IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Review of Computer Engineering Studies
Vol. 6, No. 1, March, 2019, pp. 23-27
Journal homepage: http://iieta.org/Journals/RCES

Study of Two Kinds of Analysis Methods of Intrusion Tolerance System State Transition Model

Zhiyong Luo*, Xu Yang, Guanglu Sun, Zhiqiang Xie

School of Computer Science and Technology, Harbin University of Science and Technology, Harbin 150080, China

Corresponding Author Email: luozhiyongemail@sina.com

https://doi.org/10.18280/rces.060105

Received: 11 January 2019
Accepted: 20 February 2019

Keywords:
intrusion tolerance, state transition, finite automata, semi-markov process

ABSTRACT

The existing network security technologies cannot prevent all of intrusion, so the purpose of this study is to ensure that the system can continue to operate normally after the invasion. On the basis of existing intrusion tolerance model, increased to learning Status, the optimal state transition model of the invasion-tolerant system is proposed and analyzed respectively with the theory of finite automata and markov theory, further establish intrusion tolerance system. The experimental results show that increasing the learning state can enhance the tolerance of the system and ensure the stable operation of the system. The significance of this study is to provide a new idea for intrusion tolerance technologies.

1. INTRODUCTION

Traditional security work can be summarized into two aspects: prevent the occurrence of attacks and constantly solve the security vulnerabilities existing in the system [1]. However, with the continuous development of network technology, network attacks tend to be more diverse and complex, there are many unpredictable forms of attacks, and it is impossible to completely eliminate the existence of new security vulnerabilities [2]. Therefore, the third generation network security technology with intrusion tolerance technology as the core was born. Tolerance technology to admit the existence of system vulnerabilities, and assume that with the development of the time, some of the vulnerabilities may be an intruder using, its design goal is to make the system in the case of errors or invasion, still can guarantee the key function to continue, key systems continue to provide services (may be demoted mode)[3]. As this method not only considers the protection of system availability, but also considers the protection of security attributes such as confidentiality and integrity of system data and services, it can achieve the purpose of preventing the attack from coming, so it is called the last line of defense in system security protection [4].

Literature [5] by using the hidden markov model method of time series, portrays the safety situation of the different time, the parameters of the optimization model, in order to increase the accuracy of the model parameters and objectivity, and use the forward algorithm and backward algorithm with the combination of methods to identify the probability of a single state, finally using victor than algorithm to predict the change trend of the security situation, provide reasonable data for network managers to improve the work efficiency and effectiveness. Literature [6] perceiving and obtaining security-related metadata from time and space dimensions through technical means, dynamically reflecting network security status and predicting its future development trend through data information fusion analysis, and finally providing reliable decision support for enhancing network security. Literature [7] proposed a quantitative method to evaluate the effectiveness of security control of distributed power supply systems based on the concept of intrusion tolerance. The average compromise time (MTTC) model is used to estimate the abstract variables, and the model is modified according to the proposed evaluation method. In addition, into-csi can quantitatively evaluate network security control and enable security designers to achieve the efficiency level of a specific target system.

Based on the structure of SITAR intrusion tolerance system, this paper increases the attack learning state and puts forward an optimized state transition model of intrusion tolerance system. Since the state transition diagram is an important part of the automata theory, the intrusion tolerant system can be abstracted into automata and analyzed with the automata theory. Because the transition between states of the system satisfies markov property, markov theory can be used to analyze the invasion tolerant system. Based on the above two methods, this paper comprehensively analyzes the intrusion tolerance system and provides theoretical guidance for constructing a reliable, feasible, confidential and complete intrusion tolerance system.

This paper mainly discusses the intrusion tolerance model from four aspects. Firstly, the state transition model of the intrusion tolerance system is introduced; Secondly, the intrusion system is analyzed with the finite automaton; Thirdly, the system is markov; And finally the parameter analysis results are introduced.

2. AN OPTIMIZED STATE TRANSITION MODEL FOR A TRANSMISSION-TOLERANT SYSTEM

Due to the invasion system can protect the object is diversity, so each let invasion system adopted by the system framework, strategy, security algorithm are different, in order to facilitate abstractly describes the dynamic behavior of the intrusion tolerance system, this paper on the basis of SITAR intrusion tolerance system structure, increase the attack learning State (Learn State), optimization of State transition model is put

forward, the model is shown in Figure 1.

