Network Attack and Defense Game Theory Based on Bayes-Nash Equilibrium

Liang Liu[1], Cheng Huang[1*], Yong Fang[1] and Zhenxue Wang[2]
[1] College of Cybersecurity,Sichuan University,
Chengdu, Sichuan, P.R.China
[e-mail: liangzhai118@163.com]
[e-mail: opcodesec@gmail.com]
[e-mail: yfang@scu.edu.cn]
[2] College of Electronics and Information Engineering, Sichuan University,
Chengdu, Sichuan, P.R.China
[e-mail: 2272150119@qq.com]
*Corresponding author: Cheng Huang

Received December 4, 2018; revised March 20, 2019; accepted May 4, 2019; published October 31, 2019

Abstract

In the process of constructing the traditional offensive and defensive game theory model, these are some shortages for considering the dynamic change of security risk problem. By analysing the critical indicators of the incomplete information game theory model, incomplete information attack and defense game theory model and the mathematical engineering method for solving Bayes-Nash equilibrium, the risk-averse income function for information assets is summarized as the problem of maximising the return of the equilibrium point. To obtain the functional relationship between the optimal strategy combination of the offense and defense and the information asset security probability and risk probability. At the same time, the offensive and defensive examples are used to visually analyse and demonstrate the incomplete information game and the Harsanyi conversion method. First, the incomplete information game and the Harsanyi conversion problem is discussed through the attack and defense examples and using the game tree. Then the strategy expression of incomplete information static game and the engineering mathematics method of Bayes-Nash equilibrium are given. After that, it focuses on the offensive and defensive game problem of unsafe information network based on risk aversion. The problem of attack and defense is obtained by the issue of maximizing utility, and then the Bayes-Nash equilibrium of offense and defense game is carried out around the security risk of assets. Finally, the application model in network security penetration and defense is analyzed by designing a simulation example of attack and defense penetration. The analysis results show that the constructed income function model is feasible and practical.

Keywords: Bayes-Nash, Nash equilibrium, network attack and defense, game theory, Bayes

1. INTRODUCTION

With the rapid development and popularisation of Internet technology, the cybersecurity has developed from a series of technical problems to a strategic concept [1-2]. Globalization and the Internet give individuals, organizations, and countries amazing new capabilities based on the continuous development of network technologies. Meanwhile, information collection, communications, fundraising, and public relations have all gone digital. As a result, all political, economic and military conflicts now have a cyber dimension whose scope and impact are hard to predict. Battles in cyberspace may be more important than any other on the ground. For this reason, cyber-attacks capabilities and cyber defense levels will determine the outcome of a cyber war game. All in all, the Internet makes the distance of world grow short, and cyber confrontation has become a serious strategic issue for all countries in the world.

Both the network attack and defense are carried out around the information assets of the target network. The result is related to the utility (revenue) function of both parties, and the utility (revenue) function is not only a function of the security risk probability of the target network system but also a function of the strategic combination of both attacking and defending parties [3-5]. Therefore, when constructing the network attack and defense game model, the change of the security risk probability of the target network system should be considered. At the same time, we should also consider the impact of the strategic combination of both offensive and defensive sides on the overall performance of the system.

This paper is going to present the function between the optimal strategic combination (Bayes-Nash equilibrium point) of the two parties, the security probability and risk probability of information assets based on incomplete information game model and engineering mathematics method to solve Bayes-Nash equilibrium. In this paper, we mainly study how to construct the risk-averse utility (revenue) function for information assets, and reduce the solution of equilibrium point to the problem of maximizing utility (revenue).

Information imperfection game model is common in cyber warfare, and most policymakers are risk-averse. If both the attacking and defending parties have accurate knowledge of the game situation and the game benefits, it is called the complete information attacking and defending game. If the above requirements are not met, it is incomplete information attacking and defending game [6-8]. Also, if both the offensive and defensive parties have observed and remembered the behaviour schemes chosen by both parties before, it is called the perfect information game [9-10]. Otherwise, it is called imperfect information game. Harsanyi proposed a way to handle the incomplete information game between 1967 and 1968, which is widely introduced in other research [11-14]. His method translates incomplete information into imperfect information by introducing virtual player zero, which is “nature”. This transformation is called the Harsanyi conversion, which is very important for studying the problem of the uncertain game model [15-21].

At present, research on network security based on the information game has made some progress, but most of the models applied in the cybersecurity are based on the complete information game theory. Wei J and his team [22] uses privileged state to construct the complete information game model. LYE [23] analyzes the strategic interaction between attackers and defenders through complete information game. WEI L [24] proposes a complete information stochastic game method to protect the power grid from the attacks. LEI [25] studies the incomplete model but does not address the applicability of benefit functions. In our paper, by the above research, we build the incomplete information game model and

Bayesian-Nash equilibrium solution. We also propose the revenue function model under different scenarios, so as to obtain the relationship between the optimal strategic combination and the risk probability. More importantly, different from the laboratory environment simulation of many researches, this paper makes the game analysis with actual cases.

Our innovations are as follows:

(1) The incomplete information game and the transformation of Harsanyi are discussed intuitively through an attack and defense example.

(2) The strategy formulation of incomplete information static game and the engineering mathematics method are proposed to solve Bayes-Nash equilibrium.

(3) The problem of incomplete information network attack and defense game based on risk aversion is mainly discussed.

