information

MDPI

Article

Game Analysis of Access Control Based on User Behavior Trust

Yan Wang [1,2,*], Liqin Tian [3] and Zhenguo Chen [3]

[1] Department of Computer, QingHai Normal University, Xining 810008, China
[2] College of Physics and Electronic Information Engineering, Qinghai Nationalities University, Xining 810007, China
[3] Department of Computer, North China Institute of Science and Technology, Beijing 101601, China; tianliqin@ncist.edu.cn (L.T.); rayoo1110@163.com (Z.C.)
* Correspondence: wangy01028@126.com; Tel.: + 86-187-6997-1542

Received: 13 February 2019; Accepted: 3 April 2019; Published: 9 April 2019

Abstract: Due to the dynamics and uncertainty of the current network environment, access control is one of the most important factors in guaranteeing network information security. How to construct a scientific and accurate access control model is a current research focus. In actual access control mechanisms, users with high trust values bring better benefits, but the losses will also be greater once cheating access is adopted. A general access control game model that can reflect both trust and risk is established in this paper. First, we construct an access control game model with user behavior trust between the user and the service provider, in which the benefits and losses are quantified by using adaptive regulatory factors and the user's trust level, which enhances the rationality of the policy making. Meanwhile, we present two kinds of solutions for the prisoner's dilemma in the traditional access control game model without user behavior trust. Then, due to the vulnerability of trust, the user's trust value is updated according to the interaction situation in the previous stage, which ensures that the updating of the user's trust value can satisfy the "slow rising-fast falling" principle. Theoretical analysis and the simulation experiment both show that this model has a better performance than a traditional game model and can guarantee scientific decision-making in the access control mechanism.

Keywords: access control; user behavior trust; game theory; prisoner's dilemma

1. Introduction

Access control is one of the most important methods for guaranteeing information security. Conventional access control mechanisms, such as discretionary access control (DAC) [1,2], mandatory access control (MAC) [3,4], and role-based access control (RBAC) [5–8], satisfy the access control requirements of most service providers. However, static and predefined access control policies cannot measure user's access behavior precisely, especially because users at different levels of trust can bring about benefits or losses in different amounts [9]. Therefore, a service provider demands a reasonable and accurate access control mechanism in which the interactions between information sharing and protection bring about a socially positive result for both the service provider and its users [10]. In 1996, Blaze M [11] proposed the concept of trust management and introduced a trust mechanism into security research for the first time, thus providing a new way of solving security problems. Afterwards, the trust mechanism has been widely applied in the access control area. The basic idea in these studies is providing different access permissions according to the user's trust degree. The higher the user's trust degree, the more resources he can access. However, due to the dynamic and subjective characteristics of the trust, trust evaluation and updating is still a difficult problem.

Game theory has been applied in many research domains related to information security, including network security [12–15], intrusion detection [16,17], and access control [10,18], to move forward the development of academic research. Game theory provides a mathematical analysis method for the study of the essence of competition among entities [19,20]. There exists a game between users and the service providers who adopt a strategy to maximize their own utility. Traditional access control based on game theory [15,16] did not consider the influence of the user behavior trust value, which made the access control model lack accuracy and adaptability. Therefore, an access control mechanism that combines user trust based on game theory is established in this paper. The major contributions of this paper are summarized as follows:

- We build an access control game analysis model combining with the user's trust level, in which the trust and risk achieve unity. To the best of our knowledge, we are the first to present a utility quantification mechanism for users and the service providers, using the adaptive regulator and the user's trust level. Then, the method of decision-making based on the Nash equilibrium of the service provider is proposed. At the same time, a solution to the prisoner's dilemma in the traditional access control game model without user trust is also proposed in this paper.
- Due to the dynamic and vulnerable characteristics of trust, a novel trust updating mechanism that follows the principle "slow-rising and fast-falling" is proposed.
- The experiment shows that the user's trust value presents a slowly increasing trend on the whole with the increase of interaction times. This is because our game model has potential incentive effects on the benign collaboration between the user and the service provider.

The remainder of this paper is organized as follows: Section 2 outlines the related work about the access control model. Section 3 introduces our main work. Section 4 presents the solutions for the prisoner's dilemma in the access control game model, in which the user behavior trust is not included. Section 5 presents an access control game model combining with user behavior trust and provides the scientific basis for decision-making. Section 6 proposes a trust value updating mechanism according to the interaction situations in the previous stage and ensures that the trust value satisfies the "slow rising-fast falling" principle.

