Computer and Information Science
www.ccsenet.org/journal.html
Vol. 2, No. 2
May 2009

A Model of Intrusion Tolerant System Based on Game Theory

Huawang Qin, Yuewei Dai & Zhiquan Wang
School of Automatization, Nanjing University of Science and Technology
Nanjing 210094, China
E-mail: qin_h_w@163.com

Abstract

Intrusion tolerance is the rising third generation technology of network security. For the shortcomings of existing models, a model of intrusion tolerant system based on game theory is proposed. The intrusion tolerant system and the intruder are seen as the two sides of the game. The income functions of the two sides are designed basing on some given concepts. Through quantifying and analyzing the income functions, the optimum strategies of the intrusion tolerant system and the intruder are obtained, and the Nash equilibrium of the game system is achieved finally. The results of analysis show that, this proposed model of intrusion tolerant system is consistent with the practical system.

Keywords: Intrusion tolerance, Network security, Game theory, Nash equilibrium

1. Introduction

The security of network system has been a topic of concern with the intrusion incidents occurring continually. Although the firewall and intrusion detection software can protect the network effectively, the practices have show that no firewall or intrusion detection software can guarantee the network from being intruded absolutely. Under such circumstance, intrusion tolerance was born. Intrusion tolerance is the third generation technology of network security. The concern of intrusion tolerance is not how to defend or detect the intrusion, but how to mask or restrain the intrusion when the network has been intruded. Intrusion tolerance can guarantee the confidentiality and integrality of data as well as the usability of service when the network has been intruded.

Intrusion tolerance is a rising research topic in the field of network security, and it has broad application future. With the promotion of the USA's OASIA and the European Union's MAFTLA, the technology of intrusion tolerance has developed rapidly in recent years. For the study of domestic and foreign academia, the modeling(Goseva P. K., Wang F., & Wang R, 2001)(Peng W. L., Wang L. N., & Zhang H.G, 2005)(Cui J. S., Wang L. N., & Zhang H. G, 2004), security analysis(Madan B. B., Goseva P. K., Vaidyanathan K., & Trivedi K. S, 2004)(Yin L.H., & Fang B.X, 2006)(Singh S., Cukier M., & Sanders W. H, 2003), and design method(Jing J. W., & Feng D. G, 2002)(Castro M., & Liskov B, 2000)(Liu P, 2002)(Arsenault D., Sood A., & Huang Y, 2007) have all acquired abundant results.

The modeling of intrusion tolerant system is the pivotal and basic work for studying the technology of intrusion tolerance. Goseva et al. proposed a model of intrusion tolerant system based on the conversion of multimode (Goseva P. K., Wang F., & Wang R, 2001), and classified the work states of intrusion tolerant system typically. Peng et al. designed a model based on the finite state automaton machine (Peng W. L., Wang L. N., & Zhang H.G, 2005), and described the dynamic property of intrusion tolerant system. Cui et al. gave a model based on resource and control (Cui J. S., Wang L. N., & Zhang H. G, 2004), and the model can describe the corresponding properties when the intrusion tolerant system has been intruded in parallel.

Although these proposed models can describe the properties of intrusion tolerant system from some sides commendably, they still have the following shortcomings.

(1) These models only describe the property of intrusion tolerant system, and not take into account the behavior of intruder. So the description of the models for the intrusion tolerant system is not comprehensive.

(2) These models do not analyze the cost and reward of intrusion tolerance. However, in order to design a cost-effective intrusion tolerant system, it is necessary to evaluate the cost and reward of intrusion tolerance.

(3) These models are lack of the quantitative methods, and only describe the intrusion tolerant system roughly through qualitative analysis.

For the above three problems, a model of intrusion tolerant system based on game theory is proposed in this paper. The intrusion tolerant system and the intruder are seen as the two sides of game. The two sides both want to obtain the larger reward through smaller cost, so as to obtain the maximal income. In the proposed model, the optimum strategies of the intrusion tolerant system and the intruder are obtained through quantifying their incomes, and the Nash equilibrium of the game system is achieved lastly.

2. The optimum strategy of intrusion tolerant system

2.1 Tolerance cost and tolerance probability

Definition 1 Tolerance cost: all the expenditures that the intrusion tolerant system needs on hardware, software and wage for the function of intrusion tolerance are called tolerance cost.

The tolerance cost includes three parts: hardware expenditures, software expenditures, and wage expenditures. The hardware expenditures are used to buy and maintain the additional agents, servers, memories, communications equipments etc; the software expenditures are used to buy and maintain the additional operating systems, encryption and authentication software, communications software, and other application software etc. the wage expenditures are the payment for the employees who design and maintain the intrusion tolerant function.