The remainder of this paper is organized as follows: Section 2 discussed the incomplete information game and Harsanyi conversion. The strategy formulation and Bayes-Nash equilibrium are explained in Section 3. This is followed by incomplete information attack and defense game model based on risk aversion in Section 4. Finally, application examples and simulation analysis in Section 5.

2. INCOMPLETE INFORMATION GAME AND HARSANYI CONVERSION

The main research method of this paper is to discuss and deduce the incomplete information game and several core issues in the complex attack and defense environment. This paper studies from the perspective of decision making, including attackers, defenders and network points. By deducing the strategy choices of different decision makers in the incomplete information game, the game problem is discussed in depth.

The example assumes that the target network system has a defender and a potential attacker. The defending party decides to adopt two strategies that are defensive or non-defensive, and the attacking party decides whether to launch an attack against the target network. We know that cyber defense is costly, including high and low costs. Suppose the attacker does not know whether the defense cost is high or low, but the defender knows it. The benefits of this game model are shown in **Table 1**. The benefits of attacking party depend on whether the defense adopts a defensive strategy, not directly on the cost of defense. It is profitable for an attacker to choose to attack if and only if the defender chooses not to defend. However, the choice of defense depends on the defense cost.

Table 1. An attack and defense game of incomplete information (strategic)

Benefits when defense costs are high

	Attack	**Non-attack**
Defense	(0,-1)	(2, 0)
Non-defense	(2, 1)	(3, 0)

Benefits when defense costs are low

	Attack	**Non-attack**
Defense	(1.5,-2)	(3.5, 0)
Non-defense	(2, 1)	(3, 0)

A common approach In this case, the attacker seems to be playing with two different defenders, one the high-cost and the other a low-cost defensive guard. Generally, if the defender has possible different cost functions, it means the attacker seems to be playing with different guards. Before 1967, game theorists argued that such problems were impossible to

analyze because the rules of a game were not defined when a player did not know whom he was playing with. It was not to solve the problem until 1967-1968 that Harsanyi proposed his conversion.

In order to simulate and handle the problem of incomplete information game, we introduce the virtual player "0", namely "nature" according to Harsanyi's method. "Nature" first chooses the type (defense cost) of the defender. In this transition game, the attacker's incomplete information about the defender's defense costs becomes imperfect information about "natural" action, so that the transition game can be analysed using standard techniques.

The conversion from incomplete information game to imperfect information game is shown in Figure 1. In the figure, "0" stands for "nature", "1" for defender, "2" for attacker, the numbers in brackets for the probability of "nature" action, and the numbers in parentheses for the benefits of game (the numbers on the left represent the benefits of the defense side, and the numbers on the right represent the benefits of the attack side). Also, the figure contains an implicit standard assumption that the attacking and defending parties have a consistent judgment of the probability distribution of "natural" action (although this is a standard assumption. It makes more sense for a "natural" action to represent a public event, such as cybersecurity than the action to describe a personal feature, such as the benefits of person). Once this hypothesis is adopted, the problem will convert a standard game model. Thus the standard game model can be handled with the concept of Nash equilibrium. The Bayes equilibrium (or Bayes-Nash equilibrium) of Harsanyi refers to the equilibrium of the imperfect information game.

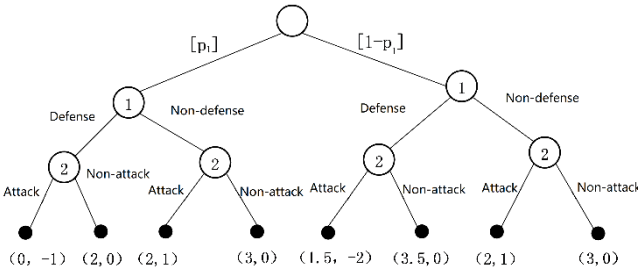

Fig. 1. The transformation of incomplete information game to imperfect information game (game tree)

In **Table 1**, x represent the probability that defenders choose to defense the attack when the defense cost is low (it is irrational for the guards to select protection when the defense cost is high). y represent the probability that the attacker decides to launch an attack. The optimal strategy of the attacker is, if $x < \frac{1}{2(1-p_1)}$, then $y = 1$ (attack). If $x > \frac{1}{2(1-p_1)}$, then $y = 0$ (non-attack). If $x = \frac{1}{2(1-p_1)}$, then $y \in [0,1]$. Similarly, the defense's optimal response at low defense costs is, if $y < \frac{1}{2}$, then (defense). If $y > \frac{1}{2}$, then $x = 0$ (non-defense). If $y = \frac{1}{2}$, then $x \in [0,1]$. To solve the Bayes-Nash equilibrium, we need to find a group of (x, y) that make x is the optimal strategy of the defender when the defense cost is low. Meanwhile, the optimal strategy of the attacker is given in the case of the attacker's judgment p_1 about the defense situation and the strategy of the defense party. For example, for any p_1, the policy portfolio $(x = 0, y = 1)$ is a balance (that is the defender is not defending, and the attacker is attacking).

If and only if $p_1 \le \frac{1}{2}$, the strategic combination $(x=1, y=0)$ constitutes a balance (that is, when the defense cost is low, the defender chooses to defense and the attacker abandons the attack).

From the above example, the basic approach to the Harsanyi conversion can be summarized as follows:

(1) Introduce a virtual person, namely "nature" or "god", he does not have to think about his gains and losses. His only role is to give players the type vector $\theta = (\theta_1, \theta_2, \ldots, \theta_n)$ in the game. Where $\theta_i \in \Theta_i$ Θ_i is called available type space. It is a complete description of the characteristics of person i.