2. Related Work

Access control ensures that access requests from users to objects are validated according to predefined rules. These rules form an authorization policy and the way of defining and enforcing them constitutes an access control model [1]. Early access control model consists of discretionary access control (DAC) [1,2], in which the owner of the resource decides who can access the resource and how to access it, and mandatory access control (MAC) [3,4], in which the access rules were defined by the system. However, because of the complexity of the network environment, DAC and MAC can no longer meet the needs of actual applications. Subsequently, the role-based access control model [5,6] was proposed. Since RBAC introduces a middle layer (role) between users and permissions, the flexibility and security of access control system can be ensured, even if dealing with mass data and large-scale business, which shows a large advantage in meeting the security needs of large-scale enterprise-wide systems. Thus, the RBAC has become a hot topic in the access control research area. However, it is only fit for dealing with access control requests from predefined known users. Meanwhile, the policy is relatively static and inflexible. Due to the dynamic and stochastic features of user access behavior, researchers have proposed methods to incorporate user behavior trust into the access control system [7–9,21]. The basic idea in these studies is providing different access permissions according to the user's trust degree. Roose et al. [18] adopt three-level trust to control decision-making, but the trust evaluation mechanism is not discussed. Bhatti et al. [9] assessed trust based on the user profile, which is used for XML-based RBAC. In fact, a user with a different trust degree could bring about different risk levels. Bijon et al. [22] introduced the concept of risk in an RBAC system to prevent permission abuse. A role will be activated when the total risk does not exceed a threshold [23,24].

Researchers [25,26] combined user trust with the risk to conduct an access control study. Trust is user-related, risk is permission-related, and these two are intrinsically correlated because the users and permissions are main and indispensable elements in the access control system [10]. Trust and risk are effectively combined together in our paper and risk appears in the game model in an implicit way. In fact, the service provider and users all aim at maximizing the benefits under any circumstances. Many researchers [12–15] apply game theory to the fields of information security, which provides a scientific method of decision making. Manshaei et al. [13] discussed how to make use of game theory to control the limits of compromise. Rontidis et al. [27] proposed a decision-making system to reduce the security risks based on game theory. Researchers [20] have also used game theory to establish a privacy protection model by setting the access permission according to the privacy tolerance threshold of service providers. However, these studies lack utility quantification mechanisms related to the user behavior trust and risk. Therefore, an access control mechanism that combines the user trust level with risk based on game theory is proposed in this paper, which provides a more scientific method for controlling decisions.

3. Proposed Model

Game theory is playing an increasingly important role in information security and provides a scientific method for advanced security-related decision making. In this paper, the access control game analysis model based on the data resources of a school library is constructed wherein there are two players, the service provider and its user. When the user accesses a permission, he might bring gains or losses for the service provider. If the service provider grants the user's normal or no-cheating access request, it will bring benefits for both of them. For example, the obtaining knowledge or data resources for the user and gaining benefits or improving reputation for the service provider. However, if the service provider grants the user's malicious or cheating access request (e.g., setting up proxy servers privately or reselling data or papers to other people), it will bring extra benefits for users but bring losses for the service provider. The benefits and losses will be listed in detail as follows. The symbol definitions are shown in Table 1.

Table 1. Symbol definition.

Symbol	Definition
δ	Discount factor (the extent to which future cooperation opportunities are concerned by users)
M	Number of trust levels
β_j	adaptive regulatory factor, $\beta_j \in [0,1], (j = 1,2,\ldots 6)$
x	User's trust level $x = (1,2,\ldots M)$
p	The service provider grants the user's access request with probability of p, and deny the user's access request with probability of $1 - p$.
q	User adopting no-cheating access strategy with probability of q, and cheating access strategy with probability of $1 - q$.
q_τ	The threshold probability in the decision-making process
T_p	User's trust value after the $p-$th interaction
λ	The control factor determining the trust reduction rate in the trust updating equation $\lambda \in (0,1)$
r	The control factor determining the trust increment rate in the trust updating equation $r < \lambda$
T_{max}	Maximum Trust Value. We set $T_{max} = 1$ in this paper

The strategies of the user are cheating access and no-cheating access and the strategies of the service provider are grant and deny access. The utility of using different strategies is summarized as follows:

- $Sloss_g^c > 0$ denotes the service provider's loss for granting the user's cheating access. Examples are overloading the data resources or setting up proxy servers privately by the user.
- $Sbenefit_g^n > 0$ denotes the service provider's benefits for granting user's no-cheating access. Examples are gaining benefits by providing downloading services or enhancing a reputation through good interactions.
- $Sloss_d^n > 0$ denotes the service provider's loss for denying the user no-cheating access. An example is losing the opportunity for potential long-term cooperation.
- $Ubenefit_g^n > 0$ denotes user's benefits for no-cheating access. Examples are downloading the data resources or obtaining some knowledge in the access process.
- $Uextra_g^c > 0$ denotes user's extra benefits for cheating access. Examples are overloading or setting up proxy servers privately.

In this paper, we propose two types of access control game models, one is the game model without user trust and the other is the game model considering user trust. The major contents are as follows:

- In the first game model, all of the users' benefits are regarded as equal and different users bring the same utility to the service provider. Therefore, this game model is also regarded as the traditional access control game model. We present two kinds of solutions for the prisoner's dilemma in this game model.
- Construct access control game model considering user trust, in which the utility of the user and the service provider are quantified using user trust level x and adaptive regulatory factor β_j, and risk is reflected in an implicit way in the utility function. Afterwards, the rational decision-making conditions for the service providers by analyzing the payment matrix is established. Finally, the user's trust value is updated reasonably after each interaction.

