Research on cost budget model of information security based on Game Theory

Rong Chen[1,2*], Qiying Cao[1]

1 School of information science and technology, Donghua University, China
2 Shanghai Customs College, China
**Corresponding Author*

ABSTRACT. *In the face of the widespread use of information technology today, the information security problem has begun to receive extensive attention. In this paper, based on game theory, the cost budget model of information security was studied and analyzed, and the minimax fuzzy game model was proposed. In this model, evidence theory was used to describe the fuzziness of information, and the minimax regret principle of acceptable income was introduced to avoid unacceptable gains and excessive pessimism. The minimax fuzzy game model was applicable to multiple attackers and multiple defenders, and attackers and defenders need not observe their strategies first, so that they can act at the same time.*

KEYWORD: *Game theory; Information security; Cost of safety; Cost budgeting model*

1. Introduction

With the rapid development of computer network technology, the information industry has become an important pillar of the national economy. Information network is related to many fields such as government, military, culture and education in the country. Some information about storage, transmission and processing is such as macroeconomic regulation and control policy, business economic information, scientific research data and other important information [1]. Many of them are sensitive information or even state secrets, so it will inevitably attract all kinds of human attacks around the world, such as information leakage, information theft, computer virus and so on[2]. It is often difficult to use computer crime to leave criminal evidence, which greatly stimulates the occurrence of in computer high tech crime cases [3]. With the rapid increase of computer crime rate, computer systems in many countries, especially the network system, are facing great threat and become a serious social problem. In the face of these terrorist attacks and security threats, various countries' security institutions have invested a large amount of funds and other resources to increase the protection of information security.

However, these resources are, after all, limited, and security institutions can not provide full security for all information at any time [4]. How to find the optimal scheduling scheme of limited resources to obtain the best income is the key problem that needs to be solved urgently in the distribution of resources in the security field.

2. State of the art

The application of information technology has improved the productivity of social labor and the efficiency of social operation, and has become a major driving force for the development of social economic activities [5]. Especially in recent years, sensor technology, RFID (radio frequency identification devices) the rapid development and application of technology greatly, wireless transmission technology and data processing technology and networking technology the people's life, which improve the utilization rate of resources and reduce the production cost. The role of production factors and strategic resources can be fully played [6]. Therefore, the development of the Internet of things can bring great economic benefits and social benefits. However, with great benefits, the application of the Internet of things has also aggravated the serious information security problem in the information age [7]. Serious matter networking wireless transmission characteristics of information age can easily be exploited by hackers. The wireless network is vulnerable to DoS (Denial of Service) attack and the result is light network degradation, heavy paralysis of the entire network needs mutual cooperation and sharing of information between enterprises. The degree of collaboration between enterprises depends on the communication network. However, in addition to helping enterprises to cooperate with each other, the communication network will also increase the probability of the enterprise information system to be broken. In order to cooperate better, an enterprise usually allows other enterprises to access their systems directly through trust links, which facilitates the spread of security attacks. A hacker who successfully breaks an enterprise information system can easily break through the other enterprises in the network through a trust link. The attack of hacker will not only give the attacked enterprise, but also bring huge loss to the partner enterprise in the network. The result is that enterprises in the network no longer trust each other and eventually may lead to disintegration of inter-enterprise cooperation.

3. Methodology

3.1 Bayes game

The Bias game, also known as incomplete information game, is an extension of the Stackelberg game. The classic Stackelberg game is a double game made up of an attacker and a defender. The defender first determines its own mix strategy, and the attacker first sees the defender's strategy and then chooses the strategy that maximizes its income. Each participant in the Stackelberg game can be extended into a variety of possible types and the value of each type is different, so that it becomes a Bias game. In the security field, it is usually assumed that the type of defender is determined, and the attacker may be one of many types. Bias in the game, the attacker knows its own type, so it has complete information on the defense and their own income; the type of uncertainty due to the attacker defender, cannot take that each strategy gains, but the possibility, the defender is known in advance to various types of attacks appear namely: defenders with incomplete information for the attacker and its own income.

