A Novel Network Survivability Analysis and Evaluation Model

Wang Chunlei
Department of Computer Science and Technology
Tsinghua University
Beijing, China
wcl08@mails.tsinghua.edu.cn

Miao Qing
Nation Key Laboratory of Science and Technology on Information System Security
Beijing, China
miaofj@163.com

Fang Lan
Nation Key Laboratory of Science and Technology on Information System Security
Beijing, China
Flan721@yahoo. cn

Wang Dongxia
Nation Key Laboratory of Science and Technology on Information System Security
Beijing, China
dongxiawang@126.com

Ming liang
Nation Key Laboratory of Science and Technology on Information System Security
Beijing, China
Mingliang78@yahoo.com.cn

Dai Yiqi
Department of Computer Science and Technology
Tsinghua University
Beijing, China
dyq@theory.cs.tsinghua.edu.cn

***Abstract*—Network survivability has the characteristics of complexity, dynamic evolution and uncertainty, which has become one of the most important factors for analyzing and evaluating network performance. Network survivability analysis and evaluation is a process of analyzing and quantifying the degree to which network system can survive in network threats. This paper proposes a novel network survivability analysis and evaluation model.Firstly, network survivability is abstracted as a dynamic game process among network attacker, network defender and normal user, thereafter network survivability evolutionary game model is established and network survivability analysis algorithm is proposed based on the game model. Secondly, the survivability characteristics of the network can be measured and evaluated based on the analyzed information based on the proposed immune evolutionary algorithm for network survivability metric weight solving and network survivability evaluation method using multiple criteria decision making. Finally, the proposed network survivability analysis and evaluation model is experimented in a typical network environment and the correctness and effectiveness of the model is validated through experimental analysis.**

Keywords-network survivability; evolutionary game model; network threat analysis; survivability evaluation model; immune evolution; multiple criteria decision making

I. INTRODUCTION

With the rapid development of network technologies and wide popularization of network applications, network scale becomes more immense and network configuration becomes more complex, network security has become the emphasis of national security strategy. Network security technology research is developing from traditional intrusion defense, intrusion detection to intrusion tolerance, and moving toward the direction of supporting network survivability from network isolation and network assurance. And the objective of network survivability is to guarantee the accomplishment of critical tasks in a timely manner when network suffers from intentional attacks or accidental incidents and ultimately ensure the adequate information availability and service continuance.

Currently, there is no unified definition of survivability. From the point of view of software engineering, the definition of survivability is [1]: the degree which essential functions are still available even though some part of the system is down. The research team from CMU/SEI argues survivability is the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents [2]. Network survivability analysis and evaluation is in essence a process of confirming the degree which the survivability technologies and mechanisms can defend network threats. The survivability characteristics of network can be measured, analyzed and evaluated based on the model and extracted information.

The current research of network survivability includes the following three aspects: 1) Network survivability evaluation model based on the system structure [3][4][5]. The modeling of physical structure of network is the early modeling techniques for survivability analysis, for instance, the usage of graph theory to represent network topology, etc. This modeling method is static and problem specific, however it is difficult for modeling large-scale network systems and the analysis techniques of the model are also very complicated and hard to understand. 2) Network survivability evaluation model based on the system state [6][7][8]. These evaluation modeling methods generally define system states firstly, and then analyze system survivability based on varieties of system states. It generally uses finite state machines, markov chain etc. to describe the models. These methods are beneficial for the analysis of dynamic behaviors of the system, but they need the understanding of system implementation in detail. 3) Network survivability evaluation model based on the system service components [9][10][11][12]. These models focus on the service components provided by the information system, simplifying and modeling the system according to the related

Published by Atlantis Press, Paris, France.

system service components, which is usually described as a tree-like structure. These methods are more concerned about the service performance of the whole system which have a more widely usage perspective, however the conversion from the system services to the evaluation model is a difficult problem.

Network survivability has the characteristics of complexity, dynamic evolution and uncertainty, the goal of network survivability analysis and evaluation is to find the satisfactory solutions from the limited schemes in the given conditions and constraints. In this paper, we propose a network survivability analysis and evaluation model considering the dynamic evolution of network survivability, and validate the correctness and effectiveness of the proposed model through experimental analysis.