4. Analysis of the Access Control Game Model Without User Behavior Trust

4.1. The Analysis of the Game Model

The payment matrix between the user and service provider is as follows (Table 2). Assuming that the user and service provider are completely rational, they aim to maximize their profits. It can be seen from the Table 2 that there exists a pure-strategy Nash equilibrium (cheating, deny). However, the Nash equilibrium here is contradictory with the basic principle of information communication and sharing advocated in the network. In fact, most of the users and service providers do not choose these strategies (cheating, deny). This situation is the prisoner's dilemma in a traditional game model. An important question is how to obviate the prisoner's dilemma for users and service providers to cooperate with one another to obtain more long-term future benefits.

Table 2. Payment matrix between user and service provider.

		User			
		No-Cheating		**Cheating**	
Service provider	grant	$Sbenefit_g^n$	$Ubenefit_g^n$	$-Sloss_g^c$	$Ubenefit_g^n + Uextra_g^c$
	deny	$-Sloss_d^n$	0	0	0

4.2. Presenting Two Kinds of Solutions for the Prisoner's Dilemma

To remove the prisoner's dilemma, we set up the game model on the basis of an infinite repeated game, since we do not know when the game will end. In addition, the history of the past actions of each player is observable and players not only consider the utilities generated by the current game stage, but also the utilities of future games. Therefore, we perform two possible solutions for different types of users.

1. Grim-trigger strategy.
   The service provider always grants the user's no-cheating access. Once the user adopts cheating access, the service provider will always deny the user's access request.
2. Stage grim-trigger strategy.
   The service provider always grants the user's no-cheating access request and once the user adopts the cheating access strategy, the service provider will deny the user's access request for several successive game stages. Afterwards, the service provider will grant the user access again.

Due to the characteristics of infinite repeated games, the time to obtain benefits cannot be ignored because the value of the same benefit to a user, at different time points, is not the same. Users are usually more concerned about recent benefits than future benefits. Suppose that we have a discount factor $\delta \in [0, 1]$. If δ is closer to 1, the users are more concerned about future cooperation opportunities, and vice versa.

The expected benefit of a user adopting the no-cheating access strategy is the following:

$$Ubenefit_g^n + Ubenefit_g^n \delta + Ubenefit_g^n \delta^2 + \ldots\ldots = \frac{Ubenefit_g^n}{1-\delta} \tag{1}$$

First solution (grim-trigger strategy), as follows: If a user chooses the cheating access strategy at a certain stage, he/she will obtain an extra benefit once, except normal access benefits. Afterward, the user's benefit becomes zero. A rational user will not choose cheating the access strategy if

$$\frac{Ubenefit_g^n}{1-\delta} \geq Ubenefit_g^n + Uextra_g^c \tag{2}$$

$$\text{we can get } \delta \geq \frac{Uextra_g^c}{Uextra_g^c + Ubenefit_g^n}. \tag{3}$$

Second solution (stage grim-trigger strategy), as follows: For brevity, suppose that the service provider denies the user's access for one game stage. In this case, the benefit of the user is

$$Ubenefit_g^n + Uextra_g^c + 0 \times \delta + Ubenefit_g^n \times \delta^2 + Ubenefit_g^n \times \delta^3 + \ldots\ldots = Ubenefit_g^n + Uextra_g^c + \delta^2 \frac{Ubenefit_g^n}{1-\delta} \tag{4}$$

A rational user will not choose cheating the access strategy if

$$\frac{Ubenefit_g^n}{1-\delta} \geq Ubenefit_g^n + Uextra_g^c + \delta^2 \frac{Ubenefit_g^n}{1-\delta} \tag{5}$$

$$\text{we can get } \delta \geq \frac{Uextra_g^c}{Ubenefit_g^n}. \tag{6}$$

Discount factor δ denotes the extent to which future cooperation opportunities are concerned by users. The larger the value of δ is, the more the user cares about the future cooperation opportunities. It can be seen from Equations (3) and (6) that using stage grim trigger strategy requires a higher discount factor δ than using grim trigger strategy. Therefore, the number of denial times of the service provider is inversely proportional to the discount factor. This arrangement means the users who care little about future cooperation opportunities receive greater punishment than the users who are more concerned about future cooperation opportunities, which is consistent with the phenomenon that is present in society.

5. Constructing an Access Control Game Model with User Behavior Trust

This approach is due to the above game model, in which all of the users' benefits are regarded as equal. In fact, in the actual access control system, the cooperation between the service provider and the user will be deeper with an increase in the user's trust value. Correspondingly, the service providers will provide those users who hold high a trust value with more access to resources and higher-level access permissions. Therefore, normal cooperation will bring about more benefits to those users and service providers. However, once the users with high trust value adopt the cheating access strategy, the extra benefits will be even higher and the losses or the risks of the service providers will become more serious. Thus, trust and risk coexist in access control. From another perspective, users with a high trust values will also bring greater risks. Under these circumstances, the service providers should punish the deceptive users severely, such as reducing their trust value fast. Based on all of the above, designing a game model that can reflect both trust and risk is necessary.

5.1. Establishing a Payment Matrix for the Service Provider and User

In this game model, we assume that the user with a high trust value will bring greater benefits than the user with a low trust value for both the user and service provider when he/she adopts the no-cheating access strategy and will also result in more serious losses or risks for service provider once the cheating access strategy is adopted. This assumption is consistent with the overall phenomenon in the actual access control process.