(2) The virtual person "nature" tells the true type θ_i of person i to himself, but does not let other persons know. However, "nature" will tell each person the probability distribution $p(\theta_1, \theta_2, \ldots, \theta_n)$ on $\theta = (\theta_1, \theta_2, \ldots, \theta_n)$.

(3) All roles make choices at the same time. The strategy s_i is selected from the strategy space S_i by the players, where the strategy space of player i is related to the type space θ_i of player i, generally denoted as $S_i(\theta_i)$.

(4) The payment (revenue) function for all players except "nature" is:

$$u_i = u_i(S_1, S_2, \ldots, S_n; \theta_i), \ i = 1, 2, \ldots, n$$

According to the "nature" action, the static game of incomplete information is converted into a complete but imperfect information game. The game consists of two stages, the first is the preparatory stage. In this stage, the "nature" takes action, and it determines the probability vector $p(\theta_1, \theta_2, \ldots, \theta_n)$. The second stage is the actual game stage. Players n will move simultaneously. Although they know the type that "nature" had chosen for themselves, they did not know the type that "nature" had chosen for other people (at least one other person). So at least one player in the bureau has an imperfect message about "natural" action. However, the type space of each person and its probability distribution are common knowledge. In this way, we can analyse the problem of incomplete information game by the probability theory (especially "Bayes' rule").

With the Harsanyi conversion, in example 1, "nature" determines that the defender has two types that are $\theta_1 = (\theta_{11}, \theta_{12})$. In this formula, θ_{11} stands for high defense cost and θ_{12} stands for low cost. "Nature" determines that attackers have a type that is $\theta_2 = (\theta_{21})$. If the defender belongs to type θ_{11} (high defense cost) and the attacker has only one type θ_{21}, it constitutes a static complete information game on the left side of **Table 1**. In contrast, if the defender belongs to type θ_{12} (low defense cost), and the attacker has only one type θ_{21}, it constitutes a static complete information game on the right side of **Table 1**.

The defense knows its type, and the attacker does not know the type of defense. However, in our research, both the offense and defense have consistent judgments about the probability distribution of the defense type determined by "nature".

3. STRATEGY FORMULATION AND BAYES-NASH EQUILIBRIUM

In the previous chapter, we introduced the standard solution to incomplete information, which is the Harsanyi conversion. In this solution, the incomplete information game is transformed into the game under different players. Thus the game results can be solved. However, the effect depends on the type of player in the situation. We give the following definitions in the paper:

Definition 3.1 The type set of players is the set of information about their own decision-making characteristics in the game. All the elements of this set of information types are called the types of player in the bureau. Each player does not hope that other players know exactly which type the player is.

Definition 3.2 Incomplete information static game includes the following four elements:

The set of players $\underline{N} = \{1, 2, \ldots, n\}$

Each player's type space $\Theta_i = \{\theta_i\}, i \in \underline{N}$. Moreover, probability distribution $p(\theta_1, \theta_2, \ldots, \theta_n)$ in the total type space $\Theta_i = \{\theta_i\}, i \in \underline{N}$.

Each player has a policy set $S_i = \{s_i\}, i \in \underline{N}$ associated with its type θ_i . Moreover, the policy set S_i is independent of the other players' type θ_i .

Each player has its revenue function $u_i(s_1, s_2, \ldots, s_n; \theta_i)$, which depends not only on the strategy combination $(s_1, s_2, \ldots, s_n)$ but also on its type.

All four elements are common knowledge. In the situation, each participate chooses strategies to maximize their benefits.

This game is called incomplete information static game, also known as Bayes static game [7]. The game model can be expressed by the following formula:

$$G = [\ \underline{N}, \{\ \Theta_i\ \},\ p\ , \{\ S_i(\theta_i)\ \}, \{\ u_i\ \}\ ] \tag{1}$$

In the formula, $\underline{N}\{1, 2, \ldots, n\}$ is the set of players. Θ_i is the type set of player i and $\forall i \in \underline{N}$. Θ is the probability distribution function on all type space p . $S_i(\theta_i)$ is the strategy set of player i . When the type θ_i of i changes, so does S_i and similarly $\forall i \in \underline{N}$. u_i is the revenue function of player i . It depends on the strategy and type of all the players. We introduce the notation as follows:

$$\theta_{-i}(\ \theta_1, \ldots, \theta_{i-1}, \theta_{i+1}, \ldots, \theta_n\ )$$

It represents the type combination of all players except for n-1. It is also $\theta = (\ \theta_1, \theta_2, \ldots, \theta_n\ ) = (\ \theta_i, \theta_{-i}\ ), i = 1, 2, \ldots, n$. Any game player i , although knows oneself type θ_i , do not knows the type of other players θ_{-i} . But i is not totally don't know about θ_{-i} , at least understand $p(\theta_1, \ldots, \theta_n)$. At the same time, it is assumed that they have a knowledge of conditional probability $p_i(\theta_{-i} \mid \theta_i)$, that is, player i see the distribution probability of each type θ_{-i} of the other n-1 players when the player's type is θ_i .