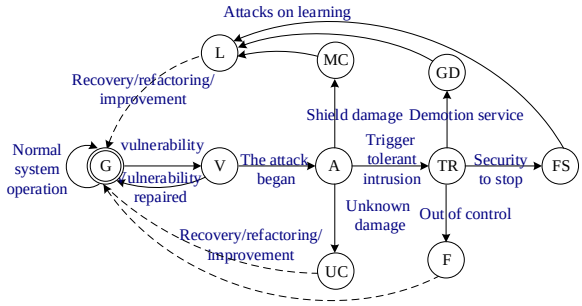

Figure 1. State transition model of intrusion tolerance system

The state transition model describes the possible events, the state and the processing mode of a generalized invasion-tolerant system in resisting intrusion through the influence of various attacks on the system services. The basic state of the state transition model including normal G (Good), fragile state of V (Vulnerable), was attacked status (Active attack), A shield damage state of MC (Masked Compromised) and unknown damage state of UC (Undetected Compromised), TR (Triage) state trigger, degraded service states GD (Graceful Degradation), safety state stopped the FS (Fail Secure), Failed state F(Failed) and intrusion learning state L(Learn). When the system is in the shielding damage state, degraded service state and security stop state, the learning function of intrusion learning state can be used to identify the type of attack and store it, thus laying a foundation for quick response measures in case of attack again. When the system is in an abnormal state, sometimes it can be automatically restored to the state of G, and sometimes it needs to be manually restored.

This state transition model can be used to handle any unknown attack that has a similar impact on the services provided by the system as the known state. Therefore, the model can deal with unknown forms of attack. The system is divided into several state levels, and each state can adopt corresponding security policies to ensure the normal operation of the system, so the model has certain flexibility and security.

3. FINITE AUTOMATON ANALYSIS OF A TRANSMISSION-TOLERANT SYSTEM

Finite automaton [8] is a kind of automaton with limited control state and limited symbol set, which is divided into deterministic finite automaton (DFSA) and nondeterministic finite automaton (NDFSA).

As shown in figure 1, with the operation of the intrusion tolerance system, the system transitions from one state to another, which may be normal state or abnormal state. Different system states represent different meanings. At a certain moment, there is a certain state corresponding to the system. No matter how the system operates, it will eventually be in the termination state. Therefore, the state of the system is finite. Moreover, because of the characteristics of the non-deterministic finite automata, the next state cannot be uniquely determined in the case of a given state and symbol. Therefore, this paper USES the theory of nondeterministic finite automata to study the formal description method of the invasion tolerance system.

3.1 NDFSA for the invasion-tolerant system

A nondeterministic finite automaton NDFSA is a five-tuple NDFSA= (Q, sigma, t, q_0, F) [9], where:

Q is a non-empty finite set of states, and each of its elements becomes a state;

$\sum$ is a nonempty finite input alphabet whose elements each become an input character;

Map t is a subset of Q×$\sum$→Q, that t is a multivalued mapping;

$q_0 \subseteq Q$ is a non-empty initial state set;

$F \subseteq Q$ is the termination state set and can be null.

If the automaton is in state q, and input character a, the system will be transferred to state q', then $t(q,a) = q'$.

The working state of a nondeterministic finite automaton can be represented by a state transition table and a transition diagram. Suppose there are M system state nodes and n transition conditions, then this state transition diagram contains M state transition nodes, the maximum value of each node is n, each arc is marked by an input condition, and each state transition diagram contains a unique system initial node and several system termination nodes.

According to figure 1, the model of the transmission-tolerant system can be abstracted as the non-deterministic finite automaton M=(Q, $\sum$, t, q_0, F), Among them Q={G, V, A, MC, UC, TR, GD, FS, L, F}; $\sum$={0， 1， ε}, 1 and 0 respectively represent the success and failure of the security policy of the invaded tolerant system, and ε represents the null shift; q_0={G}; F={G}.

