Analysis and Optimization of System Intrusion Tolerance Capacity Based on Markov

Zhiyong Luo[1,2], Bo You[2], Peng Wang[1], Jie Su[1], and Yi Liang[2]
(Corresponding author: Zhiyong Luo)
School of Computer Science and Technology , Harbin University of Science and Technology[1]
Harbin 150080, China
School of Mechanical Engineering, Harbin University of Science and Technology[2]
(Email: luozhiyongemail@sina.com)
(Received June 17, 2016; revised and accepted Aug. 20 & Sept. 3, 2016)

Abstract

After the occurrence of network intrusion, the system is running in a state of the lower quality. Along with the system's tolerant capacity decline, it eventually stops providing services or even shutdown. This paper developed a Markov intrusion tolerance model (SMP), aiming at difficultly evaluates and enhances the system's tolerant capacity issues. Based on formalized related security state of the model, the quantitative analysis of system's tolerant capacity is performed. Then calling the parameters solution algorithm to calculate the SMP model's average time of system fault (ATOSF) under each security state. After analyzing the variety track of ATOSF, found the system's tolerant key points. Maintenance of these key points, it can enhance the system's tolerant capacity, so as to increasing the availability of the system. The experiment results provide evidence that using the Markov to the system's tolerant capacity in the quantization process is feasible and effective.

Keywords: Capacity Analysis; Intrusion Tolerance; Markov; SMP; State Transition

1 Introduction

People use the network resources facilitate because of the Internet openness, but it also brings a lot of security threat [7]. Early network security technology focuses on solving two problems contains block the way to the invasion and repair the system security vulnerabilities. Intrusions and system vulnerabilities have unpredictability [5]. Therefore, it is impossible to repair the system in advance of all security vulnerabilities. It will certainly lead to the success of network intrusion. Researchers need to develop a mechanism to guarantee the system operating correctly under state invasion. Researchers need to develop a mechanism to guarantee the system operating correctly under state invasion, and it is called Intrusion Tolerance Technology.

In 1985, Fraga and Powell [3] have proposed intrusion tolerance technology. However, in recent years, it develops under the impetus MAFTIA and OASIS projects. It is as the current network security core technology, Intrusion tolerance technology allows weaknesses in the system. With the operation of the system, these weaknesses are likely to be captured intruder and use. Finally, it will be successful invasion. Intrusion tolerance technology is in this case to ensure the system's key features and essential services (allow degraded model) continues to run. In the study of intrusion tolerance system, we use the security attributes quantitative analysis method to accurately predict the performance of the system, and we find the weaknesses and the existence of critical points system. We raise key intrusion tolerance and achieve the purpose of increasing the system running security and long.

Currently, we use quantitative methods to analyze the intrusion tolerance system has been taken seriously by scholars. Abroad, Madan [6] uses a quantitative method SMP model to analyze the intrusion tolerance system. Denning et al. [2] built an intrusion tolerant system, which improves the tolerance by establishing the steady-state probability for each state node. Ilgun et al. [4] had established the state analysis rules of intrusion tolerance system, which can effectively improve the system tolerance. In China, Jia et al. [12] establish an intrusion tolerance public key encryption scheme in a standard model and use a probabilistic analysis for quantitative analysis model. Chen et al. [1] use the theory of Markov to quantitative analysis database security in intrusion tolerant systems, which ensure the safe operation of the database server. Xing et al. [11] putted forward the calculation method of a kind of measurement tolerance, in the case of attack is inevitable, as long as not beyond measure, the system should provide effective services to legitimate users. Through the evaluation of the results of simulation experiment, for different attack tolerance strategy to provide effective help. Wei et al. [10] built tolerating invasion

ability model to obtain stability probability of model in integrity status using the Markov chain, and they constructed multi-term index of tolerating invasion ability, such as network information machine density, integrity, system autonomy and service availability, and carried out quantitative calculation according to influence on network system of invasion and function of tolerating invasion.

In this paper, we add the Intrusion Learning State based on SITAR [9] intrusion tolerant system architecture, and build an optimized state transition model. Since the state of the model between the transfers meet the transfer of Markov, we use the Markov model to quantitative analysis. It provides a theoretical guidance to build a reliable, confidential and complete tolerance system.

2 Optimized Tolerant System State Transition Model

Tolerant system that protects objects is diversity. The framework, tolerance policy, security algorithms of each tolerant system is different. In order to abstract describe the dynamic behavior of intrusion tolerant system, we build the optimized SITAR model, and its structure is shown in Figure 1.