Definition 3.3 The conditional probability $p_i(\theta_{-i} \mid \theta_i)$ of player's type is called the belief of the type for the other players' type. According to the Bayes rule:

$$p_i(\theta_{-i} \mid \theta_i) = \frac{p(\theta_i, \theta_{-i})}{p(\theta_i)} = \frac{p(\theta_i, \theta_{-i})}{\sum_{\theta_{-i} \in \Theta_{-i}} p(\theta_i, \theta_{-i})} \tag{2}$$

In the formula,

$$\Theta_{-i} \triangleq \prod_{\substack{j=1 \\ j \neq i}}^{n} \Theta_j, \quad i = 1, 2, \ldots, n$$

When players have common knowledge of the rules, they will know the distribution of other players.

When the type of player i is θ_i, the expected benefit of strategy s_i is:

$$\sum_{\theta_{-i} \in \Theta_{-i}} p(\theta_{-i} \mid \theta_i)\, u_i(s_{-i}(\theta_{-i}), s_i, \theta_i) \tag{3}$$

Through the expectation criterion, the concept of Nash equilibrium has a natural extension of Bayes-Nash equilibrium in the incomplete information static game.

Definition 3.4 A game formula is given as follows:

$$G = [\underline{N}, (\Theta_i), (p_i), (S_i), (u_i)] \tag{4}$$

If the strategic combination satisfies the condition, that is for every i and any $s_i \in S_i, \theta_i \in \Theta_i$, there is

$$\sum_{\theta_{-i} \in \Theta_{-i}} p(\theta_{-i} \mid \theta_i)\, u_i(s^*_{-i}(\theta_{-i}), s^*_i, \theta_i) \geq \sum_{\theta_{-i} \in \Theta_{-i}} p(\theta_{-i} \mid \theta_i)\, u_i(s^*_{-i}(\theta_{-i}), s_i, \theta_i) \tag{5}$$

The strategic combination $(s^*_1(\theta_1), \ldots, s^*_i(\theta_i), \ldots, s^*_n(\theta_n))$ is a Bayes-Nash equilibrium.

Bayes-Nash equilibrium is obtained by Bayes formula. It considers its excepted returns through the probability distribution. The expected revenue in Bayes static game is the expected return under different types of other players, rather than the expected return under its type. Bayes-Nash equilibrium studies the strategic choices of players in a situation, and this strategic choice depends on their type. Thus when the type is different, the strategy they choose is different.

4. INCOMPLETE INFORMATION ATTACK AND DEFENSE GAME BASED ON RISK AVERSION

The target network can be divided into lots of attack and defense points N, where the assets included in the point k are denoted as A_k. The probability that A_k will be at risk due to attack is q_k, so its security probability can be expressed as:

$$p_k = 1 - q_k \tag{6}$$

The attacking and defending parties carry out the game against the points k (that is an asset A_k). Among the game, the defensive side has a defensive strategy set as follows:

$$S_1(\theta_1) = (s_{11}(\theta_1), s_{12}(\theta_1), \ldots, s_{1m}(\theta_1))$$

Meanwhile, the attacker has their attack strategy set as follows:

$$S_2(\theta_2) = (s_{21}(\theta_2), s_{22}(\theta_2), \ldots, s_{2n}(\theta_2))$$

When the defensive party choose a strategy $s_{1i}(\theta_1) \in S_1(\theta_1), 1 \le i \le m$, and the attacking party choose a strategy $s_{2j}(\theta_2) \in S_2(\theta_2), 1 \le j \le n$ $\{ s_{1i}(\theta_1), s_{2j}(\theta_2) \}$, constitutes a strategic combination. For each strategic combination $\{ s_{1i}(\theta_1), s_{2j}(\theta_2) \}$, the security probability of asset A_k is $p_k(s_{1i}(\theta_1), s_{2j}(\theta_2))$, then the risk probability is:

$$q_k(s_{1i}(\theta_1), s_{2j}(\theta_2)) = 1 - p_k(s_{1i}(\theta_1), s_{2j}(\theta_2)) \tag{7}$$

In the formula, θ_1 is the type set of the defending party and θ_2 is the type set of the attacking party. In the practice of cyber-attacks, there is much evidence that a majority of decision-makers will avoid the risk. They are called risk-averse decision-makers. We assume that both attacking and defending sides are risk-averse. Also, the defenders have only one type, that is $\theta_1 = \{\theta_{11}\}$, and the attackers have two types $\theta_2 = \{\theta_{21}, \theta_{22}\}$, that indicates the level of risk aversion of the attacker. In the formula, θ_{21} is the risk aversion I and θ_{22} is the risk aversion II. In the cyber-attack situation, the attackers usually will make a decision first so that the defender can make a decision according to the strategy of the attacker. By the Harsanyi conversion for incomplete information game. It can be considered that "nature" determines the types of attackers and defenders and informs them which types they are. If the probability distribution in the type space given by "nature" is

$$\text{p(risk aversion I)}=\mu, \qquad \text{p(risk aversion II)}=1-\mu$$

μ is a constant and $\mu=\frac{1}{3}$ in the example, then

$$\text{p}(\theta_{21} \mid \theta_{11}) = \frac{1}{3}$$
$$\text{p}(\theta_{22} \mid \theta_{11}) = \frac{2}{3}$$
$$\text{p}(\theta_{11} \mid \theta_{21}) = p(\theta_{11} \mid \theta_{22}) = 1$$

By increasing or decreasing the risk probability q_k (security probability p_k) of A_k, we can obtain the attack and defense benefits of asset A_k. The defenders hope that p_k is big enough (so q_k is as small as possible), while the attackers want the opposite. Therefore, the benefit

function of attack and defense is not only the function of strategic combination $\{ s_{1i}(\theta_1), s_{2j}(\theta_2) \}$, but also the function of security risk probability $\{ p_k, q_k \}$.