We divide the user's trust value into M levels, assuming that the user's trust level is denoted by x, $(x = 1, 2 \ldots M)$. The trust level is inversely proportional to the trust value ($x = 1$ denotes total trust or the highest level of access permission, while $x = M$ denotes total distrust or the lowest level of access permission). Thus, we can obtain the payment matrix of the service provider and user, as shown in Table 3.

Table 3. Payment matrix between user and service provider with user trust.

		User	
		No-Cheating	**Cheating**
Service provider	grant	$Sbenefit_g^n\beta_2^{x-1}$ $Ubenefit_g^n\beta_4^{x-1}$	$-Sloss_g^c\beta_1^{x-1}$ $Ubenefit_g^n\beta_4^{x-1} + Uextra_g^c\beta_5^{x-1} - Upunish\beta_6^{x-1}$
	deny	$-Sloss_d^n\beta_3^{x-1}$ 0	0 $-Upunish\beta_6^{x-1}$

$Upunish$ denotes the punishment for the user cheating access, while $\beta_j \in [0,1]$, $(j = 1, 2 \ldots \cdot 6)$ denotes the adaptive regulatory factor of the game analysis, which depends on the granularity of the trust division and the differences between the utilities of each access permission. The service provider should increase the value of β_j if the differences between the utilities of each access permission is relatively small, and vice versa. Our game model is in line with our hypothesis. Taking $Sbenefit_g^n\beta_2^{x-1}$ as an example, owing to $\beta_j \in [0,1], x \in \{1, 2 \ldots \cdot 6\}$, β_j^{x-1} is a monotonically decreasing function of x. In addition, the trust level x is inversely proportional to the trust value of the user, so β_j^{x-1} is proportional to the user's trust value. Therefore, $Sbenefit_g^n\beta_2^{x-1}$ increases with an increase in the user's trust value.

5.2. Game Analysis Based on the User's Trust Level

It can be obtained, through the lineation method, that there is no pure strategy equilibrium in this game model. However, we can obtain the Nash equilibrium of the mixed strategy. Assume that the service provider grants an access request with the probability of p and denies an access request with the probability of $1 - p$. Then, the mixed strategy of the service provider is $P = (p, 1 - p)$. Assume that the user adopts a cheating access strategy with the probability of q and a no-cheating access strategy with the probability of $1-q$. Therefore, the mixed strategy of the user is $Q=(q,1-q)$. The expected utility of the user when adopting no-cheating access strategy is

$$U_n = p \times Ubenefit_g^n \beta_4^{x-1} + (1-p) \times 0 \tag{7}$$

The expected utility of the user when adopting cheating access strategy is

$$U_c = p(Ubenefit_g^n \beta_4^{x-1} + Uextra_g^c \beta_5^{x-1} - Upunish\beta_6^{x-1}) + (1-p) \times Upunish\beta_6^{x-1} \tag{8}$$

Thus, the average utility of the user is

$$E_u = q \times U_c + (1-q) \times U_n = pqUextra_g^c \beta_5^{x-1} + pUbenefit_g^n \beta_4^{x-1} - qUpunish\beta_6^{x-1} \tag{9}$$

The first-order optimality conditions are obtained by solving the following differential equations:

$$\frac{\partial E_u}{\partial q} = pUextra_g^c \beta_5^{x-1} - Upunish\beta_6^{x-1} = 0 \tag{10}$$

then, we obtain

$$p^* = \frac{Upunish\beta_6^{x-1}}{Uextra_g^c \beta_5^{x-1}}. \tag{11}$$

Thus, $(p^*, 1-p^*)$ is the Nash equilibrium of the mixed strategy of the service provider. It can be seen from Equation (11) that the grant probability of the service provider is only related to the extra benefit and punishment that the user receives by cheating access. Therefore, the service provider who wants to improve the probability of grant access should increase the punishment and reduce the extra benefits for the user who adopts the cheating access strategy. In the same way, we can obtain the Nash equilibrium of the mixed strategy of the user.

$$q^* = \frac{\left(Sbenefit_g^n \beta_2^{x-1} + Sloss_d^n \beta_3^{x-1}\right)}{\left(Sloss_g^c \beta_1^{x-1} + Sbenefit_g^n \beta_2^{x-1} + Sloss_d^n \beta_3^{x-1}\right)} \tag{12}$$

So, $(q^*, 1-q^*)$ is the Nash equilibrium of the mixed strategy of the user.