Map t：Q×$\sum$→Q is:

t(G, 0) =V, t(G,1)=G;
t(V, 0) =A, t(V,1)=G;
t(A, 0) =UC, t(A,1)=MC, t(A, ε)=TR;
t(MC, 0) =A, t(MC,1)=L;
t(UC, 0) =UC, t(UC,1)=G;
t(TR, 0) =F, t(TR,1)=[GD,FS];
t(GD, 0) =GD, t(GD,1)=L;
t(FS, 0) =FS, t(FS,1)=L;
t(L, 1) =G;
t(F, 0) =F, t(F, 1)=G.

The state transition table of the non-deterministic finite automaton for the model of the invasion tolerant system is shown in table 1.

Table 1. State transition table of nondeterministic finite automaton for a transmission-tolerant system

State \ Symbol	0	1	ε
G	V	G	
V	A	G	
A	UC	MC	TR
MC	A	L	
UC	UC	G	
TR	F	[GD, FS]	
GD	GD	L	
FS	FS	L	
L		G	
F	F	G	

The state transition diagram of the non-deterministic finite automaton for the model of the invasion tolerant system is shown in Figure 2.

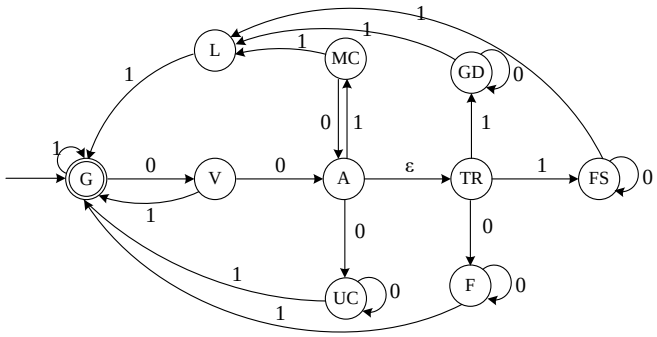

Figure 2. State transition diagram of a nondeterministic finite automaton for a transmission-tolerant system

In figure 2, a framework reflecting the dynamic behavior of intrusion tolerance systems is depicted. The system adopts various policies to support and maintain different levels of security requirements, and the state transition mode represents the corresponding measures of the attack behavior and the actual security requirements of the system.

3.2 The working process of the finite automaton in the system of tolerance for invasion

The system is in a normal state at the initial operation. Due to its inherent weakness, the system is easy to enter the vulnerable state V. At this time, the attacker has not caused damage to the application and service. If the vulnerable point can be repaired in time, the system will be restored to the state G. If the attack bypasses the protection measures and the system enters the attacked state A, in which some parts or functions of the application server have been damaged, the damage may be static, one-time or dynamic and continuous. If the intrusion is not detected, but some fault-tolerant measures have been prepared in the system design, the damage can be controlled and eliminated. If the intrusion is not detected and no measures are taken to control and eliminate it, then the system enters into the unknown damage state UC. After the attack is detected, the intrusion tolerance mechanism is triggered and the system enters the triggered state TR. In this state, the system can enter the degraded service state GD or the security stop state FS as required. If the invasion tolerance mechanism Failed, and the system went into the out-of-control state F(Failed), an alarm should be given immediately and the system should be manually restored by the administrator. When the system returns to G state from MC, GD and FS state, L state can learn and feed back the attack suffered, so as to enhance the system function and prepare for future attack.

4. SEMI-MARKOV PROCESS ANALYSIS OF A TRANSMISSION-TOLERANT SYSTEM

From the state transition model of the system, it can be seen that the transition between the states of the system satisfies the markov property: when the state of the process at time is known, then the condition distribution of the state at time is independent of the state of the process before time. In this paper, it is assumed that the residence time of the state is randomly distributed, and the state transition point satisfies the memory-free property. Therefore, the semi-markov process (SMP) can be used to describe the state transition model of the invasion-tolerant system.

4.1 System state transition model DTMC

Discrete time Markov Chain (DTMC) is a Markov process with Discrete time values, and state space is also a Discrete set. The one-step transition probability between all states constitutes a state transition matrix, and DTMC can be completely determined by this matrix. In order to analyze the SMP model of the system, the state transition model of the system was further abstracted, and the embedded discrete time markov chain (DTMC) was obtained.