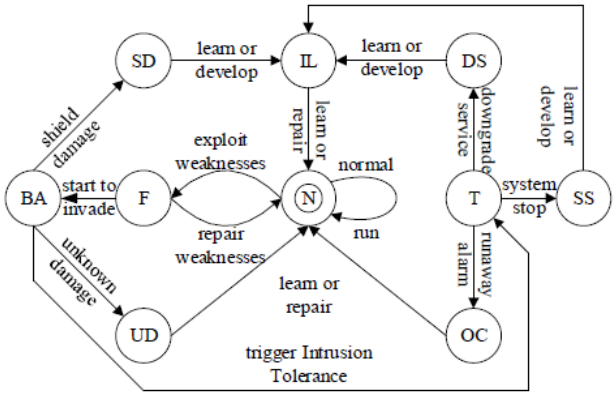

Figure 1: Tolerant system state transition model

In Figure 1, the system in the first State N (Normal State) is normal operation. The intruders detect weaknesses in the system and use these weaknesses. The system will enter the F state (Fragile State) and still run. If the system detects its own weakness in F state and is repaired successfully, the system will return to State N. If the intruders successfully exploit the system weaknesses to start to invade the system, the system will enter State BA (Being Attacked State). If the system which is under the invasion can mask the relative harm, the system will enter State SD (Shield Damage State). The system will wait to learn or improve and enters IL (Intrusion Learning State). If the system which is under the invasion cannot mask the relative harm and the tolerant system is not triggered, the intruders will make some damage to the system. The system will enter State UD (Unknown Damage State). The system will wait the improvement or repair of the administrators and return to State N. If the system which is under the invasion cannot mask the relative harm and the tolerant system is triggered, the system will enter State T (Trigger State). The system runs in State T, the tolerant system will evaluate the system's current status.

After the assessment, if we take the lower level of strategy to continue running, the system will enter State DS (Downgrade Service Status). The system will wait to learn or improve and enters IL. After the assessment, if we take the safe stop strategy, the system will enter State SS (Security Stopped States). The system will wait to learn or improve and enters IL. After the assessment, if the system is completely out of control, the system will enter State OC (Out of Control State). The system will wait the improvement or repair of the administrators and return to State N. The system is in the IL state and completes the learning, improvement or perfect. The system will return State N and start again.

After analyzing, we find that the model in each state node has certain closeness. The conversion in each state node does not affect the previous state. The characteristics of the model meet the Markov process SMP (Markov Process). Therefore, we can use Markov to analyze the model. Additionally, the model contains a number of states. Each state can take the appropriate security policy and make sure the system run normally. Therefore, the model also has a certain degree of flexibility and security.

3 Build the SMP Probability Model

We assume that the duration of each state of the node is random and has an arbitrary distributed. The conversion in each state node does not have the memory. Meanwhile, in order to simplify the analysis, we will all pay the cost of the attack are considered time cost.

3.1 DTMC Matrix

DTMC (Discrete-time Markov Chain) matrix is that we use discrete time values and combine the Markov chain technology to make each node of the state space in the process of the Markov. Each node transition probabilities in a state space form a matrix, which is called the DTMC Matrix. We analyze the Optimized SMP model and get the state space of the system, which is called $S_{space} = \{N, F, BA, SD, UD, T, DS, SS, OC, IL\}$. In addition, P_{s_l}, P_d, $P_{s_i}, P_w, P_a, P_s, P_u, P_d, P_h, P_1, P_2, P_3, P_n$, P_{on}, P_{un}, P_{in} represent a conversion between the probability of each state. The SMP probabilistic model is shown in Figure 2.

In Figure 2, the meanings of the probability symbols are as follows:

$P_{s_l} : SD \to IL$, it is a probabilistic that the system shields the intrusion harms but needs to learn or develop.

$P_{d_i} : DS \to IL$, it is a probabilistic that the system can provide the downgrade service but needs to learn or develop.

$P_{s_i} : SS \to IL$, it is a probabilistic that the system is safe to stop running and needs to learn or develop.

$P_w : N \to F$, it is a probabilistic that the system has weak and is found.

$P_a : F \to BA$, it is a probabilistic that the system successfully exploits vulnerabilities invasion.

$P_s : BA \to SD$, it is a probabilistic that the system successfully shields the intrusion.

$P_u : BA \to UD$, it is a probabilistic that the system cannot find the intrusion.