Definition 1. The Bias game can be defined as a five tuple (N,ζ,θ,P,U):-N={1,2}, Represents a collection of participants, 1 of which are attackers and 2 are defenders. —ζ={a1,a2,…,am}, n represents the set of attackers, where m is the total number of attackers, —θ={θ1,θ2} represents a set of pure policies, and theta 1 and theta 2 represent the pure policy set of the defender and the attacker, respectively. —P={p(t)|t∈ζ} represents the probability of the attacker type distribution, in which p (T) is the probability of type T. -U={U1,U2},U1={u1i(s1,s2)|i∈ζ,s1∈θ1,s2∈θ2},U2={u2i(s1,s2)|i∈ζ,s1∈θ1,s2∈θ2}, A represents the return matrix of the attacker and the defender, respectively. In the Bias game, all the participants act at the same time. The attacker's action space depends on its type, and its income is type dependent. The Bias game is remodeled as a complete but imperfect game. A virtual participant nature is introduced into the original game, and nature is substituted for participants to select a type with a certain probability. As a result, the Bias Nash equilibrium can be obtained as follows:

Definition 2: the optimal strategy of the (N,ζ,θ,P,U) record s*2∈θ2 for a given Bias game, that is, the expected return of the s*2 maximizing defender, and

$$s_2^* = \arg\max_{s_2 \in \theta_2} \{EU_2(s_2) = \sum_{t \in \xi} u_t^2(s_1^*, s_2)\, p(t)\}$$

3.2 Minimax fuzzy game model

Most of the phenomena in the objective world are uncertain. Sure, the so-called rules of the phenomenon will only result in a certain condition and under specific conditions. Therefore, the knowledge and information describing the objective phenomena are also uncertain, that is, fuzziness. In the security game, when the probability distribution of participants is explicitly known, information is completely determined, that is, the degree of fuzziness is 0. When the participant type is completely unknown, the information is completely uncertain, that is, the ambiguity degree is 1. In ABGMR, the ambiguity is used to measure the accuracy of the participants' type information. The minimax fuzzy game (ABGMR) is the expansion of Bias's game. On the basis of it, the minimax principle of fuzziness and acceptable income is introduced. In ABGMR, the information of the attacker and the defender is known to be incomplete and blurred.

(1) D-S theory. The theory of evidence establishes a one-to-one correspondence between propositions and sets, and transforms the uncertainty of the proposition into the uncertainty of the set. The theory of evidence is also considered to be the theory

of reliability function, which is the extension of the Bayesian theory of subjective probability. Evidence theory by introducing the reliability function, the likelihood function, the good representation of the important concept of “uncertainty” and “unknown unknown” cognition. The reliability function allows us to deduce the probability of a related problem based on the probability of using a problem.

Set a set of all the possible values of the variable x, and the mutual exclusion of all the elements, called the sample space of the theta as X. In the D-S theory, any subset A of theta corresponds to a proposition about X, which is called “the value of X in A”.

Definition 3. Suppose the function f:2 [0 1], 0, and meet the:

f($\varnothing$)=0

$$\sum_{A\subseteq\theta} f(A)=1$$

F is called the probability distribution function on 2 theta, and f (A) is called the basic probability number of A. If A: D is f (A) =0, f A is called a focal element.

Definition 4. The proposition of reliability function Bel:2 [0 1], and: Bel(A)= $\sum_{B\subseteq A}$ f(B)(A:θ)

The Bel function is also called the lower limit function and Bel(A)represents the degree of trust that the propositional A is true.

Definition 5. The proposition of the likelihood function of Pl:2 [0 1], and:

Pl(A)=1-Bel($\neg$ A)(A $\subseteq$ θ)

The Pl function is also called the non refutable function or the upper limit function. Because Bel (A) represents the true degree of trust for A, then Bel(¬A) represents the degree of trust that A is false, and thus the Pl (A) can be introduced to represent the degree of trust that is non - false to A.

Therefore, the degree of trust in the event A: EB(A) $\in$ [Bel(A),Pl(A)].