Definition 2 Tolerance probability: for some special tolerance cost, the statistical probability that the intrusion tolerant system can tolerate the intrusion and avoid the losses when it has been intruded is called tolerance probability.

The tolerance probability is used to describe the performance of intrusion tolerance quantitatively. An intrusion tolerant system can increase its tolerance probability through increasing redundancy, enhancing the performance of hardware and software, and improving the skill of design and maintenance engineers. Obviously, these measures will all increase the tolerance cost of the system. For an intrusion tolerant system which is designed commendably, it can be considered that its tolerance probability increases monotonously with its tolerance cost increasing, that is, larger tolerance cost corresponds to larger tolerance probability. If the tolerance cost nears infinity, we can consider that the redundancy of the system is infinite, the performance of hardware and software is perfect, and the skill of engineers is perfect too. Under such circumstance, it can be considered that the system can tolerate any intrusion, that is, the tolerance probability of the system is 1. If the tolerance cost is 0, we can consider that the system has no redundancy, and the hardware, software as well as the design technology all have no function for intrusion tolerance. In this case, it can be considered that the system can not tolerate any intrusion, that is, the tolerance probability is 0.

For example, in the typical (t, n) threshold intrusion tolerant system, a data is divided into n shadows and distributed to n different servers. Any t or more servers can recover the data, but any fewer than t servers can not recover the data. Therefore, if the number of the servers which are controlled by the intruder is less than t, the intruder can not get the data; if the number of unspoiled servers is not less than t, the system can still recover the data. Obviously, the data in the (t, n) threshold system can tolerate the intrusion on both the confidentiality and the integrality. The tolerance probability of the (t, n) threshold system can be increased through increasing the value of n and t, and enhancing the security of each server. But this will also increase the tolerance cost of the system. If the tolerance cost of the (t, n) threshold system nears infinity, then the values of n and t can also near infinity, and the security of each server will almost be perfect. Under such circumstance, the tolerance probability of the system can be considered 1 apparently. If the tolerance cost of the system is 0, then there is no redundancy in the system, that is, the data is saved in only one server. In this system, if the server is intruded by the intruder, the intruder can not only obtain the data but also destroy the data. So the data has no tolerance function for intrusion, and the tolerance probability of the system will be 0 accordingly. In practical (t, n) threshold system, the values of n and t are not decided according to some quantitative criteria, but often decided roughly according to the importance of system, the limit of cost, and the experience of deviser etc.

When studying the security of the fault-tolerant control system or the network system, the exponential distribution is usually be assumed so as to adopt the stochastic modeling tools such as Markov decision process and stochastic Petri net etc. Moreover, Jonsson and Olovsson verified the exponential distribution property of the intrusion behavior in internet through special experiments (Jonsson E., & Olovsson T, 1997). In view of this, we define the relationship between the tolerance cost and the tolerance probability through exponential function.

$$P_S = 1-e^{-\lambda c} \qquad C \geq 0 \tag{1}$$

Where, P_S is the tolerance probability; C is the tolerance cost; λ is the parameter of the exponential function, it is influenced by the network's functions, security, and physical environment etc. It can be seen from Formula (1) that, tolerance probability increases with the increasing of tolerance cost; if the tolerance cost is 0, then the tolerance probability is also 0; if the tolerance cost nears infinity, then the tolerance probability is 1. Besides, because of the property of exponential function, the tolerance probability does not change equably with the changing of tolerance cost. When the tolerance cost is smaller, its change generates greater influence on the tolerance probability; and with the tolerance cost becoming larger, its change generates less influence on the tolerance probability. For a practical intrusion tolerant system, when its tolerance cost is smaller, its performance of intrusion tolerance can be improved distinctly if its tolerance cost increases rationally, such as through increasing the redundancy, enhancing the security performance of hardware and software, optimizing the configuration, and improving the skill of engineers etc. However, when the tolerance cost of the system is larger, its performance of intrusion tolerance can not be improved clearly if its tolerance cost increases because that the redundancy, the resource of hardware and software, the configuration, and the skill of engineers etc have already achieved higher level.