$P_d : T \to DS$, it is a probabilistic that the system finds the intrusion and provides the downgrade service.

$P_h : T \to SS$, it is a probabilistic that the system finds the intrusion and is to stop running successfully.

$P_1 = 1 - P_w - P_a : F \to N$, it is a probabilistic that the system finds the weak and repair successfully.

$P_2 = 1 - P_s - P_u : BA \to T$, it is a probabilistic that the system detects the presence of the invasion and successfully triggers intrusion tolerant systems.

$P_3 = 1 - P_d - P_h : T \to OC$, it is a probabilistic that the system eventually stops running because of the invasion caused the fault occurs.

$P_n : N \to N$, it is a probabilistic that the system is safe to run.

$P_{on} : OC \to N$, it is a probabilistic that the system is completely out of control, but improved or repaired return to normal operation.

$P_{un} : UD \to N$, it is a probabilistic that the system is not found in the invasion, and it improves or repairs to rerun after a period of time.

$P_{in} : IL \to N$, it is a probabilistic that the system develops and returns to normal after learning, improving or perfecting.

In Figure 2, transition probability matrix P describes the possibility of the system transferring between the various states. The probability value can be determined by the experience of the network management or determined through the intrusion injection mode. The transition probability matrix P of the system state transition model DTMC:

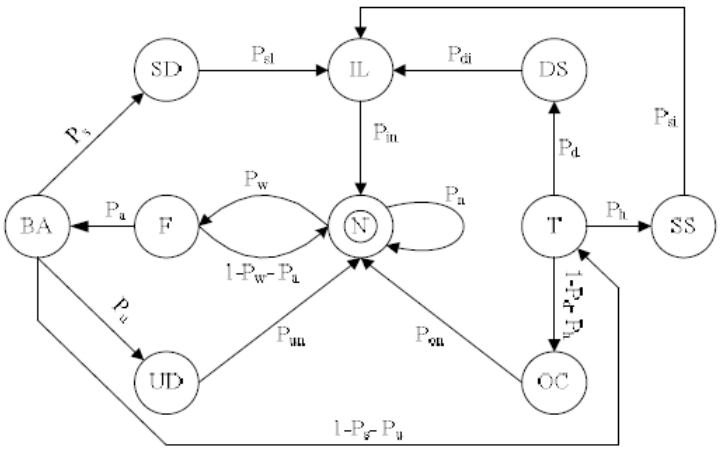

Figure 2: DTMC transition model

$$P = \begin{array}{c} \\ N \\ F \\ BA \\ SD \\ UD \\ T \\ DS \\ SS \\ OC \\ H \end{array} \begin{array}{c} \begin{array}{cccccccccc} N & F & BA & SD & UD & T & DS & SS & OC & H \end{array} \\ \begin{bmatrix} P_n & P_w & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ P_1 & 0 & P_a & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & P_s & P_u & P_2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & P_{s_1} \\ P_{un} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & P_d & P_h & P_3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & P_{d_i} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & P_{s_i} \\ P_{on} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ P_{in} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

3.2 DTMC State Duration

The state duration is that each state holds time in SMP model. H represents the duration matrix of the SMP model. h_i represents some a state duration in SMP model, $i \in S_{space}$, $H = [h_N, h_F, h_{BA}, h_{SD}, h_{UD}, h_T, h_{DS}, h_{SS}, h_{OC}, h_{IL}]$. In Figure 2, the meanings of the state duration are as follows:

h_N: It is a time that the system runs normally and its weakness is not found by an intruder.

h_F: It is a time that the system is not successful invasion when the intruder finds the weakness and uses it.

h_{BA}: It is a time that the system finds invasion and triggers a successful intrusion tolerance.

h_{SD}: It is a time that the system shields invasion successfully and runs normally.

h_{UD}: It is a time that the system cannot find invasion and runs normally.

h_T: It is a time that the system is evaluated and decides what the security policies the system can use to deal with the invasion.

h_{DS}: It is a time that the system finds the invasion, but cannot block it and only provide the downgrade service.

h_{SS}: It is a time that the system is safe to stop running.

h_{OC}: It is a time that the system is completely out of control.

h_{IL}: It is a time that we learn the invasion and optimizes the system.

4 SMP Model Analysis

According to the quantitative analysis of the SMP model analysis, the network administrator can better safeguard system. In order to quantify the simplified SMP model and accurately, this paper gives the following definition.

