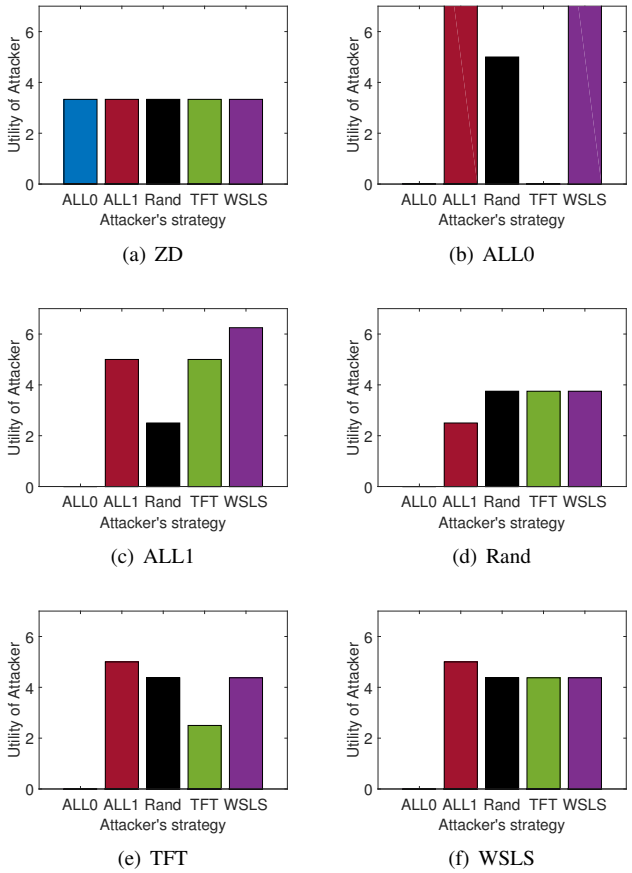
Fig. 4. The attacker's utility changes with different defender's strategy variables in the probabilistic model.

model has similar properties. It is worth noting that Fig. 4(c)(d) shows that τ has a linear relationship with $\tilde{u}_a$, where the higher the τ, the lower the attacker's utility.

In addition, to verify the effectiveness of our scheme, we compare the defender's ZD strategy with other five classic strategies. We simulate the entire process of the defender and the attacker in the deterministic model, for 50 rounds, in which the defender uses the ZD, All-Zero (ALL0) [20], All-One (ALL1) [20], Random (Rand) [20], Tit-For-Tat (TFT) [21], and Win-Stay-Lose-Shift (WSLS) [22] strategies. The attacker adopts ALL0, ALL1, Rand, TFT, and WSLS strategies. Specifically, ALL0 strategy is defined as: the defender always takes the action of not sending the signal no matter what the opponent does and the attacker always chooses to quit. ALL1 strategy means that the defender always sends the signal and the attacker always chooses to attack. With the Rand strategy, each player selects the action of 0 with the probability of 0.5. TFT strategy is defined as the player follows the choice of the opponent in the previous round. While WSLS strategy is defined as the player follows the choice if it won in the previous round, but changes to the other action otherwise.

By comparing Fig. 5(a) with the other five figures, we can easily find that when the attacker adopts ALL1, Rand, TFT and

WSLS strategies, the defender's ZD strategy can effectively control the attacker's utility at a lower level. This can prove that unless the attacker adopts the ALL0 strategy, the ZD strategy is better than other classic strategies. However, in the real audit environment, it is almost impossible for the attacker to adopt ALL0 strategy, because it means that the attacker does not attack at all. Similarly, we can find in Fig. 5(b) that if the defender adopts the ALL0 strategy, she can achieve good results in some cases but the rest can be bad, which reflects that the inactive defender suffers heavy losses when the attacker attacks and can only hope that the attacker would quit, which can not happen in reality.