2.2 The income function and the optimum tolerance cost

The income of the intrusion tolerant system is influenced by the reward and the cost of intrusion tolerance. It is defined by Formula (2).

$$U_S = P_A P_S E\text{-}C \tag{2}$$

Where, U_S is the income of the intrusion tolerant system; P_A is the probability that the intruder can intrude into the system successfully (see Definition (4) and Formula (5) in Section 3.1); P_S is the tolerance probability; E is the losses when the system has been intruded and it can not tolerate the intrusion; C is the tolerance cost. When the system is intruded, the function of intrusion tolerance decreases the probability of losses, and this is the reward of intrusion tolerance. So the ($P_A P_S E$) in Formula (2) is the reward. According to Formula (1) and (2), we can obtain Formula (3).

$$U_S = P_A(1\text{-}e^{-\lambda c})E\text{-}C \tag{3}$$

The goal of optimum strategy is to make the intrusion tolerant system get maximal income. Compute the partial derivative of income function in Formula (3) for tolerance cost, we will get the tolerance cost which can maximize the income. Let

$$\frac{\partial(U_S)}{\partial(C)} = \frac{\lambda P_A E}{e^{\lambda C}} - 1 = 0$$

Can obtain

$$C^* = \begin{cases} \lambda^{-1}\ln\lambda P_A E & \lambda P_A E \geq 1 \\ 0 & \lambda P_A E < 1 \end{cases} \tag{4}$$

Therefore, in order to maximize the income of the intrusion tolerant system, the tolerance cost should equal $\lambda^{-1}\ln\lambda P_A E$ when $\lambda P_A E \geq 1$, and the tolerance cost should be 0 when $\lambda P_A E<1$. This tolerance cost C* is called the optimum tolerance cost. The optimum strategy of the intrusion tolerant system is to make its tolerance cost equal the optimum tolerance cost.

It can be seen from Formula (4) that, when $\lambda P_A E \geq 1$, the probability that the system may be intruded is larger, then the optimum tolerance cost is larger, that is, the dangerous system needs large tolerance cost; in addition, the possible losses are larger, then the optimum tolerance cost is larger, that is, expensive system also needs large tolerance cost. When $\lambda P_A E<1$, the possible losses for intrusion will become very small. In this case, it is always uneconomical no matter how much that the system expends for intrusion tolerance. So the optimum strategy is to do nothing for intrusion tolerance, and the tolerance cost is 0. From the above analysis, we can see that the computation result of the optimum tolerance cost C* is in accord with the actual system.

3. The optimum strategy of intruder

3.1 Intrusion cost and intrusion probability

Definition 3 Intrusion cost: in order to intrude into one network system, the intruder's expenditures for buying intrusion tools and technologies, as well as the convertible expenditures for spent time and energy are called intrusion cost.

Of cause, the intrusion cost may also include the legal sanction and the moral condemnation. But in reality, the probability of legal sanction for network intrusion is very small, and the intruder does not care about the moral condemnation in general, so these expenditures can be ignored.

Definition 4 Intrusion probability: for some special intrusion cost, the statistical probability that the intruder can intrude into one network system successfully is called intrusion probability.

The practices have shown that, the network systems in reality almost all have some vulnerabilities, and some vulnerabilities have been found but others have not been found. Besides, the existing firewall and intrusion detection software can not guarantee the network from being intruded absolutely. So in theory, the intruder always has the probability of intruding into one network system successfully. For the intruder, it can be considered that her/his intrusion probability increases monotonously with her/his intrusion cost increasing, that is, larger intrusion cost corresponds to larger intrusion probability. If the intrusion cost nears infinity, we can consider that the intruder can spend infinite time and energy on intrusion, and her/his technology for intrusion is perfect. Under such circumstance, it can be considered that the intruder can intrude into the network system absolutely, that is, the intrusion probability is 1. If the intrusion cost is 0, the intruder expends nothing for the intrusion. Obviously, the intruder can not intruder into the network system, that is, the intrusion probability is 0. In the light of Formula (1) in Section 2.1, the intrusion probability is described by Formula (5) in the following.

$$P_A = 1\text{-}e^{-\gamma D} \qquad D \geq 0 \tag{5}$$

Where, P_A is the intrusion probability; D is the intrusion cost; γ is parameter of the exponential function, it is influenced by the skill of the intruder, the environment of the network, and the security of the network etc.