Due to different levels of risk aversion (different types) of attackers, their revenue functions should also be different. u_2^I represent the revenue of risk aversion I and u_2^{II} represent the revenue of risk aversion II. Both functions are concave functions [6]. According to the features of offensive and defensive confrontation and the strategy dependence of both parties, u_2^I、u_2^{II} can be described as follows:

$$u_2^I = p_k - q_k[s_{2j}(\theta_{21}) - s_{1i}(\theta_{11})]\} \cdot s_{2j}(\theta_{21}) \tag{8}$$

$$u_2^{II} = q_k - p_k[s_{2j}(\theta_{22}) - s_{1i}(\theta_{11})]\} \cdot s_{2j}(\theta_{22}) \tag{9}$$

The defender has only one type compared to two types of attacker. From the formula (3) the expected revenue obtained by the defense party when defender select strategy $s_{1i}(\theta_{11})$ is:

$$\begin{aligned} u_1 = {} & \frac{1}{3}\{p_k - q_k[s_{2j}(\theta_{21}) - s_{1i}(\theta_{11})] - K\} \\ & \cdot(-s_{1i}(\theta_{11})) + \\ & \frac{2}{3}\{q_k - p_k[s_{2j}(\theta_{22}) - s_{1i}(\theta_{11})]\} \cdot (-s_{1i}(\theta_{11})) \end{aligned} \tag{10}$$

K is the “risk premium” [6] that the defense is willing to pay for reducing the defense risk. For the attacker, the question of revenue maximization arises the function as follows:

$$\frac{\partial u_2^I}{\partial s_{2j}(\theta_{21})} = p_k - 2q_k s_{2j}(\theta_{21}) + q_k s_{1i}(\theta_{11}) = 0$$

$$\frac{\partial u_2^{II}}{\partial s_{2j}(\theta_{22})} = q_k - 2p_k s_{2j}(\theta_{22}) + p_k s_{1i}(\theta_{11}) = 0$$

Thus the response function of the attacker is:

$$s_{2j}(\theta_{21}) = \frac{1}{2}\frac{p_k}{q_k} + \frac{1}{2}s_{1i}(\theta_{11}) \tag{11}$$

$$s_{2j}(\theta_{22}) = \frac{1}{2}\frac{q_k}{p_k} + \frac{1}{2}s_{1i}(\theta_{11}) \tag{12}$$

For the defender, the question of revenue maximization arises the function as follows:

$$\frac{\partial u_{1}}{\partial s_{1i}(\theta_{11})} = \frac{1}{3}\{p_{k} - k - q_{k} s_{2j}(\theta_{21}) + 2q_{k} s_{1i}(\theta_{11})\}$$

$$+\frac{2}{3}\{q_{k} - k - p_{k} s_{2j}(\theta_{22}) + 2p_{k} s_{1i}(\theta_{11})\}$$

$$= 0$$

Thus the response function of the defender is:

$$s_{1i}(\theta_{11}) = \frac{1}{2}\frac{3K - p_{k} - 2q_{k}}{2p_{k} + q_{k}} + \frac{1}{2}\frac{q_{k}}{2p_{k} + q_{k}} s_{2j}(\theta_{21}) + \frac{p_{k}}{2p_{k} + q_{k}} s_{2j}(\theta_{22}) \tag{13}$$

Bayes-Nash equilibrium $\{s^{*}_{1i}(\theta_{11}), s^{*}_{2j}(\theta_{21}), s^{*}_{2j}(\theta_{22})\}$ can be obtained by equation (11-13), which is related to the attack and defense game of asset A_{k} security risk. The equilibrium is:

$$\begin{cases} s^{*}_{1i}(\theta_{11}) = \frac{1}{3}\frac{6K - p_{k} - 2q_{k}}{2p_{k} + q_{k}} \\ s^{*}_{2j}(\theta_{21}) = \frac{1}{2}\frac{p_{k}}{q_{k}} + \frac{1}{6}\frac{6K - p_{k} - 2q_{k}}{2p_{k} + q_{k}} \\ s^{*}_{2j}(\theta_{22}) = \frac{1}{2}\frac{q_{k}}{p_{k}} + \frac{1}{6}\frac{6K - p_{k} - 2q_{k}}{2p_{k} + q_{k}} \end{cases} \tag{14}$$

5. CASE AND SIMULATION ANALYSIS

The case is an essential cyber penetration. In the process of network boundary intrusion, the attackers obtain relevant information, which is the target company has several servers on the network boundary for the customers. Different web applications and database systems are respectively running in the hosts, in which a service system is written using Tomcat middleware and JSP framework, and the database is SQL server.

The system topology of the service is shown in **Fig. 2**.

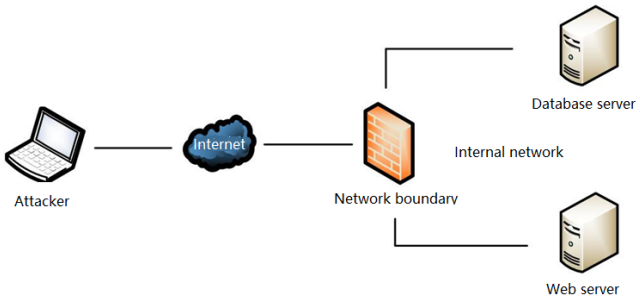

Fig. 2. Topology diagram of a company's network service system

After investigation analysis of service system, it is found that the system has three critical points for penetration. The priority of attack and defense should be determined by game theory.