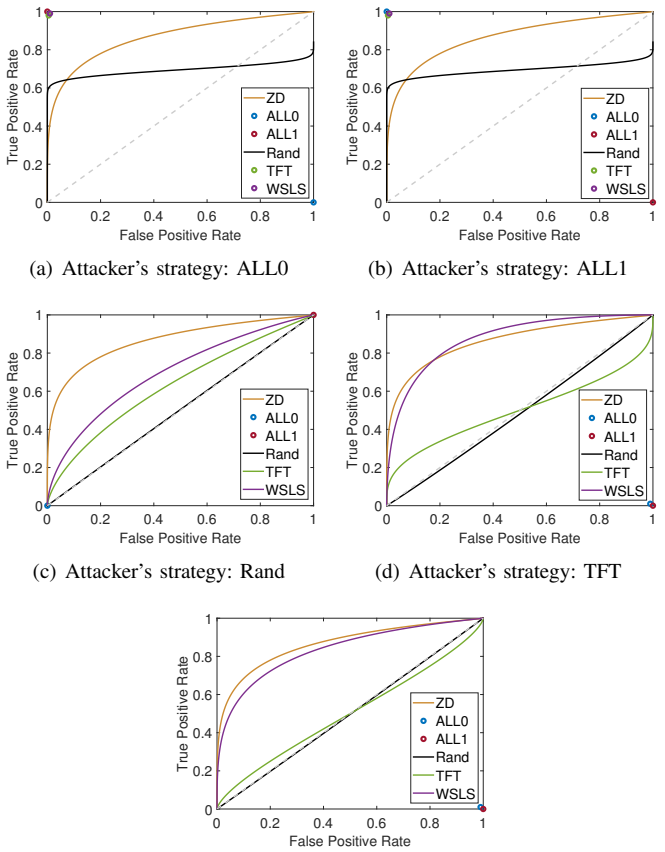
(a) ZD (b) ALL0

(c) ALL1 (d) Rand

(e) TFT (f) WSLS

Fig. 5. The attacker's utility under different strategy combinations of the attacker and the defender in the deterministic model.

Next, we explore the detection performance of the ZD strategy for potential attacks and plot the Receiver Operating Characteristic (ROC) curves for the defender deploying the ZD strategy and other strategies when the attacker uses a classic strategy in Fig. 6. We regard a test sample as a true positive if the defender chooses to send a signal and the attacker chooses to attack. Similarly, we define a sample as a false positive when the defender sends a signal while the attacker does not attack. Assuming a sample as a true negative if the defender does not send any signal but the attacker carries out the malicious action, and as a false negative if both sides do nothing. The x-axis depicts the False Positive Rate (FPR). Denoting FP and TN as the numbers of false positive samples and true negative samples, respectively, we can calculate FPR $= \frac{\text{FP}}{\text{FP+TN}}$.



(a) Attacker's strategy: ALL0 (b) Attacker's strategy: ALL1

(c) Attacker's strategy: Rand (d) Attacker's strategy: TFT

(e) Attacker's strategy: WSLS

Fig. 6. ROC curves under different strategy combinations of the defender and the attacker in the deterministic model.

The y-axis represents the True Positive Rate (TPR), which is calculated by TPR $= \frac{\text{TP}}{\text{TP+FN}}$ with TP denoting the number of true positive samples and FN denoting the number of false negative samples.

From Fig. 6, we can see that the ZD strategy outperforms almost all other strategies since its Area Under the Curve (AUC) is larger than the AUCs of other strategies. Besides, the gray dotted line represents the ROC curve of random guessing with AUC$= 0.5$, which is used as a reference for comparison. Specifically, in Figs. 6(a) and (b), the ROC curves of WSLS, TFT, ALL1, and ALL0 strategies degenerate to the point (0,1) or (1,0) as the defender only executes the same action when the attacker deploys the ALL0 or ALL1 strategy. For example, when the attacker uses the ALL1 strategy and the defender adopts the TFT strategy, the action in each round is $ad = (1, 1)$, refering to the point (0,1) in the ROC curve. In Fig. 6(d), the AUC of the WSLS strategy is close to that of the ZD strategy, which indicates that the performance of these two strategies is quite similar when the attacker adopts the TFT strategy.