The lemma 1. A: 0, Pl (A) = Bel (A). Prove:

$\because$ Bel(A)+Bel(¬A)

$$=\sum_{B\subseteq A} \text{f(B)+ΣC:¬Af(C)}$$

$$\le\sum_{E\subseteq\theta} \text{f(E)}$$

$$\text{and}\because \sum_{E\subseteq\theta} \text{f(E)=1}$$

$\therefore$ Bel(A)+Bel(¬A)≤1

$\therefore$ Pl(A)-Bel(A)

=1-Bel(¬A)-Bel(A)

=1-[Bel(¬A)+Bel(A)]≥0

∴Pl(A)≥Bel(A)

Definition 6. Let delta be the degree of fuzziness of the probability distribution function f, and:

$$\delta(\mathrm{f}) = \begin{cases} \dfrac{\sum_{A\subseteq\theta} f(\mathrm{A})\cdot\log_2|A|}{\log_2|\theta|} & |\theta|>1 \\ 0 & others \end{cases}$$

Among them, |A| and|θ| represent the cardinality of the set A and θ, respectively. For the upper form, there are two special cases: (1) A: θ, when and only when |A|=1, f (A) >0, then δ(f) =0. In this case, it is completely unambiguous (fully trusted), knowing enough information about X, and F as a probability function. This is the Bias game. (2) A: θ, if A≠θ, f (A) =0, then δ(f) =1. In this case, the information about X is completely unknown, that is, completely blurred. Therefore, the probability distribution function of F fuzzy degree δ in [0, 1], [0, β degrees of ambiguity aversion, 0.5]. the minimax fuzzy game model.

Definition 7. Minimax fuzzy game (ABGMR) can be defined as a six tuple (ζ,γ,θ,U,F,G): —ζ={a1,a2,…,am} represents the collection of attackers, in which m is the total number of attackers; —γ={d1,d2,…,dS} , is the collection of defenders, in which S is the total number of defenders, that is, the total number of resources. —θ={t1,t2,…,tn}, is the target set, that is, the pure policy set of the attacker and the defender, in which the n is the total target. —U={Ua,Ud},Ua={uais(k)|i∈ζ,s∈γ,k∈θ},Ud={udis(k)|i∈ζ,s∈γ,k∈θ}, represents the return matrix of the attacker and the defender respectively. uais(k)={uais(j,k)|j ∈ θ},udis(j)={udis(j,k)|k ∈ θ}, shows the benefits of attackers and defenders when attacker I attacks target K and defender's s defense target J.

-Fs={fs(A)|A⊆ζ}, represents the probability distribution function of the type information of the attacker known by the defender s, and f (A) is the probability that an attacker belongs to the type A set.—Gi={gi(A)|A ⊆ γ}, The probability distribution function that represents the type information of a defender known by an attacker I, G (A), the probability of a defender belonging to a type A set. In the above minimax fuzzy game model, both the attacker and the defender are uncertain of the types of each other, and there is a degree of fuzzy trust. That is to say, the defender knows the possible set of the attackers, but does not know the exact probability distribution of each type.

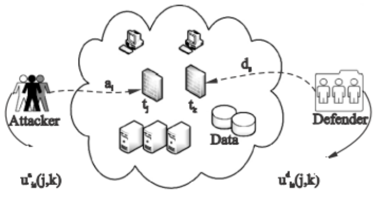

Figure.1 State of ABGMR

As shown in Figure 1, it is the game situation map of ABGMR Attacker, Defender and Data respectively, the attacker defender and target cluster. Attacker ai attack target tj,defender ds defense target tk,, attacker and defender received $u_{is}^{a}(j,k)$, $u_{is}^{d}(j,k)$ .The ambiguity of ABGMR consists of two parts, (δF,δG), namely, the ambiguity of the attacker and the blur of the defender. In ABGMR, the defender knows all possible attackers type ζ, but does not know the exact probability distribution. The defender needs to learn the probability distribution function of the attacker type first, and understand the type information of the attacker. In order to get the best game strategy, defenders need to know the acceptable regret value of the strategy selected by the defender in order to get the best game strategy. Besides the defender's income matrix, the defensive value is σ_{s}^{d} , and the value is determined by the game strategy and the self earning matrix adopted by both offenders and defenders. In the same way, the attacker should also learn the opponent information and consider the acceptable regret σ_{i}^{a} before the attacker's strategy is selected.