Definition 1. *DTMC state probability, the probability of each state of the system into SMP model. In this paper, we use matrix to express V. So $V = [v_N, v_F, v_{BA}, v_{SD}, v_{UD}, v_T, v_{DS}, v_{SS}, v_{OC}, v_{IL}]$, v_i expresses State i DTMC state probability, $i \in S_{space}$.*

Definition 2. *SMP stability probabilities, the system in the state SMP model and continue to stay in the percentage of the whole model of duration. It is expressed by π, so π_i expresses State i SMP stability probability.*

Definition 3. *Average Time of System Fault (ATOSF), The system starts from a state of implementation of the SMP model in the reach system to stop running state of the average length of time due to failure caused by the invasion.*

4.1 SMP Model Security

Attributes SMP model security attributes mainly consider three main aspects. It each expresses the availability, confidentiality and integrity.

The availability expresses that the model can provide services for legitimate users, the probability of occurrence is expressed by P_{Ava}.

The confidentiality expresses that the model cannot be stolen the data by the intruder, the probability of occurrence is expressed by P_{Con}.

The integrity expresses that the model is not modified by the intruder; the probability of occurrence is expressed by P_{Int}.

The state space of node S_{space} as shown in Figure 2 is divided into two subsets: The invaders invasion behavior node space S_I and The response behavior of the system adopted in the post invasion node space S_R, $S_I = \{N, F, BA\}$; $S_R = \{SD, UD, T, DS, SS, OC, IL\}$. In State S_R, the system is in a certain state, SMP model security attributes will be lost, the state format safety damaged space S_D. Contrary, the system is in another certain state, SMP model security attributes will not be lost, and the state format safety not damaged space S_U.

Through the analysis, the probability of SMP model security attributes is related to the stability probability of each state node space S_{space}. If we use π to express the stability probability, π_i expresses each state node space S_{space}, $i \in S_{space}$.

The system in the UD, SS, OC state stops running and does not provide any service. The safety damaged space of the system $SD = \{UD, SS, OC\}$, safety not damaged space $SU = \{SD, T, DS, IL\}$. At this time, the availability probability $P_{Ava} = 1 - \pi_{UD} - \pi_{SS} - \pi_{OC}$.

The system is in the UD, OC state, when the intruder attacks the server and makes the system in unsafely stopping state. The system will make the data stolen. The safety damaged space of the system $SD = \{UD, OC\}$, The safety not damaged space of the system $SU = \{SD, T, DS, SS, IL\}$. At this time, the confidentiality probability $P_{Con} = 1 - \pi_{UD} - \pi_{OC}$.

The system in the UD, SS, OC state, the integrity will be damaged by the intruder. The safety damaged space of the system $SD = \{UD, SS, OC\}$, the safety not damaged space of the system $SU = \{SD, T, DS, IL\}$. At this time, the integrity probability $P_{Int} = 1 - \pi_{UD} - \pi_{SS} - \pi_{OC}$. Therefore, the probability of SMP model security attributes:

$$P_k = 1 - \sum_{j \in S_D} \pi_j, \quad k = Ava, Con, Int \tag{1}$$

SMP model security attributes is inversely proportional to the probability of the safety damaged space π_j.

4.2 SMP Model Parameters Algorithm

The stability probability of SMP model each state mainly consider two input parameters: each state DTMC transition probability matrix P and each state DTMC duration matrix H. Through the above analysis, SMP model parameters algorithm is shown.

Step 1: Through Equation (2), we calculate Figure 2 each state DTMC probability matrix V.

$$\begin{cases} V' & = V \cdot P \\ \sum_{i \in S_{space}} v_i & = 1 \end{cases} \tag{2}$$

The matrix P is DTMC transition probability matrix. Through Equation (2), we can calculate the relationship of each state's DTMC probability in SMP model, which is shown in Equation (3).

$$\begin{aligned} v_N &= P_n v_N + P_1 v_F + P_{un} v_{UD} + P_{on} v_{OC} + P_{in} v_{IL} \\ &= [P_n + P_1 P_w + P_{un} P_u P_a P_w + P_{on} P_3 P_2 P_a P_w \\ &\quad + P_{in}(P_{sl} P_s P_a P_w + P_{d_i} P_d P_2 P_a P_w \\ &\quad + P_{s_i} P_h P_2 P_a P_w)] v_N \\ v_F &= P_w v_N \\ v_{BA} &= P_a v_F = P_a P_w v_N \end{aligned}$$