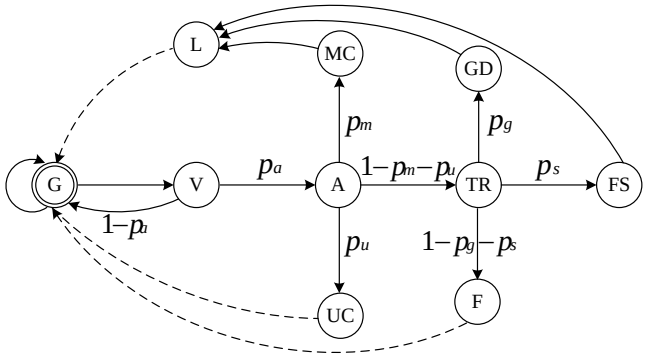

Figure 3. The system state transition model is embedded in markov chain

The transition probability matrix P in Figure 3 describes the possibility of system transition between states, where the probability value can be determined by empirical knowledge or determined by intrusion injection. The system state transition model DTMC transition probability matrix P is:

$$P = \begin{array}{c} \\ G \\ V \\ A \\ MC \\ UC \\ TR \\ GD \\ FS \\ L \\ F \end{array} \begin{array}{c} \begin{array}{cccccccccc} G & V & A & MC & UC & TR & GD & FS & L & F \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ p_1 & 0 & p_a & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & p_m & p_u & p_2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & p_g & p_s & 0 & p_3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

where, $p_1 = 1 - p_a$, $p_2 = 1 - p_m - p_u$, $p_3 = 1 - p_g - p_s$.

4.2 SMP steady state probability

The steady-state probability refers to the distribution probability of each state of the system under the stable working state. π_i represents the probability that the system SMP is in steady state, then $\sum \pi_i = 1, i \epsilon X_s$; v_i is used to represent the steady-state probability of the state in DTMC, then $\bar{v} = [v_G, v_V, v_A, v_{MC}, v_{UC}, v_{TR}, v_{GD}, v_{FS}, v_L, v_F,]$; h_i is the average holding time of state i; P is DTMC state transition probability matrix. The calculation method of π_i is shown in formula (1), v_i satisfies equation (2).

$$\pi_i = \frac{v_i h_i}{\sum_j v_j h_j}, i, j \in X_s \tag{1}$$

$$\begin{cases} \bar{v} = \bar{v}P \\ \sum_i v_i = 1, i \in X_s \end{cases} \quad (2)$$

The average duration of state is determined by all random times of the model in this state, and these times are determined by the attacker's ability, technical level and technical means adopted by the system, etc. Therefore, mean state holding time is adopted to simplify the analysis of the model. Let$\{h_G, h_V, h_A, h_{MC}, h_{UC}, h_{TR}, h_{GD}, h_{FS}, h_L, h_F, \}$ be the average holding time of each state, and the parameter H is introduced. According to equations (1) and (2), the steady-state probability of each state is calculated as follows:

$$\pi_G = h_G/H$$
$$\pi_v = h_v/H$$
$$\pi_A = p_a h_A/H$$
$$\pi_{MC} = p_a p_m h_{MC}/H$$
$$\pi_{UC} = p_a p_u h_{UC}/H$$
$$\pi_{TR} = p_a(1-p_m-p_u)h_{TR}/H$$
$$\pi_{GD} = p_a p_g(1-p_m-p_u)h_{GD}/H$$
$$\pi_{FS} = p_a p_s(1-p_m-p_u)h_{FS}/H$$
$$\pi_L = p_a[p_m+(p_g+p_s)](1-p_m-p_u)h_L/H$$
$$\pi_F = p_a(1-p_m-p_u)(1-p_g-p_s)h_F/H$$
$$\mathrm{H} = h_G + h_V + p_a[h_A + p_m h_{MC} + p_u h_{UC} + p_m h_L + (1 - p_m - p_u)(h_{TR} + p_g h_{GD} + p_s h_{FS} + (p_g + p_s)h_L + (1-p_g-p_s)h_F]$$

5. NUMERICAL ANALYSIS RESULTS

Since the actual values of model parameters need to be obtained through experimental observation and analysis, the estimated parameter values are adopted. The parameter values used are as follows:

5.1 System state transition probability

Assuming that the weakness existing in the system is detected, the system enters into state V from state G, and the intruder attacks successfully with this weakness, and the probability of the system entering into state A from state V is p_a=0.4; If the weakness of the system is repaired, the probability of the system from state V to normal state G is 1-p_a=0.6; When the system is attacked by the intruder, the probability of successfully shielding the attack is p_m=0.3; The probability that the system finds no attack is p_u=0.2; The probability of an attack being detected and triggering the intrusion tolerance mechanism is 1-p_m-p_u=0.5; The probability that the system enters state GD and state FS by state TR is p_g=0.6 and p_s=0.3 respectively; The probability that the system cannot handle the attack and therefore the alarm stops is 1-p_g-p_s=0.1.