II. NETWORK SURVIVABILITY ANALYSIS AND EVALUATION MODEL

Network systems are generally in the process of dynamic and continuous variations, network nodes are interconnected for fulfilling information distribution and sharing. Network system usually suffers from various kinds of attack threats. In case one node in the network is successfully compromised, this threat can be propagated to other nodes connected with the compromised node, so as to make these affected nodes meeting similar security threats. Meanwhile, network threats themselves are generally dynamic and evolutionary, which continuously change their threat levels and produce different losses accordingly. Therefore, it is inadequate for analyzing the survivability of network nodes statically and individually when analyzing the holistic survivability of network. It requires that network survivability analysis process should be considered the dynamic evolution and propagation of network threat, so as to determine the influences about the network survivability. In this section, we define the relevant concepts and propose network threat evolution model based on network threat evolutionary behaviors and threat propagations.

A. Network Survivability Analysis Based on Evolutionary Game Theory

Game theory is a method of studying strategic decision making. Game theory is mainly used in economics, political science, and psychology, as well as logic and biology. Recently, game theory has gradually been used for network security analysis. For instance, Sallhammar et al. utilized game model to analyze attacker intentions [13], Shen Dan et al. established a markov game for cyber situational awareness [14]. The above mentioned research work regards information security problems as the dynamic game between attackers and defenders, and investigates information security problems from the interactions between attackers and defenders and the corresponding strategy enforcement. However, currently research work generally aims at certain security techniques or analyzing certain security metrics, it still lacks of systematic analysis and research about network survivability. In this paper, we abstract network survivability as the dynamic game process among network attackers, network defenders and network normal users considering the dynamic evolution of network survivability, and establish network survivability game model for each threat t in the set of network threats.

Definition 1 (Network Survivability Game Model, NSGM). Network Survivability Game Model can be represented as a 5-tuple, $NSGM = (N, S, H, p, U)$, which:

(1) $N = \{a, d, n\}$ refers to the set of game players, in which a refers to network attacker who usually behaves as network threat and compromises network object through threat propagation and dynamic evolution, d refers to defender who protects network object through mending network weakness exploited by threat or cut off the propagation paths of the threat, and n refers to neutral network user whose behaviors generally affected by network attackers and defenders.

(2) $S = \{s_1, s_2, \cdots, s_n\}$ refers to the state space consisting of all possible states of network threat evolution model $TEM(t)$, the state at time k represented as $s_k = \{n^i(k), e^j(k)\}$, $i = 1, 2, \cdots, M$ are M propagation nodes, $i = 1, 2, \cdots, N$ are N propagation paths, $n^i(k) = (id_i, value_i, \rho_i^k, t_{if}^k, w_{if}^k)$ refers to the state of i propagation node at time k, $e^j(k) = (id_{js}, id_{jd}, value_j, \rho_j^k, p_j^k)$ refers to the state of j propagation path at time k.

(3) $H = \{H_a, H_d, H_n\}$ refers to all possible behavior paths (i.e. strategy set) of game players, in which H_a refers to attacker behaviors which represented as threat t propagating to other parts of the network in certain probability according to $TEM(t)$, H_d refers to defender behaviors which implemented through performing network survivability scheme, such as mending weaknesses, cut off threat propagation paths etc., and H_n refers to neutral user behaviors generally representing as the changes of network access statistics.

(4) $p = \{p_1, p_2, \cdots, p_n\}$ refers to network state transition probabilities caused by game players selecting possible behaviors, $p_k = p(TEM(t, k+1) \mid TEM(t, k), h_a^k, h_d^k, h_n^k)$, refers to network state changes at time k, $TEM(t, k+1) \mid TEM(t, k)$ refers to network state at time $k+1$ and time k, and h_a^k, h_d^k, h_n^k refers to the behaviors of attackers, defenders and neutral users at time k, and each players select corresponding behaviors in certain probabilities.

(5) $U = \{u_a, u_d, u_n\}$ refers to the payoff functions of game players selecting strategies for calculating gains and losses of each game players, in which: u_a refers to the payoff function of attacker represented as network losses, since the goal of attacker is to compromise network in maximal degree; u_d refers to the payoff function of defender represented as the reduction of network losses due to network manager adopting network protection scheme, since the goal of defender is to alleviate network losses caused by network

Published by Atlantis Press, Paris, France.

attack in maximal degree; u_n refers to the payoff function of neutral user represented as the degree of normal network user utilizing network services, since the goal of neutral user is to make use of network resource in maximal degree.

Network survivability analysis is the iterative process of each player selecting behaviors from behavior space based on the current states of network, network transferring to new states, and each player making decisions according to the newly transferred states. For each threat t, three game players select respective strategies and obtain their payoffs. Each player maximizes its strategy selection based on the respective payoff function. Network state at time k is represented as $TEM(t,k)=\{n^i(k),e^j(k)\}$, in which $n^i(k)$ refers to the state of threat node i at time k, $e^j(k)$ refers to the state of threat path j at time k. Network state at time $k+1$ is represented as $TEM(t,k+1)$, and the transition probabilities of network states are determined by survivability game strategy selection.