$$\begin{aligned} v_{SD} &= P_s v_{BA} = P_s P_a P_w v_N \\ v_{UD} &= P_u v_{BA} = P_u P_a P_W v_N \\ v_T &= P_2 v_{BA} = P_2 P_a P_w v_N \\ v_{DS} &= P_d v_T = P_d P_2 P_a P_w v_N \\ v_{SS} &= P_h v_T = P_h P_2 P_a P_w v_N \\ v_{OC} &= P_3 v_T = P_3 P_2 P_a P_w v_N \\ v_{IL} &= P_{sl} v_{SD} + P_{d_i} v_{DS} + P_{s_i} v_{SS} \\ &= (P_{sl} P_s P_a P_w + P_{d_i} P_d P_2 P_a P_w \\ &\quad + P_{s_i} P_h P_2 P_a P_w) v \end{aligned} \tag{3}$$

Through $\sum_{i \in S_{Space}} v_i = 1$, we can get $v_N + v_F + v_{BA} + v_{SD} + v_{UD} + v_T + v_{DS} + v_{SS} + v_{OC} + v_{IL} = 1$. We put it into Equation (3) and get the DTMC probability of State N:

$$\begin{aligned} v_N &= 1/[P_n + P_1 P_w + PA + PB + PC] v_N \\ PA &= P_{un} P_u P_a P_w \\ PB &= P_{on} P_3 P_2 P_a P_w \\ PC &= P_{in}(P_{sl} P_s P_a P_w + P_{d_i} P_d P_2 P_a P_w \\ &\quad + P_{s_i} P_h P_2 P_a P_w) \end{aligned} \tag{4}$$

We put Equation (4) into Equation (3) and get each state DTMC probability matrix V of the SMP model.

Step 2: We put the DTMC probability matrix V and duration matrix H into Equation (5).

$$\pi_i = fracv_i h_i \sum_j v_j h_j, \quad i, j \in S_{Space} \tag{5}$$

We calculate the SMP model each state stability probability as shown:

$$\begin{aligned} Sum &= \sum_{j \in S_{space}} v_j h_j \\ &= [h_N + h_F P_w + h_{BA} P_a P_w + h_{SD} P_s P_a P_w \\ &\quad + h_{UD} P_u P_a P_w + h_T P_2 P_a P_w \\ &\quad + h_{DS} P_d P_2 P_a P_w + h_{IL}(P_{sl} P_s P_a P_w \\ &\quad + P_{d_i} P_d P_2 P_a P_w + P_{s_i} P_h P_2 P_a P_w)] v_N \\ \pi_N &= h_N v_N / Sum \\ \pi_F &= h_F P_w v_N / Sum \\ \pi_{BA} &= h_{BA} P_a P_w v_N / Sum \\ \pi_{SD} &= h_{SD} P_s P_a P_w v_N / Sum \\ \pi_{UD} &= h_{UD} P_u P_a P_w v_N / Sum \\ \pi_T &= h_T P_2 P_a P_w v_N / Sum \\ \pi_{DS} &= h_{DS} P_d P_2 P_a P_w v_N / Sum \\ \pi_{SS} &= h_{SS} P_h P_2 P_a P_w v_N / Sum \\ \pi_{OC} &= h_{OC} P_3 P_2 P_a P_w v_N / Sum \\ \pi_{IL} &= h_{IL}(P_{sl} P_s P_a P_w + P_{d_i} P_d P_2 P_a P_w \\ &\quad + P_{s_i} P_h P_2 P_a P_w) v_N / Sum \end{aligned} \tag{6}$$

Step 3: We put the SMP model state stability probability into Equation (1) and get the security attributes probability:

$$\begin{aligned} P_{Ava} &= 1 - (h_{UD} P_u P_a P_w + h_{SS} P_h P_2 P_a P_w \\ &\quad + h_{OC} P_3 P_2 P_a P_w) v_N / Sum \\ P_{Con} &= 1 - (h_{UD} P_u P_a P_w \\ &\quad + h_{OC} P_3 P_2 P_a P_w) v_N / Sum \\ P_{Int} &= 1 - (h_{UD} P_u P_a P_w + h_{SS} P_h P_2 P_a P_w \\ &\quad + h_{OC} P_3 P_2 P_a P_w) v_N / Sum \end{aligned} \tag{7}$$

According to SMP model parameters algorithm, we combine the specific parameters of the network intrusion tolerance system and can accurately quantify tolerance system and provide data basis for the future analysis.