Attacker gains represent an attack after attacker gains. That is the degree of threat to data information and the loss to the attacked system. The greater the value of the attacker's income, the more sensitive and important the acquired information asset is the greater the threat and the greater the loss to the attacked system. Defender gains represent the reward of a defender against a certain attack strategy. That is to contain the degree of attacker attack and protect the whole system assets. The greater the value of the defenders' returns, the more significant the effect of containment of the attacker's behavior and the stronger the ability protect the entire system's assets.

4. Result analysis and discussion

4.1 Minimax maximum fuzzy game Nash equilibrium

ABGMR introduces the minimax regret value principle of acceptable returns. When making a strategy selection, a defender considers minimizing the maximum regrettable value of the acceptable yield, rather than maximizing the expected return. In a certain state, the loss value caused by the lack of a relative optimal scheme is called a regrettable value. The maximum regret of a strategy is the difference between the minimum return value of the strategy and the maximum value that can be obtained in a given state. The smaller the difference, the strategy that shows the closer to the maximum value. The minimax regret of acceptable income.

The principle of value is simple, that is, on the basis of considering the minimum expected return value of the strategy is acceptable income, the strategy that can minimize the maximum regret value is selected. The principle avoids the overly pessimistic situation in the minimax strategy. The maximum performance strategy is a relatively conservative strategy, which means that the strategy adopted by the player is the strategy to maximize the minimum income that you can get. For example, a ticket price of ￥1, 99% could win $5000. The minimum income for buying and not buying a lottery is ￥－1and￥ 0 respectively. It's a clear violation of our intuition that we refuse to buy the lottery by following the principle of minimax strategy. But in the acceptable principle of minimax regret returns, if the loss of ￥1 is acceptable, it will bear the risk. The principle also avoids the potential loss that is unacceptable in the minimax regret strategy. The minimax regret strategy refers to the strategy that the game player adopts to minimize the maximum regrets they can obtain. For example, a ticket price of ￥1000, 99% could win ￥5000. The biggest regret to buy and do not buy lottery tickets were ￥1000 and ￥4000. The principle of following the minimax regret strategy will accept the price, which is contrary to the reality. The acceptable principle of minimax regret returns, will first consider whether the ￥1000 is acceptable loss, and then decide whether to accept the purchase of lottery tickets. These advantages of the minimax regret principle of acceptable income are very applicable in the information security protection of the real world.

4.2 Experimental analysis

In this paper, we use IBMILOGCPLEX software to solve the linear programming problems in ABGMR. IBMILOGCPLEX is a linear programming tool, supporting various programming languages. In this experiment, we use JAVA language programming. In order to illustrate the application of minimax fuzzy game in the resource allocation scenario of information security field, this paper establishes a secure game model based on cloud platform. In this model, the attacker will select the appropriate data source to attack and the security department will arrange the key protection for the key data.

Multi attacker multi defender experiment. The minimax fuzzy game model proposed in this paper is suitable for multiple attackers of multiple defenders. In this experiment, it is assumed that three defenders, (γ={D1,D2,D3}) and three types of attackers, (ζ={T1,T2,T3}) to defend the three key targets of the airport, (θ={data1,data2,data3}) .The pure strategy of the defender and the attacker is θ. In this experiment, the fuzzy degree of the experimental data ((0.1946, 1, 0), (0, 0.6047, 0.3155)), namely: D1, D2, D3 defense of the attacker type information, Partial fuzzy, completely fuzzy, unambiguous; T1, T2 and T3 respectively, the attacker to defender type information not fuzzy, fuzzy, fuzzy part.