3.2 The income function and the optimum intrusion cost

The income of the intruder is influenced by the reward and the cost of intrusion. It is defined by Formula (6).

$$U_A = P_A\,(1\text{-}P_S)R\text{-}D \tag{6}$$

Where, U_A is the income of the intruder; P_A is intrusion probability; P_S is the tolerance probability of the intrusion tolerant system (defined in Section 2.1); R is the reward when the intruder can intrude into the system and the system can not tolerate the intrusion; D is the intrusion cost. According to Formula (5) and (6), Formula (7) can be obtained.

$$U_A = (1\text{-}e^{-\gamma D})\,(1\text{-}P_S)R\text{-}D \tag{7}$$

The goal of the intruder's optimum strategy is to get maximal income. Compute the partial derivative of income function in Formula (7) for intrusion cost, we will get the intrusion cost which can maximize the intruder's income. Let

$$\frac{\partial(U_A)}{\partial(D)} = \frac{\gamma(1 - P_S)R}{e^{\gamma D}} - 1 = 0$$

Can obtain

$$D^* = \begin{cases} \gamma^{-1}\ln\gamma(1 - P_S)R & \gamma(1 - P_S)R \geq 1 \\ 0 & \gamma(1 - P_S)R < 1 \end{cases} \tag{8}$$

D* is the optimum intrusion cost of the intruder. The optimum strategy of the intruder is to make her/his intrusion cost equal optimum intrusion cost. It can be seen from Formula (8), when $\gamma(1\text{-}\ P_S)R\geq1$, the reward that the intruder may obtain is larger, then the optimum intrusion cost is larger, that is, the intruder can expend much when the network system is profitable. Besides, the tolerance probability of the intrusion tolerant system is smaller, then the optimum intrusion cost is larger, that is, the intruder can expend much when the network is vulnerable. When $\gamma(1\text{-}\ P_S)R<1$, the reward that the intruder may obtain will become very small. In this case, no matter how much that the intruder expends for intrusion, she/he is always uneconomical. So her/his optimum strategy is to do nothing for intrusion, and the intrusion cost is 0 obviously. From the above analysis, it can be seen that the computation result of the optimum intrusion cost D* is consistent with the actual situation.

4. The Nash equilibrium of the intrusion tolerant system and the intruder

If the intrusion tolerant system is designed according to its optimum tolerance cost C*, and the intruder does not change her/his strategy unilaterally (that is, she/he does not change her/his intrusion cost D unilaterally), then the strategy of the intrusion tolerant system is the optimum strategy, and it can obtain the maximal income. Similarly, if the intruder intrudes the network system according to her/his optimum intrusion cost D*, and the intrusion tolerant system does not change its strategy unilaterally (that is, it does not change its tolerance cost C unilaterally), the strategy of the intruder is the optimum strategy. When the intrusion tolerant system and the intruder both adopt their optimum strategies, the game system achieves its Nash equilibrium.

If the intrusion tolerant system changes its strategy unilaterally, for example, it increases its tolerance cost C, the tolerance probability P_S will increase according to Formula (1). Then the optimum intrusion cost D* of the intruder will decrease according to Formula (8). If the intruder is sane, that is, she/he still uses the optimum intrusion cost which has decreased to intrude, her/his intrusion probability P_A will decrease according to Formula (5). Then the optimum tolerance cost C* of the intrusion tolerant system will decrease according to Formula (4). Therefore, this will prompt the intrusion tolerant system to decrease its tolerance cost. Similarly, if the intrusion tolerant system decreases its tolerance cost unilaterally, then the intruder who adopts the optimum strategy will prompt the intrusion tolerant system to increase its tolerance cost.

If the intruder changes her/his strategy unilaterally, for example, she/he increases her/his intrusion cost D, the intrusion probability P_A will increase according to Formula (5). Then the optimum tolerance cost C* of the intrusion tolerant system will increase according to Formula (4). If the design of the intrusion tolerant system is commendable, that is, it still uses the optimum tolerance cost which has increased to design the function of intrusion tolerance, the tolerance probability P_S will increase according to Formula (1). Then the optimum intrusion cost D* of the intruder will decrease according to Formula (8). Obviously, this will prompt the intruder to decrease her/his intrusion cost. Similarly, if the intruder decreases her/his intrusion cost unilaterally, the intrusion tolerant system which adopts the optimum strategy will prompt the intruder to increase her/his intrusion cost.

It can be seen from the above analysis that, the balance between the intrusion tolerant system and the intruder is steady.

If the two sides are all sane, that is, they do not change their strategies randomly, the normal interference will not destroy the balance.

5. The evaluation of parameters

In order to obtain the optimum tolerance cost C*, the intrusion tolerant system must know the values of λ, P_A, and E according to Formula (4). The values of λ and P_A are influenced by the network's application property, physical environment, vulnerabilities, and the defendable performance of the firewall and intrusion detection software etc. The value of E is influenced by the network's importance, accessing frequency, the number of users, and the recover cost etc. For a special intrusion tolerant system, the values of λ, P_A, and E can be evaluated through the Delphi method according to the practical situation.