(1) Point of password brute. Because this application has a management background, the password of management account can be exploded. By comparing the application user password leaked by the company and the password dictionary used in the penetration process, it is found that the password coverage of dictionary is only 20%, so the probability of the attack point being attacked is $q_1 = 0.2$. Thus the security probability $p_1 = 0.8$ can be calculated from formula (6).

(2) Point of database SQL injection. SQL injection is a common type of vulnerability in Web applications. According to the evaluation of the target framework in the process of penetration, the probability of the risk of SQL injection point being attacked is $q_2 = 0.6$, so $p_2 = 0.4$.

(3) Point of upload vulnerability. Penetration testers can upload special files to attack the server by the server file parsing vulnerabilities. The success of an attack depends on the system's code logic and the parsing vulnerability of the server. Compared with other Web server middleware, Tomcat has less vulnerability in parsing files, so the success rate of file upload attack is only 0.5. So we know $q_3 = p_3 = 0.5$.

First, the point of password burst is discussed. According to the company's emphasis on the security of cyberspace and the security protection requirements for enterprises, it can be known that the company has two types. The two types are high defense cost and low defense cos, $\theta_1 = \{\theta_{11}, \theta_{12}\}$. In this case, $p(\theta_{11}) = 0.3$ represent the probability distribution of high defense cost and $p(\theta_{12}) = 0.7$ describe the probability distribution of low defense cost. The company has a defensive strategy set, which is $S_1(\theta_1) = (s_{11}(\theta_1), s_{12}(\theta_1), \quad s_{13}(\theta_1), ..., s_{1i}(\theta_1))$. The attacker has only one type, so he can choose the attack strategy set, which is $S_2(\theta_2) = (s_{21}(\theta_2), s_{22}(\theta_2), ..., s_{2j}(\theta_2))$.

At this time there are:

$$p(\theta_{11} \mid \theta_{21}) = 0.3$$
$$p(\theta_{12} \mid \theta_{21}) = 0.7$$
$$p(\theta_{21} \mid \theta_{11}) = p(\theta_{21} \mid \theta_{12}) = 1$$

By referring to the function of the strategy dependence of the stacking and defending parties in equation (8) and (9), it can be seen that the expected revenue of the defending party is:

$$u_1^I = \{p_1 - q_1[s_{1i}(\theta_{11}) - s_{2j}(\theta_{21})]\} \cdot (s_{1i}(\theta_{11}))$$

which represent the expected revenue under high defense cost. The formula

$$u_1^{II} = \{q_1 - p_1[s_{1i}(\theta_{12}) - s_{2j}(\theta_{21})]\} \cdot (s_{1i}(\theta_{12}))$$

represent the expected revenue under low defense cost.

About equation (10), the expected revenue of strategy selected by two defense types for the attacker is

$$\begin{aligned} u_2 &= 0.3\left\{p_1 - q_1\left[s_{1i}(\theta_{11}) - s_{2j}(\theta_{21})\right] - K\right\}\cdot\left(-s_{2j}(\theta_{21})\right) \\ &+0.7\left\{q_1 - p_1\left[s_{1i}(\theta_{12}) - s_{2j}(\theta_{21})\right]\right\}\cdot\left(-s_{2j}(\theta_{21})\right) \end{aligned} \tag{14}$$

In this equation, K is the "risk premium" paid by the attacker to reduce the attack risk. According to the revenue maximization principle, the response function of the attacking party and the defending party can be calculated respectively. The response function of the attacker is calculated as follows:

$$\begin{aligned} \frac{\partial u_2}{\partial s_{2j}(\theta_{21})} &= 0.3\left\{p_1 + 2q_1 s_{2j}(\theta_{21}) - q_1 s_{1i}(\theta_{11}) - K\right\} \\ &\quad + 0.7\left\{q_1 + 2p_1 s_{2j}(\theta_{21}) - p_1 s_{1i}(\theta_{12})\right\} = 0 \end{aligned}$$

$$s_{2j}(\theta_{21}) = \frac{3K - 3p_1 - 7q_1}{14p_1 + 6q_1} + \frac{7p_1 s_{1i}(\theta_{12})}{14p_1 + 6q_1} + \frac{3q_1 s_{1i}(\theta_{11})}{14p_1 + 6q_1} \tag{15}$$

The response function of the defender is calculated as follows:

$$\frac{\partial u_1^I}{\partial s_{1i}(\theta_{11})} = p_1 + q_1 s_{2j}(\theta_{21}) - 2q_1 s_{1i}(\theta_{11}) = 0$$

$$\frac{\partial u_1^{II}}{\partial s_{1i}(\theta_{12})} = q_1 + p_1 s_{2j}(\theta_{21}) - 2p_1 s_{1i}(\theta_{12}) = 0$$

$$\begin{aligned} s_{1i}(\theta_{11}) &= \frac{p_1 + q_1 s_{2j}(\theta_{21})}{2q_1} \\ s_{1i}(\theta_{12}) &= \frac{q_1 + p_1 s_{2j}(\theta_{21})}{2p_1} \end{aligned} \tag{16}$$