5.2 Average system state holding time

Experience shows that the system works in state G for a relatively long time. So let's assume that h_G=1, h_V=1/3; When the system discovered the intrusion, it was transferred to state MC, state UC and state TR respectively. State MC was transferred to state G through learning, and state UC system needed manual intervention to be transferred to state G, make h_A=0.5, h_{MC}=0.5, h_{UC}=1, h_L=0.4; The state TR determines the direction of the system transfer according to the intrusion tolerance policy, then make h_{TR}=1/6, h_{GD}=3, h_{FS}=1, h_F=2. It should be noted that all variables of h_i(i=G, V, A, MC, UC, L, TR, GD, FS, F) are units of time.

5.3 SMP steady-state probability of the system

According to the state transition probability and average holding time of the system, the SMP steady-state probability of the system can be obtained, as shown in table 2.

Table 2. SMP steady state probability

Steady state probability π_i	Probability value	Steady state probability π_i	Probability value
πG	0.4373	πV	0.1458
πA	0.0875	πMC	0.0262
πUC	0.0350	πTR	0.0146
πGD	0.1574	πFS	0.0262
πL	0.0525	πF	0.0175

6. CONCLUSION

In this paper, an optimized state transition model of a transmission-tolerant system is put forward, which is preliminarily analyzed with automata theory and markov theory respectively, and the conditions and process of the transition between each state of a transmission-tolerant system are simulated, which provides a theoretical basis for the further construction of a transmission-tolerant system. Finally, the state transition model is simulated by numerical analysis.

ACKNOWLEDGMENTS

This work was supported in part by the Heilongjiang Province Foundation for Returnees (No.LC2018030), the National Natural Science Foundation of China (No.61772160).

REFERENCES

[1] Luo ZY, You B, Liu JH, Su J. (2016). Research of the Intrusion Tolerance State Transition System Based on Semi-Markov. Transactions of Beijing Institute of Technology 36(07): 712-717. https://doi.org/10.15918/j.tbit1001-0645.2016.07.010

[2] Wei K, Zhang F. (2016). Based on Markov Network Tolerate Invasion Ability Evaluation Model. Computer Simulation 33(07): 289-292. https://doi.org/10.3969/j.issn.1006-9348.2016.07.062

[3] Geng SX. (2018). Approach to Forecasting Multi-step Attack Based on Hidden Markov Model. Hebei normal Unversity.

[4] Gifty R, Bharathi R, Krishnakumar P. (2018). Privacy and security of big data in cyber physical systems using Weibull distribution-based intrusion detection. Neural Computing and Applications. https://doi.org/10.1007/s00521-018-3635-6

[5] Zhang Q. (2019). Research on network security situation prediction based on hidden markov model. Network Security Technology & Application 2019(03): 30-31.

[6] Yu Y. (2017). Research on network security situational awareness system. Computer knowledge and technology 13(34): 12-15, 23.

[7] Lee C, Yim HB, Seong PH. (2018). Development of a quantitative method for evaluating the efficacy of cyber security controls in NPPs based on intrusion tolerant concept. Annals of Nuclear Energy 112: 646-654. https://doi.org/10.1016/j.anucene.2017.11.002

[8] Gong YY, Liu QR, Yang ZX, Shao XY, Xing CQ, Jiao HJ, Peng ZB. (2015). Improved DFA algorithm based on multi-dimensional finite automata. Journal on Communications 36(05): 178-190. https://doi.org/10.11959/j.issn.1000-436x.2015101

[9] Fang BW, Huang ZQ, Li Y, Wang Y. (2018). Runtime Safety Verification of Stochastic System with Hidden Markov Model. Advanced engineering sciences 50(06): 198-204.