Suppose game players select respective behaviors in the condition of game equilibrium, due to the characteristics of dynamic variations of network survivability and interactions of multiple factors. The above mentioned network survivability game process can be regarded as the three roles non-zero complete information static non-cooperative game approximately, the strategies of attackers, defenders and neutral users are not transparent among each player. One of the objective of network survivability game model calculation and analysis is to predict the probability vectors of each player and network state transition probability p.

Network survivability game process is described as following: Suppose network threat evolution model *TEM* is established for certain threat t in network threat set. The three game players are attackers, defenders and neutral users, the behaviors of attackers are represented as propagating threat t to un-infected nodes according to *TEM*, the behaviors of defenders are represented as preventing threat t through performing network survivability schemes, the behaviors of neutral users are represented as normal network users increasing or decreasing network access, and network states are represented as all possible states of *TEM*. Each game player dynamically selects its behavior according to network states and its payoff function, and network transfers to the next state in certain probability according to the effects of each player's behaviors.

(1) At time k, network survivability game is in the state $s_k \in S$, where threat t acts on network object O_1, and the attacker, defender, and neutral user select strategy h_a^k, h_d^k, and h_n^k from their strategy set respectively, therefore they gain payoffs $u_a^k = u_a(s_k,h_a^k,h_d^k,h_n^k)$, $u_d^k = u_d(s_k,h_a^k,h_d^k,h_n^k)$ and $u_n^k = u_n(s_k,h_a^k,h_d^k,h_n^k)$ accordingly.

(2) At time $k+1$, threat t propagates to network object O_2, where the defender performs protection strategy aiming at O_2, and neutral user selects corresponding strategy based on network state, therefore they gain payoffs respectively. Then network state transfers to s_{k+1}, which represents the success or failure of threat t propagating in the direction.

(3) Network continuously changes its states according to the above mentioned process. For network survivability game process with limited steps (i steps), the process of network state changes firms a tree style structure from time k to time $k+i$, and each path from root node to leaf node means a possible network state change process.

For a threat t in the set of threats that network suffers, the influence over network states produced by threat t propagation is analyzed, network survivability game model is constructed, and equilibrium strategy of network survivability game is calculated. Finally, the changes of various transient and steady survivability parameters are analyzed based on the game model.

B. Network Survivability Evaluation based on Immune Computation Theory

Forming metrics system and determining the metrics weight are the basis for network survivability evaluation. In the process of network survivability evaluation, as pointed out in previous section, network survivability is a concept of relativity concerned with an organization. Each organization has its own understandings and preferences for the network survivability attributes, such as the identification, defense, response and recovery of the network threats. There are also different choices in the determination of key nodes and risk factors etc. Therefore accurately computing the metrics weight is an important problem to be solved. At present there have been many methods of determining weight, such as expert evaluation, analytic hierarchy process, entropy weight etc. These methods depend heavily on the knowledge and skills of the experts and have definite limitations such as high accuracy of the data acquisition etc., which couldn't adapt to the complex and dynamic characteristics of the large-scale network.

Network survivability evaluation is as complex problem which involves various aspects such as technologies, organizations, and external environments etc. For the reasons such as incomplete understanding, ambiguity of experience and intuition, it only gives a fuzzy range to the judgment of problem and the determination of evaluation data, thus indicates as an interval number. Therefore, in network survivability evaluation, determine metrics weight with interval numbers is more in line with the actual quantitative judgment. In this section, we use interval number structure expert judgment matrix, making it more suitable for the expression of the uncertainty of reality and the ambiguity of expert experience. And by using immune evolutionary optimization mechanism, we propose the algorithms to compute weight vector of the interval number judgment matrix.

With the immune memory mechanism, immune evolution can construct the immune operator and form the immune vaccine and optimization strategy through the effective usage of apriority knowledge. It keeps elite individuals and discards bad individuals and at the same time maintenances the diversity of individuals, effectively

Published by Atlantis Press, Paris, France.

overcomes early maturity and degradation in global search process, and improves the convergence of search process [15]. For the reference of immune evolutionary, an intelligent optimization method for solving the weight vectors of interval number judgment matrix are proposed, with the global convergence ability of the immune system, it can calculate interval numbers of the weight vectors efficiently [16].