Combined with the response function of both attack and defense, the Bayes-Nash equilibrium $\left\{s_{1i}^*(\theta_{11}), s_{1i}^*(\theta_{12}), s_{2j}^*(\theta_{21})\right\}$ of the game for the point of password brute is:

$$\begin{cases} s_{1i}^{*}(\theta_{11}) = \dfrac{1}{2}\dfrac{p_1}{q_1} + \dfrac{6K - 3p_1 - 7q_1}{42p_1 + 18q_1} \\ s_{1i}^{*}(\theta_{12}) = \dfrac{1}{2}\dfrac{q_1}{p_1} + \dfrac{6K - 3p_1 - 7q_1}{42p_1 + 18q_1} \\ s_{2j}^{*}(\theta_{21}) = \dfrac{6K - 3p_1 - 7q_1}{9q_1 + 21p_1} \end{cases} \tag{17}$$

In this formula, "risk premium" should satisfy $K > \dfrac{7q_1 + 3p_1}{6}$. After we think about all of the possible risks, we get $K = 10$. By using the probability distribution $(p_1, q_1) : (0.8, 0.2)$ of point of password brute, the optimal strategic combination is

$$\left\{ s_{1i}^{*}(\theta_{11}), s_{1i}^{*}(\theta_{12}), s_{2j}^{*}(\theta_{21}) \right\} = \left(\frac{653}{186}, \frac{1217}{744}, \frac{281}{93} \right).$$

Further use the revenue function of attack and defense, the revenue of both sides at the point of password explosion is:

$$u_1^{I}\left(\frac{653}{186}, \frac{281}{93} \right) = \frac{426409}{172980}$$
$$u_1^{II}\left(\frac{1217}{744}, \frac{281}{93} \right) = \frac{1481089}{691920}$$
$$u_2\left(\frac{653}{186}, \frac{1217}{744}, \frac{281}{93} \right) = \frac{78961}{13950}$$

Similarly, the revenue of point SQL injection and upload attack can be calculated respectively. The optimal strategic combination of SQL injection is

$$\left\{ s_{1i}^{*}(\theta_{11}), s_{1i}^{*}(\theta_{12}), s_{2j}^{*}(\theta_{21}) \right\} = \left(\frac{319}{138}, \frac{251}{92}, \frac{91}{23} \right)$$

The revenue of both sides is

$$u_1^{I}\left(\frac{653}{186}, \frac{281}{93} \right) = \frac{426409}{172980}$$
$$u_1^{I}\left(\frac{319}{138}, \frac{91}{23} \right) = \frac{101761}{31740}$$
$$u_1^{I}\left(\frac{653}{186}, \frac{281}{93} \right) = \frac{426409}{172980}$$

According to the calculation, the revenue of different offense and defense points are compared as shown in **Table 2.**

Table 2. Byes-Nash balanced income statement for three offensive and defensive points

Points	u_1^I	u_1^{II}	u_2
Password Brute	$\frac{426409}{172980}$	$\frac{1481089}{691920}$	$\frac{78961}{13950}$
SQL Injection	$\frac{101761}{31740}$	$\frac{63001}{21160}$	$\frac{8281}{1150}$
File Upload	$\frac{49}{18}$	$\frac{49}{18}$	$\frac{49}{18}$

According to comparing the Bayes-Nash equilibrium revenue generated by different penetration points, the Bayes-Nash equilibrium revenue of SQL injection point is higher than other attack points. Therefore, considering the time cost and the risk of penetration, the attacker first launches the attack to the point of SQL injection and successfully obtains the database data. **Fig. 3** shows the desensitised system information obtained using the point of SQL injection.

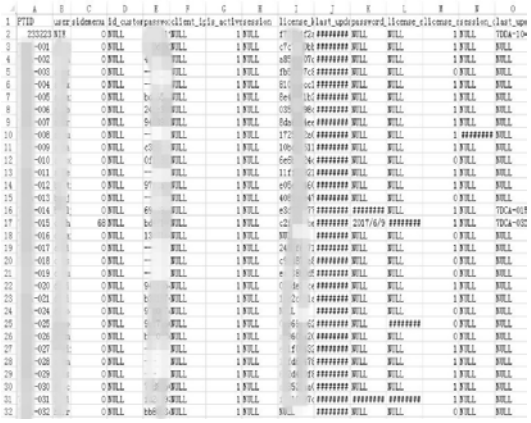

Fig. 3. SQL injection attack data after desensitization

Through the analysis of real case, we can find the Bayesian-Nash equilibrium is real in the security attack and defense. This game decision model can be used to deduce the attack behavior and predict the attack intention in advance. The game model of network attack and defense based on Bayesian-Nash equilibrium proposed in this paper not only derive the mathematical relationship of the model theoretically but also verifies the effectiveness of the model in the penetration environment.

References

[1] Kenneth Geers, *Strategic cyberspace security*, CCD COE Publication, Estonia, 2015.1.

[2] Hongsheng G, *Cyberspace Security Strategy*, Aviation Industry Press, Beijing, 2016

[3] Zhenxue W, Anming Z, Yong F, Xiaocong O, *Information System Security Risk Estimation and Control Theory*, Science Press, Beijing, 2011.

[4] Dingpi H, *Introduction to Game Theory*, China University of Science and Technology Press, Hefei, 2004.

[5] Weijin Zh, *Game Theory and Information Economics*, Truth & Wisdom Press, Shanghai Joint Publishing Press, Shanghai People's Publishing House, Shanghai, 2016.