5.3. Decision-Making Conditions for Service Providers

In the access control mechanism, the high-frequency denial of access will affect the reputation of the service provider, but the low-frequency denial of access will not achieve the purpose of alleviating abuse. We have obtained the Nash equilibrium of mixed strategy, both for the user and the service provider. In game theory, there are many discussions and controversies about mixed strategy. We prefer to adopt the view in literature [19] that the Nash equilibrium of mixed strategy is the common belief in the opponent's eyes. For example, the service provider's Nash equilibrium is $(p^*, 1-p^*)$, which means that the user believes that the service provider grants access strategy at probability p^*. Therefore, to implement an access control decision, the service provider defines a threshold q_τ in order to increase their own benefits and control the rate of denial rationally. The threshold q_τ satisfies the equation as follows:

$$-q_\tau Sloss_g^c \beta_1^{x-1} + (1-q_\tau) Sbenefit_g^n \beta_2^{x-1} = 0. \tag{13}$$

The left side of the equation denotes the utility of the service provider granting the access request. If the probability of the user's no cheating access $q \le q_\tau$, then the utility of the service provider is greater than zero. In this case, the service provider should grant the user's access request, otherwise, deny the user's access request. This method can control the denial frequency reasonably, under the condition of ensuring the profits of the service provider.

6. The Update of User Trust Behavior Value

The service provider must update the user's trust value according to the utility of each game and the user's access strategy. It is agreed that trust has a characteristic of vulnerability. Take trust in interpersonal communication as an example, the trust between people is established through good interaction for a long time, which reflects that the establishment of trust is a slow process. However, as long as a malicious deception or behavior occurs, the trust between them may be easily destroyed. In this paper, we will update the user's trust value after each interaction and the trust update mechanism follows the "slow-rising and fast-falling" principle, which is consistent with the vulnerability characteristic of trust. Note that the user's initial trust value is set to be zero and the trust value is updated on the basis of the user's strategy in the previous stage.

(1) Rising (owing to the user's no-cheating access),

$$T_{p+1} = T_p + \frac{x \cdot \gamma}{10}^{\frac{T_p}{T_{\max}}} \tag{14}$$

where $T_{p+1} \in [0, 1]$ denotes the $(p+1)th$ trust value. The value $T_{\max}$ denotes the maximum of the trust value, $T_{\max} = 1$ in this paper. Here γ denotes the factor for controlling the rate of the rise and it is a dynamic or fixed value determined by the service provider. In this paper, we set $\gamma \leq 0.5$.

(2) Falling (owing to the user's cheating access),

$$T_{p+1} = T_{p+1} - \frac{x \cdot \lambda}{10}^{\frac{T_p}{T_{\max}}} \tag{15}$$

where λ denotes the factor for controlling the rate of falling. In this paper, we set $\lambda \leq 1$. It is worthwhile to note that λ should be always be larger than γ because the trust value is difficult to increase but easy to decrease, which can reflect the vulnerability of trust.

7. Simulation and Example

7.1. Experimental Background

In order to evaluate our game model, a simulated data resource service of the digital library is constructed, where the users and service providers refer to the school students and database suppliers, respectively. User identity authentication is based on the user's IP address. As long as the user's IP address is within the legal range, the user can access the database. However, identity authentication only is not enough, because legitimate users can seek extra profits through excessive downloads or setting up a server privately, and this malicious behavior will damage the interests of the database suppliers. Here, the identity authentication is out the scope of our research. We only discuss the behavior authentication of legitimate users. In our game model, 50 legitimate students interact with the database suppliers, assuming that they are all rational and aiming at maximizing their own profits. They are divided into two equal groups, X1 and X2. Students in group X1 use the traditional access control game model and students in group X2 use our proposed game model with user trust. The two types of game models are analyzed below.