4.3 SMP State Average Fault Time

According to Definition 3, the average fault time is a measure of an important indicator of intrusion tolerance system resistance ability. SMP model some a state average fault time is bigger and it expresses the invasion of the state of the system to stop running time is long, the cost is high, the reliability of the system is also higher. We analyze the SMP model in Figure 2 and find some state is stopping running state that the system has some problems. We repair the weakness of the system or develop the system in this state by the mode administrator manual to make the system run again. We set a model in such a state is called a stop state set SE. The collection of the rest of the state is called intermediate state set SM. According to the Trivedi algorithm [8], we can get the ATOSF:

$$ATOSF = \sum_{i \in S_M} Con_i h_i \tag{8}$$

In Equation (8), Con_i expresses total number of the system in the stop State i. h_i is the duration time of State i. The system always starts in State N and the Con_N is the key. Through Figure 2, through State N probability is divided into inflow probability P_{in} and outflow probability P_{out}, $P_{in} + P_{out} = 1$. Because Con_N is the total number that the system through State N before entering the state stopped, so $Con_N = 1/P_{in} = 1/(1 - P_{out})$. In SMP model, the factor of the effect State N coming into probability P_{in} is a problem. The paper calculates the inflow probability P_{out} to ensure Con_N.

Through the analysis, the system in State N entering the stopping state has five paths: $N \to F \to BA \to SD \to IL$, $N \to F \to BA \to UD$, $N \to F \to BA \to T \to OC$, $N \to F \to BA \to T \to DS \to IL$ and $N \to F \to BA \to T \to DS \to IL$. We analysis the five path and find the system in through State BA enters the stopping state and the stopping state enters State N again by the administrator. The outflow probability of State N $P_{out} = P_a P_w$. We get the SMP model each State Con and the

Table 1: Software configuration of network server

Server ID	Operation system	Provide services	Weaknesses ID
IP_1	Windows 2003 Server	FTP Server	CVE-2004-0575 CVE-2008-0702
IP_2	Windows 2003 Server	HTTP Server	CVE-2002-0364 CVE-2006-2379
IP_3	Windows 2000 Server	SQL Server	CVE-2007-0038 CVE-2004-0893

system ATOSF.

$$
\begin{aligned}
Con_N &= 1/(1-P_aP_w) \\
Con_F &= P_wCon_N \\
Con_{BA} &= P_aP_wCon_N \\
Con_{SD} &= P_sP_aP_wCon_N \\
Con_{UD} &= P_uP_aP_wCon_N \\
Con_T &= P_2P_aP_wCon_N \\
Con_{DS} &= P_dP_2P_aP_wCon_N \\
Con_{SS} &= P_hP_2P_aP_wCon_N \\
Con_{OC} &= P_3P_2P_aP_wCon_N \\
Con_{IL} &= (P_sP_aP_w + P_dP_2P_aP_w + P_hP_2P_aP_w)Con_N \\
ATOSF &= \sum_{i \in S_M} Con_i h_i \qquad (9)
\end{aligned}
$$

ATOSF is an important index that makes the system safe and reliable. We enlarge the ATOSF to can increase the attack price. However, the ATOSF is related to the Con_i and h_i. With the fixed intrusion tolerance system, each State Con can be ensured. We can enlarge the state duration time h to make the ATOSF.

5 Experiment Analyses and Evaluation

5.1 Experimental Environment

The topological structure of the network of the SMP model is shown in Figure 3. The server IP_1 to IP_3 forms an intrusion tolerance system in the control strategy of firewall to provide the corresponding network service with the host of users inside and outside the network. The software configuration and the weakness of its specific are shown in Table 1. The author organizes the student to simulate the intrusion tolerance system, so as to obtain test data.

5.2 Experiment Analysis and Evaluation

Through the analysis of the test data and the estimation of the statistics, the following parameters values are shown: DTMC transition probability matrix P. The system is always in normal operation. So $P_n = 1$. However, when the system is managed and run again. So $P_{s_l} = P_{s_i} = P_{d_i} = P_{in} = P_{un} = P_{on} = 1$. Each server tolerance system has a lot of weakness in Figure 3, so the weakness of the system is found and its probability is $P_w = 0.3$. When the invaders found weaknesses in the system and successfully exploited these vulnerabilities to invade the tolerance system, its probability is $P_a = 0.5$. The system detects the weakness and timely repair and its probability is $P_1 = 1 - P_w - P_a = 0.2$. The system is found to be invaded and successfully shield the intrusion and its probability is $P_s = 0.4$. The system could not find the intrusion and its probability is $P_u = 0.2$. The system detects intrusion and successful trigger intrusion tolerance system and its probability is $P_2 = 1 - P_s - P_u = 0.4$. The intrusion system continues to run but providing degraded service and its probability is $P_d = 0.5$. The system finds the invasion and succeeds to stop system and its probability is $P_h = 0.4$. The system eventually stops running because of the invasion and its probability is $P_3 = 1 - P_d - P_h = 0.1$.