B. Maximizing the Utility Difference using the ZD Strategy

We investigate the correctness and effectiveness of our proposed strategy for optimizing the utility difference between the defender and the attacker. In this part, we mainly show the

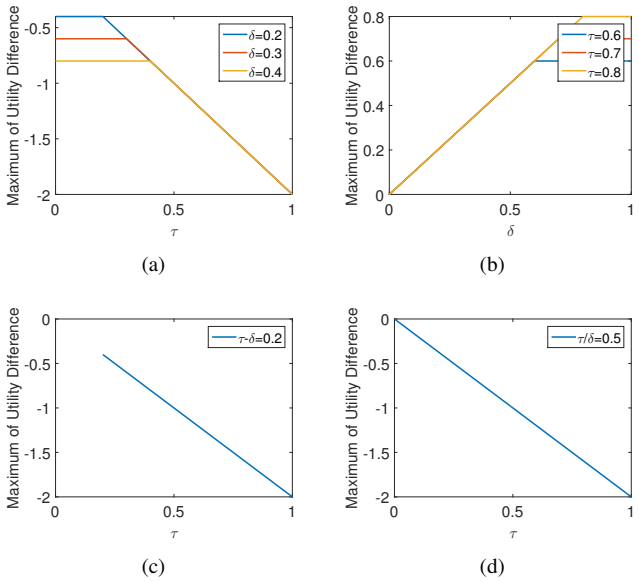


Fig. 7. The optimization goal $\tilde{u}_d - \tilde{u}_a$ changes with parameters combination in the probabilistic model.

experimental results of the probabilistic model. As demonstrated in Section V, it is easy to draw similar conclusions in the probabilistic model and the deterministic model by setting $\tau = 1$ and $\delta = 0$. In Fig. 7, we present the solution of the optimization problem that maximizes $\tilde{u}_d - \tilde{u}_a$. Based on the parameter setting mentioned before, we found that there is a feasible solution for p_i in the constraint condition if and only if $\phi < 0$. We plot the figure of the maximized utility difference changing with τ and δ when $\phi = -1$. It can be seen that under this condition, the maximum value of the optimization target is negatively correlated with τ and positively correlated with δ. This is because if the defender considers the utilities of both herself and the attacker, she has to consider appropriately reducing the probability of auditing (τ) after signaling because of the cost of the audit. But the defender cannot reduce this probability without any limit, because when it reaches a certain value, it no longer has an impact on the maximum value of the optimization goal. Fig. 7(c) shows that if the defender changes τ and δ at the same time while keeping the difference between them unchanged, τ will have a linear effect on the maximum utility difference. It is worth noting that in Fig. 7(d) if we set τ and δ proportionally, the influence of τ on the optimization goal is also linear.

To verify the effectiveness of our ZD strategy-based scheme, we set $\tau = 0.6$ and $\delta = 0.2$, and compare the optimization goal of ZD scheme with those obtained by other classic strategies, i.e., ALL1, Rand, TFT, and WSLS strategies. Fig. 8 displays the optimization goal $\tilde{u}_d - \tilde{u}_a$ when the defender takes different strategies. By comparing Fig. 8(a) with the other five figures, one can conclude that the ZD strategy gets a larger maximum value of the optimization target, except for the situation that the attacker adopts the ALL0 strategy and some situations that the defender adopts the ALL0 strategy. However, it is rare for an attacker to adopt the ALL0 strategy. In this case, an active defender consumes more audit budget than an inactive defender, which makes the total utility less. Besides, if the defender adopts the ALL0 strategy for a long time, then she can only hope that the attacker will never attack (also adopts the ALL0 strategy), which hardly occurs in actual situations. So in most common cases, using the ZD strategy can effectively make the difference between the defender's utility and attacker's utility stay at a high level.