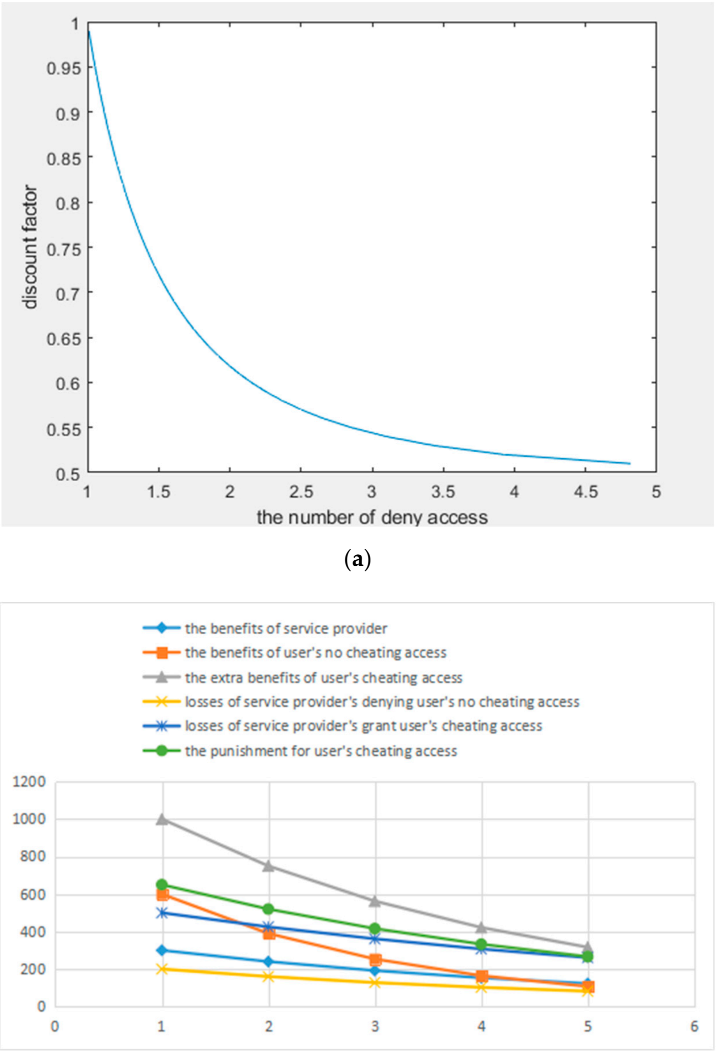
7.2. Simulation Analysis

7.2.1. The Relationship Between the Discount Factor and the Number of Denials-of-Access in the Traditional Game Model

We randomly set a different discount factor δ for these users of group X1 in this game model. The simulation result is shown in Figure 1a, which elaborates a scenario where there is a smaller number of times that the users are denied if they are more concerned about future cooperation opportunities. This simulation result is consistent with that confirmed by our theory.

7.2.2. Simulations in the Game Model with User Behavior Trust

To simplify the analysis, the service provider divides the trust value into 5 levels, ($x = 1, 2, \ldots 5$; $x = 1$ denotes total trust or the highest level of access permission, and $x = 5$ denotes total distrust or the lowest level of access permission). Adaptive regulatory factors $(\beta_1 \ldots \beta_6)$,in the game analysis model, are set as 0.8, 0.65, 0.8, 0.85, 0.75, and 0.8, respectively. The initial value of instance parameters and the calculated result value are listed in Table 4.



(**a**)

(**b**)

Figure 1. (**a**) The relationship between discount factor and the number of denial times of the service provider in the access control game model without user trust; (**b**) The utility curve of the user and the service provider based on the user's trust level.

Table 4. The initial value and calculated result value.

Trust Level	1	2	3	4	5	Trust Level	1	2	3	4	5
$Sbenefit_g^n$	300	240	192	154	123	$-Sloss_d^n$	700	595	506	430	365
$Ubenefit_g^n$	600	390	254	165	107	$Uextra_g^c$	1000	750	563	422	316
$-Sloss_g^c$	200	160	128	102	82	$Upunish$	650	520	416	333	266

Figure 1b illustrates a scenario in which the benefits and the losses will rise with an increase of the user's trust value, for both the user and the service provider. Therefore, the service provider should consider the profits and losses comprehensively to decide whether to grant the user's access requests, not only based on the user's trust value. Figure 2 shows the relationship between the mixed strategy Nash equilibrium and the user's trust level, which illustrates that the user's deception probability is inversely proportional to the user's trust value, in the eyes of the service provider.

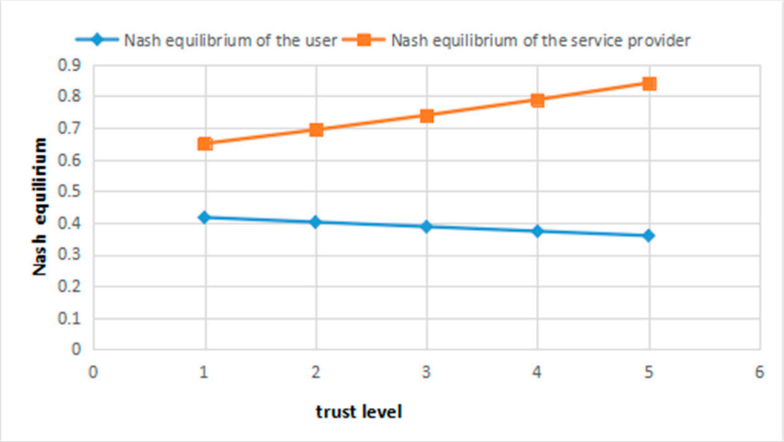


Figure 2. The Nash equilibrium strategy of the service provider and the user, based on the user's trust level.

In order to evaluate the effectiveness of our access control game model with user trust, we have performed some experiments to compare it with a traditional access control game model. The evaluation metric is the utility obtained by the database suppliers and the trust value changes of the students. Both groups of students take a no-cheating access strategy with an initial probability of 0.5. For the sake of fairness, the utility in the traditional game is equal to that in our proposed game, when the user with middle trust level $x = 3$ and $\gamma = 0.3, \lambda = 0.4$ in the trust update method. We repeat the game 100 times and randomly select 15 consecutive access stages. We repeat this experiment 30 times and calculate the average trust value. The utility comparison of the service providers in this scenario is shown in Figure 3 and variation of average trust value is shown in Figure 4.

From Figure 3, it is obvious that the average utility in our proposed game is higher than that in the traditional game. Besides, the utilities of the service provider in these two types of game models are both generally moving in the better direction. From Figure 4, we can see that the trust values of the users increase slowly with the number of interactions. It is because the service provider will provide those users who hold a high trust value with more access to resources and higher-level access permissions, which has an incentive effect on the increase of user trust value.