In immune system, antibodies realize the detection of antigen and help immune cells eliminate antigen. Once the antigens are detected, the cloning amplification is happened and produces large amount of antibodies. Then the antibodies will experience high frequency mutations. After the antigens are eliminated, the antibodies which with the lower affinity to antigen will be eliminated from the dynamic augmentation antibody library, and then the stability of antibody population will be achieved. At the same time, through the immune memory mechanism, advantage antibodies will be retained and obtain the quick response ability when experience the immune response again. In the optimization problem of solving the weight vectors, the objective function is antigen, and the judgment matrix with random certainty is antibody. Through the various immune operators to generate and keep the antibody and immune memory, antigen will be discovered, thereby quickly solve the weight vectors of interval number judgment matrix. Some of the concepts and operators involved in the algorithm which proposed by this paper to solve the weight vectors of interval number judgment matrix are described below：

(1) Antibody encoding method: The encoding method of the antibody is matrix and is consistent with the judgment matrix in the form, namely, with the same dimension. The encoding of the matrix component is real number, and each value is ascertained with the interval number. The antibody encoding method can completely traverse the matrix space which is determined with the interval number judgment matrix.

(2) Affinity function: Using the target function as affinity function, and the satisfied consistency condition as eliminate operator to realize the elimination of antibody.

(3) Clonal expansion: Choosing advantage antibodies from antibody population according to the fitness of antibody (choose proportion is m_{select}), through many times (clonal coefficient is m_{clone}) single point arithmetic crossover two-two antibodies produce the offspring antibodies. Arithmetic crossover, means two real number a and b cross produce c through the following formula $c: c = m_c a + (1 - m_c) b$, in which $0 \le m_c \le 1$ is randomly generated arithmetic crossover parameters.

(4) High frequency of mutations: Realizing the single point high frequency mutations to the antibodies produced by clonal expansion in the antibody library (mutation probability is m_{hm}). For the real number encoding elements, upper limit U and lower limit L are variables produced through the following formula, $c: c = L + m_{hm}(U - L)$.

(5) Negative selection: Achieving the stability of antibody population through discard antibodies with lower affinity for the antibody library after clonal expansion.

(6) Immune memory: Immune memory is in essence a kind of elite strategy to save the advantage antibodies.

(7) Algorithm stop: Stop searching when algorithm meets stop conditions, that is, the evolutional generation (m_{gen}) reach the maximum value.

Algorithm 1. Immune evolutionary algorithm for solving the metrics weight of network survivability

1. Initialize interval number judgment matrix and algorithm parameters;

2. Initialize antibody population (Population scale is m_{pop});

3. Choose advantage antibody for clone amplification;

4. Make high frequency mutations to clone amplified antibody population;

5. Discard the antibodies with lower affinity and maintain the stability of antibody population through negative selection;

6. Save the advantage antibodies through the immune memory mechanism;

7. Stop the algorithm when meet the stop condition, and output the advantage antibodies as antigens; Otherwise turn to step 3, repeat the step 3-step 7.

III. EXPERIMENTAL ANALYSIS

We choose a small network environment with three kinds of survivability policies, and measure the values of survivability metrics under the same network attack. The test scene is shown in Table 1.

TABLE I. THE TEST SCENE IN NETWORK ENVIRONMENT

Scene	Target aspect				Attack aspect	Survivability policies
	Node number	*Link degree*	*Routes*	*Services*		
e	100	20	20000 pieces of BGP routes	50 Web services	a worm virus attacking network connection	“Backup” strategy “Round” strategy “Repair” strategy

Test scene with its configuration is shown in Table 1, which includes target aspect, attack aspect, and survivability policies. Three kinds of survivability policies are “Backup” strategy (solution 1), i.e. to use backup connection as soon as the link is broken, the “Round” strategy (solution 2), i.e. to round the broken link by other way, and the “Repair”

strategy (solution 3), i.e. to repair the connection as soon as the link is broken. Three policies all include recognition and killing off the worm virus.

We consider eleven metrics, including 4 availability metrics, 3 controllability metrics, 2 robustness metrics, and 2 adaptability metrics. Availability metrics are Service Response Time (SRT), Network Link Degree (NLD), Throughout (THT), and Delay (DLY); controllability metrics are Threat Sensing Time (TST), Fault Trace Time (FTT), and Source Isolated Degree (SID); robustness metrics are Service Redundancy Degree (SRD) and Network Collection Degree (NCD); adaptability metrics are Service Construction Time (SCT) and Topology Reconstruction Time (TRT). In the experiment, we firstly construct network survivability game model, and then utilize the model to analyze the above listed survivability metrics based on the measured performance data. For instance, the change of SRT parameter value is depicted as Fig. 1.