The experimental results are as follows:

Defender's optimal strategy: D1={P(Data1)=0,P(Data2)=0.16, P(Data3)=0.482}D2={P(Data2)=1} D3={P(Data2)=0.183,P(Data1)=0.327, P(Data3)=0.489}}

attacker's optimal strategy: T1={P(Data2)=1} T2={P(Data1)=1} T3={P(Data1)=1}

Defender's maximum regret:D1=10.915789842088227 D2=11.0 D3=10.72948674941295

Defender's expected utility: D1=-3.747369526264689 D2=-0.0 D3=-3.188460248238846

Attacker's maximum expected utility: T1=6.0 T2=6.0 T3=11.0

The experimental data above show that the optimal mixed strategy of the defenders and the optimal pure strategy of the attackers can be obtained by ABGMR. The analysis of the results can verify the situation that ABGMR is suitable for multiple attackers and multiple defenders.

Contrast experiment. In previous studies, many methods can be used to solve the security game problem. DOBSS algorithm is one of the most effective mixed strategies that can be used to calculate leaders in Bayesian Stackelberg game. DOBSS is applicable to a variety of attackers, a defender, which follows the principle of maximizing the expected return. This is the contrast experiment between DOBSS and the ABGMR presented in this article in the case of a variety of attackers, a defender. In order to apply the two different models, the comparison experiment, assume the existence of a defense in (γ={D1}) and three types of attackers need to defend the (ζ={T1,T2,T3}) three key objectives (θ={Data1,Data2,Data3}) here only consider the defender to the attacker type information ambiguity, without considering the attacker defender type information ambiguity, the experimental results are shown in Figure 2 shown. Figure 2 is the maximum regret value comparison diagram for the defenders' decision in DOBSS and AB-GMR in the case of different attacker type ambiguity δ.It can be seen from the diagram that the maximum regret value of ABGMR decision is obviously better than that of DOBSS decision. The ABGMR model proposed in this paper is based on the minimax regret principle, which is applicable to multiple attackers and multiple defenders, and considers the ambiguity of attackers and defenders. The ABGMR proposed in this paper is more wide, more comprehensive and more in line with the application of the actual scene than the DOBSS.

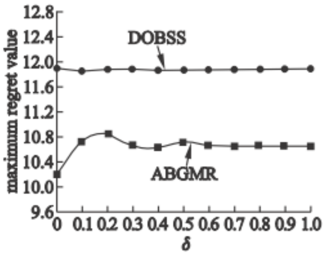

Figure.2 Comparison chart of maximum regret value

5. Conclusion

Game theory plays a more and more important role in the field of information security. In recent years, theoretical research and production practice have made great progress in the analysis of security game. This paper studied and analyzed the information security cost budget model based on game theory, and proposed a mini-max fuzzy game model, which was suitable for multiple attackers and multiple defenders. Fuzzy degree was introduced to make it more practical. This model has extended the existing Bias game model, combined D-S theory, solved the problem of fuzzy information in the types of attackers and defenders, and the mini-max regret principle of acceptable income has been introduced, and too pessimistic situations has been avoided. The superiority of the minimax fuzzy game model is proved by experimental demonstration and comparison with the experiment of the algorithm.

References

[1] Banker R D, Kauffman R J (2004). 50th anniversary article: The evolution of research on information systems: A fiftieth-year survey of the literature in management science. Management Science, vol.50, no.3, pp. 281-298.

[2] Anderson R, Moore T (2006). The economics of information security. Science, vol.314, no.5799, pp. 610-613.

[3] Cavusoglu H, Mishra B, Raghunathan S (2005). The value of intrusion detection systems in information technology security architecture. Information Systems Research, vol.16, no.1, pp. 28-46.

[4] Wang J, Chaudhury A, Rao H R (2008). Research Note-A Value-at-Risk Approach to Information Security Investment. Information Systems Research, vol.19, no.1, pp. 106-120.

[5] Dibbern J, Goles T, Hirschheim R, et al (2004). Information systems outsourcing: a survey and analysis of the literature. ACM Sigmis Database, vol.35, no.4, pp.6-102.

[6] Xiong L, Liu L (2004). Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities. IEEE transactions on Knowledge and Data Engineering, vol.16, no.7, pp.843-857.

[7] Gordon L A, Loeb M P (2002). The economics of information security investment. ACM Transactions on Information and System Security (TISSEC), vol.5, no.4, pp.438-457.