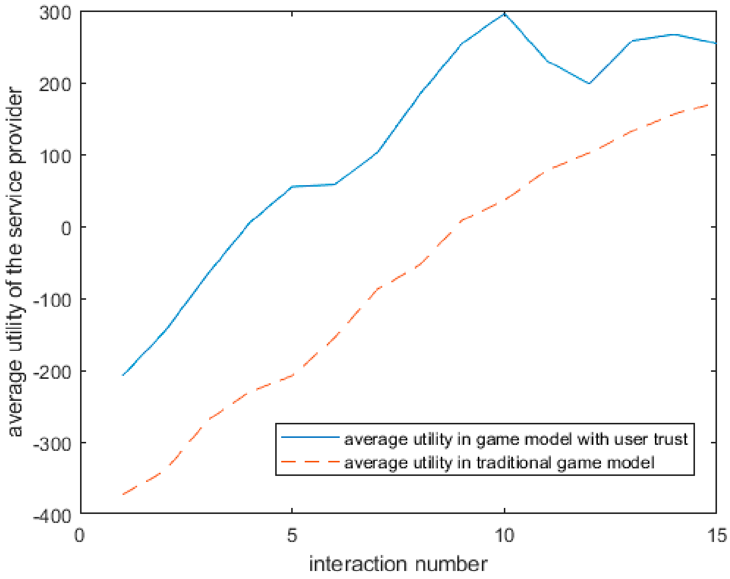


Figure 3. Utility comparison curves between the traditional game and the proposed game with user trust.

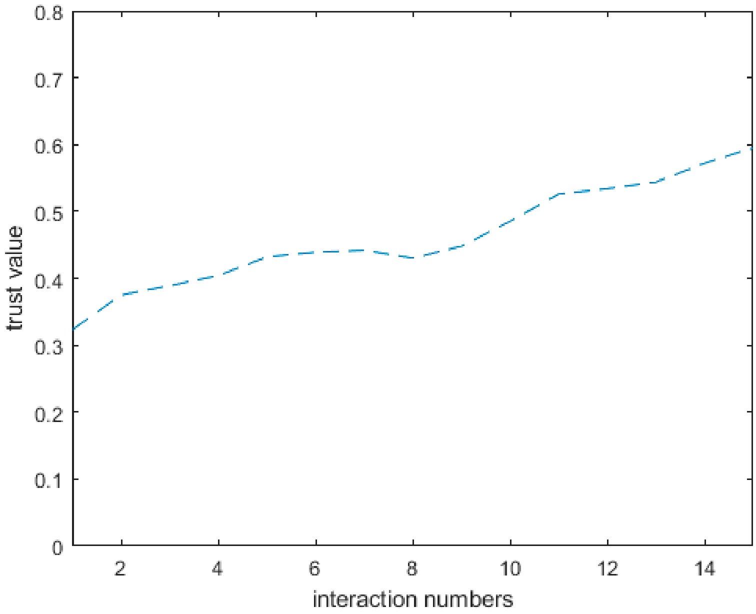


Figure 4. The variation of the average trust value with the increase of interaction numbers in the game model considering user trust.

8. Conclusions

This paper discusses access control mechanisms in the current network environment and proposes two types of general access control game models, as follows: The game model without user trust and the game model considering user trust. Meanwhile, this paper proposes two kinds of solutions for the prisoner's dilemma in the traditional access control game model. What's more, we not only quantify the utility of the service provider and the user using the adaptive regulator $(\beta_1 \ldots \beta_6)$ and the user's trust level, but also unify trust and risk in the access control game model with user trust. The simulation results reveal that the average trust values of the users rise slowly with the increase of interaction times. This approach ensures the scientific decision-making and the rational updating of the user's trust value and, more importantly, our model has an incentive effect on the increase of user trust, which is helpful to shape the user's behavior for better future utilities. Therefore, it has important guiding significance in actual access control.

However, our game model is based on the assumption that the users are all completely rational, which is difficult to guarantee in the real access control process. In future research, we intend to build an evolutionary game model in which both sides are bounded rationality and to analyze how to obtain the evolutionary stable strategy (ESS) in an access control game model.

Author Contributions: Y.W., Z.C. designed the experiments and analyzed the data; Y.W., L.T. designed the structure and conceived the idea of this paper; Y.W. wrote the paper.

Funding: This research was funded by "The national key research project (No.2017YFC0804108)", "Key Research Program of Qinghai Province (No.2017-ZJ-752,2017-ZJ-Y21)"and "Hebei IoT Monitoring Engineering Technology Research Center (3142016020)".