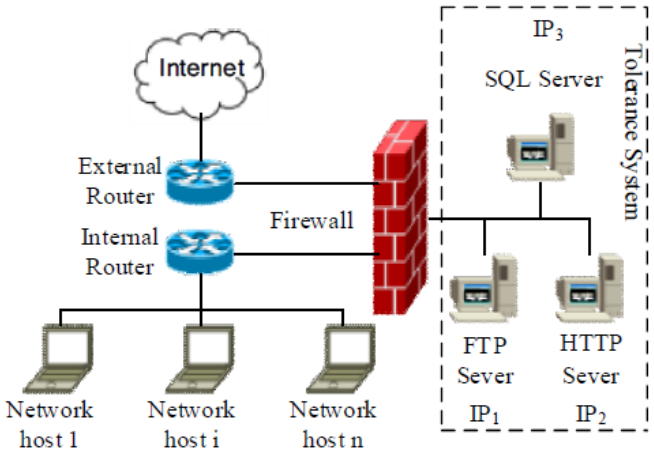

Figure 3: Topology model of the testing network

The duration time matrix H. The tests show that the system degrading service operation has most of the time. The system is the shortest in the tolerance time triggering. The test shows that the degraded service operation time of the system is the longest, the tolerance to trigger time is the shortest, the normal operation time and the no

Table 2: SMP model parameters

State i	DTMC probability v_i	SMP stability probability π_i	The visits number of each state Con_i
N	0.6098	0.6044	1.1765
F	0.1512	0.2698	0.3530
BA	0.0756	0.0299	0.1765
SD	0.0302	0.0150	0.0706
UD	0.0151	0.0150	0.0353
T	0.0302	0.0059	0.0706
DS	0.0151	0.0059	0.0353
SS	0.0121	0.0180	0.0282
OC	0.0030	0.0074	0.0071
IL	0.0575	0.0285	0.1341

found invasion to continue running time are similar, the shielding the intrusion behavior to continue running time and the learn and improve time are similar, the time of the other states are not equal. In this paper, we use the unit time measurement, and the duration of each state is set to: $h_N = 1, h_F = 1.8, h_{BA} = 0.4, h_{SD} = 0.5, h_{UD} = 1, h_T = 0.2, h_{DS} = 4, h_{SS} = 1.5, h_{OC} = 2.5, h_{IL} = 0.5$.

We put all the parameters into SMP model parameters algorithm Equation (9), and calculate the SMP related parameters the SMP parameters are shown in Table 2 We put Table 2 into Equation (7) and Equation (8). We can get the system availability probability $P_{Ava} = 0.9596$, the confidentiality probability $P_{Con} = 0.9776$, the integrity probability $P_{Int} = 0.9596$, the total probability $ATOSF = 2.2355$. We make the further analysis with Equation (8) and get SMP model each state ATOSF, which is shown in Figure 4.

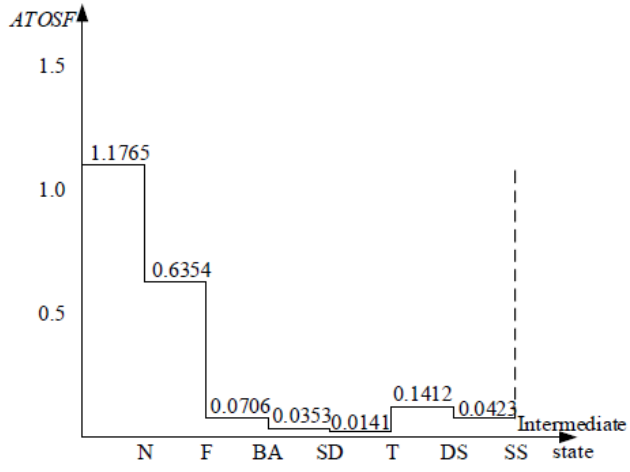

Figure 4: Change trajectory of each intermediate state's ATOSF

As can be seen from Figure 4, the duration of the intermediate state of the overall system ATOSF from big to small order: $\{N, F, DS, BA, SS, SD, T\}$. If we enlarge the intermediate state $\{N, F, DS\}$ duration time, we can get the effectively increasing the system ATOSF. At the same time, it also increases the cost of the invasion and enhances the reliability of the system.