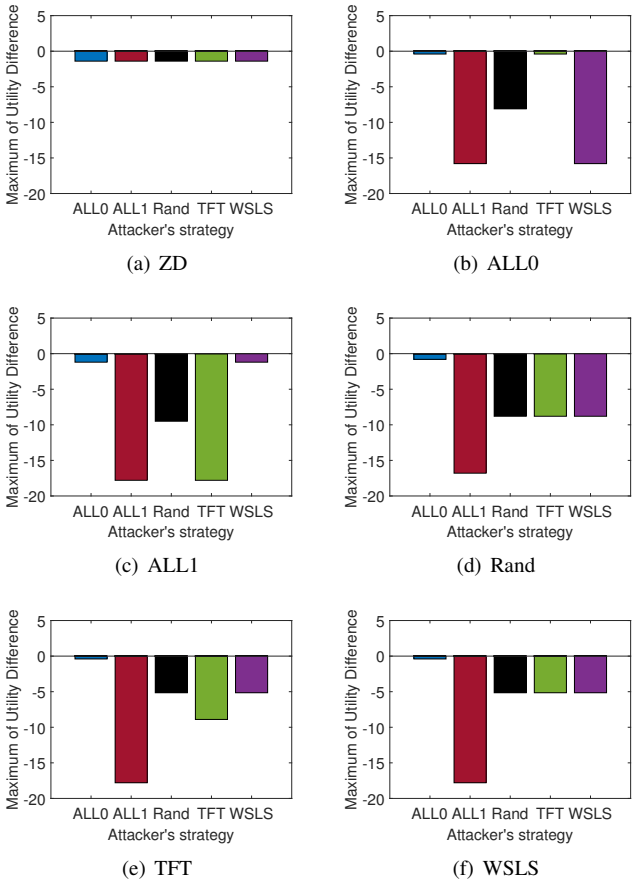


Fig. 8. Maximum of $\tilde{u}_d - \tilde{u}_a$ under different strategy combinations of the attacker and the defender in the probabilistic model.

VII. Results and Discussion

In the previous sections, we present a deterministic model and a probabilistic model to describe the sequential games in the signaling-based audit mechanism. With the help of the extended ZD strategy, we can enable the defender to unilaterally control the attacker's utility and maximize the utility difference between the defender and the attacker. However, the following limitations remain in our model assumptions and experimental design.

- **What if the attacker uses the ZD strategy?** In our experiments, we display the results of the defender's ZD strategy playing against other strategies of the attacker. However, we do not consider what would happen if the attacker also uses the ZD strategy. This may happen in an actual situation since the ZD strategy is powerful.
- **The assumption of same values for all data.** The data might have different sensitivities, reflecting different importances. Therefore, if the data protected by the defender

have different values in real situations, the proposed ZD strategy and its control capability would change, which is one of the limitations of the current assumptions.

- **Utility maximization of the defender.** Our proposed ZD strategy can achieve robust control over the attacker's utility and maximize the utility difference. However, it is not clear whether it would still work when only the defender's utility is required to be maximized.

VIII. Conclusion and Future Work

In this paper, we propose two sequential game models to describe the interaction between the defender and the attacker, where the auditing behavior of the defender is deterministic and probabilistic. Using the ZD strategy allows the defender to unilaterally control the attacker's utility no matter what strategy the attacker uses. In addition, an optimization scheme is designed for the defender based on the ZD strategy to control the utility difference between the defender and the attacker. Via comparing the ZD strategy with other classic strategies, experimental results show that the ZD strategy has better performance in controlling the attacker's utility as well as maximizing the utility difference between the defender and the attacker.

In the future, we will study the situation where the attacker also adopts the ZD strategy and consider how the defender can make better defensive actions. We are going to further consider the implementation and practicality of the ZD strategy for the audit game when the stored data have different values. Moreover, we intend to design a new strategy to maximize the defender's utility.

References

[1] A. Barth, J. Mitchell, A. Datta, and S. Sundaram, "Privacy and utility in business processes," in *20th IEEE Computer Security Foundations Symposium (CSF'07)*. IEEE, 2007, pp. 279–294.

[2] T. dailyswig, "portswigger.net," https://portswigger.net/daily-swig/data-breach-at-new-zealands-reserve-bank-after-third-party-service-hack.

[3] D. S. Terzi, R. Terzi, and S. Sagiroglu, "A survey on security and privacy issues in big data," in *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE, 2015, pp. 202–207.

[4] R. Hasan, S. Zawoad, S. Noor, M. M. Haque, and D. Burke, "How secure is the healthcare network from insider attacks? an audit guideline for vulnerability analysis," in *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, vol. 1. IEEE, 2016, pp. 417–422.