Acknowledgments: The authors would like to thank all anonymous reviewers and editors for their helpful suggestions for the improvement of this paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Lampson, B.W. Protection. In Proceedings of the 5th Annual Princeton Conference on Information Sciences and Systems, Princeton, NJ, USA, 25–26 March 1971; pp. 437–443.
2. Graham, G.S.; Denning, P.J. Protection: Principles and Practice. In Proceedings of the Spring Joint Computer Conference ACM, Atlantic City, NJ, USA, 16–18 May 1972.
3. Sandhu, R.S. Lattice-based access control models. *Computer* **1993**, *26*, 9–19. [CrossRef]
4. Bell, D.E.; LaPadula, L.J. *Secure Computer Systems: Mathematical Foundations*; The MITRE Corporation: Bedford, MA, USA, 1973.
5. Sandhu, R.S.; Coyne, E.J.; Feinstein, H.I. Role based access control models. *Computer* **1996**, *29*, 38–47. [CrossRef]
6. Liu, W.; Sun, Y.F. Role-based access control model and its Implementation in Operating System. *Comput. Sci.* **2003**, *30*, 254–265.
7. Li, N.H.; Mitchell, J.C.; Winsborough, W.H. Design of a role based trust management framework. In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, USA, 12–15 May 2002; pp. 114–130.
8. Chakraborty, S.; Ray, I. TrustBAC: Integrating trust relationships into the RBAC model for access control in open systems. In Proceedings of the 11th ACM Symposium on Access Control Models and Technologies, Lake Tahoe, CA, USA, 7–9 June 2006; pp. 49–58.
9. Bhatti, R.; Bertino, E.; Ghafoor, A. A trust-based context-aware access control model for Web-services. In Proceedings of IEEE International Conference on Web Services. *Distrib. Parallel Databases* **2005**, *18*, 83–105. [CrossRef]
10. Helil, N.; Halik, A.; Rahman, K. Non-zero-sum cooperative access control game model with user trust and permission risk. *Appl. Math. Comput.* **2017**, *307*, 299–310. [CrossRef]
11. Blaze, M.; Feigenbaum, J.; Lacy, J. Decentralized Trust Management. In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, USA, 6–8 May 1996.
12. Liang, X.; Xiao, Y. Game theory for network security. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 472–486. [CrossRef]
13. Manshaei, M.H.; Zhu, Q.; Alpcan, T.; Bacşar, T.; Hubaux, J.-P. Game theory meets network security and privacy. *ACM Comput. Surv.* **2013**, *45*, 25. [CrossRef]
14. Roy, S.; Ellis, C.; Shiva, S.; Dasgupta, D.; Shandilya, V.; Wu, Q. A survey of game theory as applied to network security. In Proceedings of the Forty-Third Hawaii International Conference on System Sciences (HICSS), Honolulu, HI, USA, 5–8 January 2010; pp. 1–10.
15. Grossklags, J.; Christin, N.; Chuang, J. Secure or Insure? A game-theoretic analysis of information security Games. In Proceedings of the 17th International Conference on World Wide Web, Beijing, China, 21–25 April 2008; pp. 209–218.

16. Alpcan, T.; Basar, T. A game theoretic approach to decision and analysis in network intrusion detection. In Proceedings of the Forty-Second IEEE International Conference on Decision and Control, Maui, HI, USA, 9–12 December 2003; pp. 2595–2600.
17. Zonouz, S.A.; Khurana, H.; Sanders, W.H.; Yardley, T.M. RRE: A game-theoretic intrusion response and recovery engine. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *25*, 395–406. [CrossRef]
18. Roos, A.; Drüsedow, S.; Hosseini, M.I.; Coskun, G.; Zickau, S. Trust Level Based Data Storage and Data Access Control in a Distributed Storage Environment. In Proceedings of the IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, San Francisco, CA, USA, 30 March–3 April 2015.
19. Osborne, M.J.; Rubinstein, A. *A Course in Game Theory*; MIT Press: Cambridge, MA, USA, 1994.
20. Zhang, Y.X.; He, J.S. A Privacy Protection Model Based on Game Theory. *Chin. J. Comput.* **2016**, *39*, 615–627.
21. Lin, G.Y.; He, S.; Huang, H. Access control security model based on behavior in cloud computing environment. *J. China Inst. Commun.* **2012**, *33*, 59–66.
22. Bijon, K.Z.; Krishnan, R.; Sandhu, R. Risk-aware RBAC sessions. *Inf. Syst. Secur.* **2012**, *76*, 59–71.
23. Díaz-López, D.; Dólera-Tormo, G.; Gómez-Mármol, F.; Martínez-Pérez, G. Dynamic counter-measures for risk-based access control systems: An evolutive approach. *Futur. Gener. Comput. Syst.* **2016**, *55*, 321–335. [CrossRef]
24. Santos, D.R.D.; Marinho, R.; Schmitt, G.R.; Westphall, C.M.; Westphall, C.B. A Framework and Risk Assessment Approaches for Risk-based Access Control in the Cloud. *J. Netw. Comput. Appl.* **2016**, *74*, 86–97. [CrossRef]
25. Helil, N.; Kim, M.; Han, S. Trust and risk based access control and access control constraints. *KSII Trans. Internet Inf. Syst.* **2011**, *5*, 2254–2271. [CrossRef]
26. Baracaldo, N.; Joshi, J. A trust and risk aware RBAC frame-work: tackling insider threat. In Proceedings of the 17th USA Conference on Access control Models and Technologies, Newark, NJ, USA, 20–22 June 2012; pp. 167–176.
27. Rontidis, G.; Panaousis, E.; Laszka, A.; Dagiuklas, T.; Malacaria, P. A game-theoretic approach for minimizing security risks in the Internet-of-Things. In Proceedings of the 2015 IEEE International Conf on Communication Workshop (ICCW), London, UK, 8–12 June 2015; pp. 2639–2644.