6 Conclusion

Intrusion tolerance technology is an important technology of network security management. It is a kind of technology to ensure the operation of the network after the intrusion happened. So the research on the intrusion tolerance is a hotspot. This paper is based on the SITAR intrusion tolerance system structure and increases the attack state and puts forward to optimize the state transfer model. Due to the conversion of the state of the model meeting the semi Markov theory, the system introduces the DTMC to construct the optimized SMP model. Through the quantitative analysis of the model, we calculate the ATOSF locus of the model each state.

Finally, through the analysis of the test data, we can get the conclusion that enlarge model intermediate state $\{N, F, DS\}$ duration time to add the difficulty of intrusion. The next step for the research will be further improved the system. We increase the tolerance of online to repair system, reduce the system stop state, and improve system availability.

Acknowledgments

This research was supported by the National Natural Science Foundation of China (Grant No.61403109). Declares: The authors declare that there is no conflict of interest regarding the publication of this manuscript.

References

[1] C. Q. Chen, X. B. Pei, H. Zhou, Y. S. Liu, "A Markov evaluation model for the survivability of real-time database with intrusion tolerance," *Chinese Journal of Computer*, vol. 34, no. 10, pp. 1907–1915, 2011.

[2] D. E. Denning, "An intrusion-detection model," *IEEE Transaction on Software Engineering*, vol. 13, no. 2, pp. 222–223, 2011.
[3] J. S. Fraga, D. Powell, "A fault and intrusion to lerant file system," in *Proceedings of the 3rd International Conference on Computer Security*, Dublin, Ireland, pp. 203–218, 1985.
[4] I. Koral, A. K. Richard, "State transition analysis:a rule-based intrusion detection approach," *IEEE Transactions on Software Engineering*, vol. 21, no. 3, pp. 181–199, 2012.
[5] Z. Luo, B. You, G. Yu, J. Su, "Research of intrusive intention self-recognition algorithm based on three-tier attack graph," *ICIC Express Letters, Part B: Applications*, vol. 6, no. 6, pp. 1575–1580, 2015.
[6] B. B. Madan et al., "A method for modeling and quantifying the security attributes of intrusion tolerant systems," *Performance Evaluation*, vol. 56, no. 14, pp. 167–186, 2004.
[7] J. Su, S. Liu, Z. Y. Luo, G. L. Sun, "Method of constructing an anonymous graph based on information loss estimation," *Tongxin Xuebao/Journal on Communications*, vol. 37, no. 6, pp. 56–64, 2016.
[8] K. S. Trivedi, *Probability and Statistics with Reliability Queuing, and Computer Science Applications*, 2nd Edition, New York: John Wiley and Sons, 2002.
[9] G. Wang, P. Wang, Z. Luo, S. Zhu, "Transfer model based on state of finite semi-markov automata intrusion tolerance," *International Journal of Security and Its Applications*, vol. 10, no. 3, pp. 183–192, 2016.
[10] K. Wei, F. Zhang, "Based on Markov network tolerate invasion ability evaluation model," *Computer Simulation*, vol. 33, no. 7, pp. 289–292, 2016.
[11] Y. F. Xing, C. Y. Luan, "A quantitative analysis and detection of intrusion tolerance system model," *Information Science*, vol. 33, no. 8, pp. 55–58, 2015.
[12] J. Yu, X. G. Cheng, F. G. Li, Z. K. Pan, F. Y. Kong, R. Hao, "Provably secure intrusion-resilient public-key encryption scheme in the standard model," *Journal of Software*, vol. 24, no. 2, pp. 266–278, 2013.

Biography

Luo Zhiyong, born in 1978, master tutor, associate professor, is currently a PhD candidate at Intelligent Machine Institute, Harbin University of Science and Technology, China. He received his bachelor degree from Harbin University of Science and Technology, China, in 2001. His research interests include network security, scientific workflow and industrial design and scheduling.

You Bo, born in 1962, doctoral tutor, professor, post doctorate, is currently working at Intelligent Machine Institute, Harbin University of Science and Technology, China.

Wang Peng, born in 1993, master, is currently studying at Harbin University of Science and Technology, China.

Su Jie, born in 1979, master tutor, associate professor, is currently working at Harbin University of Science and Technology, China.

Liang Yi, born in 1985, is currently studying at Harbin University of Science and Technology, China.