[5] J. Blocki, N. Christin, A. Datta, and A. Sinha, "Audit mechanisms for provable risk management and accountable data governance," in *International Conference on Decision and Game Theory for Security*. Springer, 2012, pp. 38–59.

[6] J. Blocki, N. Christin, A. Datta, A. Procaccia, and A. Sinha, "Audit games with multiple defender resources," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 29, no. 1, 2015.

[7] C. Yan, B. Li, Y. Vorobeychik, A. Laszka, D. Fabbri, and B. Malin, "Get your workload in order: Game theoretic prioritization of database auditing," in *2018 IEEE 34th International Conference on Data Engineering (ICDE)*. IEEE, 2018, pp. 1304–1307.

[8] H. Xu, Z. Rabinovich, S. Dughmi, and M. Tambe, "Exploring information asymmetry in two-stage security games," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 29, no. 1, 2015.

[9] S. Dughmi and H. Xu, "Algorithmic bayesian persuasion," *SIAM Journal on Computing*, no. 0, pp. STOC16–68, 2019.

[10] C. Yan, H. Xu, Y. Vorobeychik, B. Li, D. Fabbri, and B. A. Malin, "To warn or not to warn: Online signaling in audit games," in *2020 IEEE 36th International Conference on Data Engineering (ICDE)*. IEEE, 2020, pp. 481–492.

[11] M. Hedda, B. A. Malin, C. Yan, and D. Fabbri, "Evaluating the effectiveness of auditing rules for electronic health record systems," in *AMIA Annual Symposium Proceedings*, vol. 2017. American Medical Informatics Association, 2017, p. 866.

[12] A. Sinha, F. Fang, B. An, C. Kiekintveld, and M. Tambe, "Stackelberg security games: Looking beyond a decade of success." IJCAI, 2018.

[13] A. Laszka, Y. Vorobeychik, D. Fabbri, C. Yan, and B. Malin, "A game-theoretic approach for alert prioritization," in *Workshops at the Thirty-First AAAI Conference on Artificial Intelligence*, 2017.

[14] W. H. Press and F. J. Dyson, "Iterated prisoner's dilemma contains strategies that dominate any evolutionary opponent," *Proceedings of the National Academy of Sciences*, vol. 109, no. 26, pp. 10 409–10 413, 2012.

[15] C. Yan, B. Li, Y. Vorobeychik, A. Laszka, D. Fabbri, and B. Malin, "Database audit workload prioritization via game theory," *ACM Transactions on Privacy and Security (TOPS)*, vol. 22, no. 3, pp. 1–21, 2019.

[16] A. Schlenker, H. Xu, M. Guirguis, C. Kiekintveld, A. Sinha, M. Tambe, S. Sonya, D. Balderas, and N. Dunstatter, "Don't bury your head in warnings: A game-theoretic approach for intelligent allocation of cyber-security alerts," 2017.

[17] J. Blocki, N. Christin, A. Datta, A. D. Procaccia, and A. Sinha, "Audit games," *arXiv preprint arXiv:1303.0356*, 2013.

[18] D. Korzhyk, V. Conitzer, and R. Parr, "Complexity of computing optimal stackelberg strategies in security resource allocation games," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 24, no. 1, 2010.

[19] H. Kiral and H. Karabacak, "Resolution of the internal audit-based role conflicts in risk management: Evidence from signaling game analysis," *Group Decision and Negotiation*, vol. 29, no. 5, pp. 823–841, 2020.

[20] Q. Hu, S. Wang, P. Ma, X. Cheng, W. Lv, and R. Bie, "Quality control in crowdsourcing using sequential zero-determinant strategies," *IEEE Transactions on Knowledge and Data Engineering*, vol. 32, no. 5, pp. 998–1009, 2019.

[21] M. Nowak and K. Sigmund, "A strategy of win-stay, lose-shift that outperforms tit-for-tat in the prisoner's dilemma game," *Nature*, vol. 364, no. 6432, pp. 56–58, 1993.

[22] M. Posch *et al.*, "Win stay–lose shift: An elementary learning rule for normal form games," *Santa Fe Institute1997*, 1997.