In order to compute the final tolerance expenditures, the intrusion tolerant system must know the conversion relationship between the tolerance cost C and the practical expenditure, that is, a unit of tolerance cost equals how much money. The conversion relationship can be evaluated through Formula (1) and the Delphi method. Select a special value of tolerance probability and compute the corresponding value of tolerance cost through Formula (1). Then obtain the practical expenditure of the selected tolerance probability through the Delphi method according to the practical system. Thus, the conversion relationship between the tolerance cost C and the practical expenditure can be gotten.

Similarly, the intruder also needs to evaluate the values of γ, P_S, R, and the conversion relationship between the intrusion cost and the practical expenditure. The intruder can adopt the same method of the intrusion tolerant system. We do not explain it in detail here.

6. Comparison to the existing models

In the model proposed by Goseva (Goseva P. K., Wang F., & Wang R, 2001), the work states of intrusion tolerant system were summarized as good state, vulnerable state, active attack state, masked compromised state, undetected compromised stare, triage state, fail-secure state, graceful degradation state, and failed state. This model mainly described the static property of intrusion tolerant system. Basing on this model, Peng designed a model based on the finite state automaton machine (Peng W. L., Wang L. N., & Zhang H.G, 2005). The model described the dynamic property of intrusion tolerant system, and provided the condition and process of state transition. The model proposed by Cui classed the effect of intrusion on system resource and control (Cui J. S., Wang L. N., & Zhang H. G, 2004), and this model described the recourse state and recovery method of the intrusion tolerant system. Compared to these existing models, the main contributions of our model are that:

(1) Besides the property of intrusion tolerant system, the behavior of intruder is also described in the model. So the description of the model for the intrusion tolerant system is more comprehensive.

(2) The cost and reward of intrusion tolerance is analyzed in the model. In order to design a cost-effective intrusion tolerant system, this work is indeed necessary.

(3) This model adopts the method of quantitative analysis, so it can provide more accurate description compared to the qualitative analysis in the existing models.

7. Conclusions

Intrusion tolerance is the rising third generation technology of network security. It can provide the ultimate security guarantee for the information system in internet. The modeling for intrusion tolerant system is the basic work for studying the intrusion tolerance. For the shortcomings of the existing models, a model of intrusion tolerant system based on game theory is proposed in this paper. The intrusion tolerant system and the intruder are seen as the two sides of the game. The optimum strategies of the two sides are obtained through quantifying their income functions. The Nash equilibrium of the game system is analyzed in detail. The analysis results of the formulas in the model show that, the proposed model can reflect the actual property of the practical system.

References

Arsenault D., Sood A., & Huang Y. (2007). Secure, resilient computing clusters: self-cleansing intrusion tolerance with hardware enforced security (SCIT/HES). *Second International Conference on Availability, Reliability and Security*. Fairfax, Virginia.

Castro M., & Liskov B. (2000). Proactive recovery in a Byzantine-fault-tolerant system, *The 4th symposium on operating systems design and implementation*. pp. 273-288.

Cui J. S., Wang L. N., & Zhang H. G. (2004). A parallel model of intrusion tolerance system: RC model. *Chinese Journal of Computers*, 4, 500-506.

Goseva P. K., Wang F., & Wang R. (2001). Characterizing intrusion tolerant systems using a state transition model, *DARPA Information Survivability Conference and Exposition*. pp. 211-221.

Jing J. W., & Feng D. G. (2002). An intrusion tolerant CA scheme. *Journal of Software*, 8, 1417-1422.

Jonsson E., & Olovsson T. (1997). A quantitative model of the security intrusion process based on attacker behavior. *IEEE Transactions on Software Engineering*, 4, 235-245.

Liu P. (2002). Architecture for intrusion tolerant database systems. *Computer Security Applications Conference*. pp.311-320.

Madan B. B., Goseva P. K., Vaidyanathan K., & Trivedi K. S. (2004). A method for modeling and quantifying the security attributes of intrusion tolerant system. *Performance Evaluation*, 1, 167-186.

Peng W. L., Wang L. N., & Zhang H.G. (2005). Research of intrusion tolerant system based on finite state automaton machine. *MIN-MICRO SYSTEMS*, 8, 1296-1300.

Singh S., Cukier M., & Sanders W. H. (2003). Probabilistic validation of an intrusion-tolerant replication system. *Proceedings of the International Conference on Dependable Systems and Networks*. San Francisco, CA, USA, pp. 616-624.

Yin L.H., & Fang B.X. (2006). Security attributes analysis for intrusion tolerant system. *Chinese Journal of Computers*, 9, 1505-1512.