[6] Chaoyuan Y, *Decision theory and methods*, Science Press, Bejing, 2006.
[7] Aumann R J, "Game theory," *The New Palgrave Dictionary of Economics*, 2017.
[8] Roy S, Ellis C, Shiva S, et al., "A survey of game theory as applied to network security," in *Proc. of 2010 43rd Hawaii International Conference on System Sciences, Honolulu, IEEE*, 1-10, 2010. Article (CrossRef Link).
[9] Liu Y, Comaniciu C, Man H, "A Bayesian game approach for intrusion detection in wireless ad hoc networks," in *Proc. of the 2006 workshop on Game theory for communications and networks, Pisa, ACM*, 4, 2006. Article (CrossRef Link)
[10] Esmalifalak M, Shi G, Han Z, et al., "Bad data injection attack and defense in electricity market using game theory study," *IEEE Transactions on Smart Grid*, 4(1), 160-169, 2013. Article (CrossRef Link)
[11] Do C T, Tran N H, Hong C, et al., "Game theory for cyber security and privacy," *ACM Computing Surveys (CSUR)*, 50(2), 30, 2017. Article (CrossRef Link)
[12] Liang X, Xiao Y., "Game theory for network security," *IEEE Communications Surveys & Tutorials*, 15(1), 472-486, 2013. Article (CrossRef Link)
[13] Durkota K, Lisy V, Kiekintveld C, et al., "Game-theoretic algorithms for optimal network security hardening using attack graphs," in *Proc. of the 2015 International Conference on Autonomous Agents and Multiagent Systems, International Foundation for Autonomous Agents and Multiagent Systems, Istanbul, ACM*, 1773-1774, 2015.
[14] Bedi H S, Roy S, Shiva S, "Game theory-based defense mechanisms against DDoS attacks on TCP/TCP-friendly flows," in *Proc. of 2011 IEEE Symposium on Computational Intelligence in Cyber Security (CICS), Paris, IEEE*, 129-136, 2011. Article (CrossRef Link)
[15] Sandberg H, Amin S, Johansson K H, "Cyber-physical security in networked control systems: An introduction to the issue," *IEEE Control Systems*, 35(1), 20-23, 2015.
[16] Sedjelmaci H, Senouci S M, Ansari N, "Intrusion detection and ejection framework against lethal attacks in UAV-aided networks: a Bayesian game-theoretic methodology," *IEEE Transactions on Intelligent Transportation Systems*, 18(5), 1143-1153, 2017. Article (CrossRef Link)
[17] Nguyen T H, Wright M, Wellman M P, et al., "Multi-stage attack graph security games: heuristic strategies, with empirical game-theoretic analysis," in *Proc. of the 2017 Workshop on Moving Target Defense, Dallas, ACM*, 87-97, 2017. Article (CrossRef Link)
[18] Rass S, König S, Schauer S, "Defending against advanced persistent threats using game-theory," *PloS one*, 12(1), e0168675, 2017.
[19] Zhu J, Zhao B, Zhu Z, "Leveraging game theory to achieve efficient attack-aware service provisioning in EONs," *Journal of Lightwave Technology*, 35(10), 1785-1796, 2017. Article (CrossRef Link)
[20] Weiheng Zh, TAO L, "Optimal Active Defense Based on Multi-stage Attack-Defense Signaling Game," *Chinese Journal of Electronics*, 45(2), 431-439, 2017.
[21] Wei J, Binxing F, Zhihong T, etc, "Evaluating Network Security and Optimal Active Defense Based on Attack-Denfense Game Model," *Chinese Journal of Computers*, 32(4), 817-827, 2009.
[22] Wei J, Bingxing F, Zhi-hong T, "Research on defense strategies selection based on attack-defense stochastic game model," *Journal of Computer Research and Development*, 47(10), 1714-1723, 2010.
[23] Lye K, Wing J M, "Game strategies in network security," *International Journal of Information Security*, 4(1-2), 71-86, 2005. Article (CrossRef Link)
[24] Wei L, Sarwat A I, Saad W, et al., "Stochastic games for power grid protection against coordinated cyber-physical attacks," *IEEE Transactions on Smart Grid*, 9(2), 684-694, 2018. Article (CrossRef Link)
[25] Lei C, Zhang H Q, Wan L M, et al., "Incomplete information Markov game theoretic approach to strategy generation for moving target defense," *Computer Communications*, 116, 184-199, 2018.

LIANG LIU received the M.A. degree from Sichuan University, Chengdu, China, in 2010. He is currently an Assistant Professor at the college of Cyber security, Sichuan University, China. His current research interests include malicious detection, network security, and system security and artificial intelligence.

CHENG HUANG received the Ph.D. degree from Sichuan University, Chengdu, China, in 2017. From 2014 to 2015, he was a visiting student at the School of Computer Science, University of California, CA, USA. He is currently an Assistant Research Professor at the college of Cyber security, Sichuan University, Chengdu, China. His current research interests include Web security, span network, social privacy, system security, artificial intelligence.

YONG FANG received the Ph.D. degree from Sichuan University, Chengdu, China, in 2010. He is currently a Professor with college of Cyber security, Sichuan University, China. His research interests include network security, Web security, Internet of Things, Big Data and artificial intelligence.

ZHENXUE WANG is currently a Professor with college of Electronics and Information Engineering, Sichuan University, China. His research interests include network security, intelligent system, information system risk assessment and control.