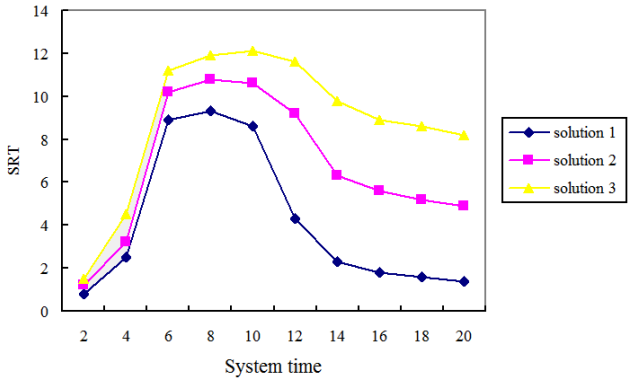

Figure 1. The values of SRT demonstrating the changes of network survivability.

From Fig.1, it shows that the survivability of solution 1 is the best in the optional solution set. Effectiveness of the proposed analysis model and approach is validated through the experiment.

IV. CONCLUSION

Network survivability analysis and evaluation process is very complex in confirming the degree which the network survivability technology and mechanism can defend network threats, considering the characteristics of network dynamic evolution and behavior uncertainty. In this paper, we propose a novel network survivability analysis and evaluation model based on evolutionary game theory and design the immune evolutionary algorithm for network survivability evaluation. Our future research will be focused on optimizing the proposed network survivability analysis and evaluation model for adapting complex network environment, investigating the testing methods of various network survivability metrics, and carrying out extensive experimental analysis to validate the effectiveness of the model.

REFERENCES

[1] John C. Knight, Kevin J. Sullivan. On the Definition of Survivability. University of Virginia, Department of Computer Science, Technical Report CS-TR-33-00.

[2] Fisher J, Linger R. Survivability:protecting your critical systems[J]. IEEE Journal of Internet Compu¬ting, 1999, 3(6):55~63.

[3] Louca Soulla, Pitsillides Andreas, Samaras George. On Network Survivability Algorithms Based on Trellis Graph Transformations[C]. The Fourth IEEE Symposium on Computers and Communica¬tions(ISCC'99), Red Sea, Egypt,1999:235-243

[4] Krings Axel W, Azadmanesh M H. A Graph Based Model for Survivability Analysis[R]. Technical Report UI-CS-TR-02-024, Computer Science Department, University of Idaho, 2002

[5] Zolfaghari Ali, Kaudel Fred J. Framework for Network Survivability Performance[J]. IEEE Journal on¬Seleeted Areas in Communications, 1994, 12(1):46-51.

[6] MeDemrott J. Attaek-Potential-Based Survivability Modeling for High-Consequence Systems[C]. Third IEEE International Workshop on Information Assurance(IWIA'05), College Park, Maryland, US, 2005:119-130.

[7] Dong Seong Kim, Khaja Mohammad Shazzad, Jong Sou Park. A Framework of Survivability Model for Wireless Sensor Network[C]. Proeeedings of the First International Conference on Availability, Reliability and Security, Washington DC, US, 2006:512-522.

[8] Jha Sanjay K, Wing Jeannette M, Linger Richard C, et al. Survivability Analysis of Network Specifica¬tions[C]. International Conference on Dependable Systems and Networks(DSN2000), New York, USA, 2000:613-622.

[9] Gao Zhixing, Ong Chen Hui, Tan Woon Kiong. Survivability Assessment: Modeling Dependencies in Information Systems[C]. The 4th IEEE/CMU/SEI Information Survivability Workshop(ISW-2001/2002), Va¬neouver, BC Canada, 2001: 515-522.

[10] Hevner Alan, Linger Riehard. The Flow-Service-Quality Framework: Unified Engineering for Large-scale, Adaptive Systems[C]. The 35th Hawaii International Conference on System Sciences, Hawaii, US, 2002: 4006-4015.

[11] R. Ellison, D. Fisher, R. Linger, H. Lipson, T. Longstaff, and N. Mead. Survivable network systems: An emerging discipline. Technical Report CMU/SEI-97-153, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA15213, November 1997.

[12] Lin Xue-gang, Zhu shen-liang, Xu Rong-sheng. Layered computation for information system survivability. Journal of Zhejiang University (Engineering Science), 2006, 40(11):1960-1965.

[13] Sallhammar K, Knapskog S J, Helvik B E. Using stochastic game theory to compute the expected behavior of attackers. In: Proc. Of the 2005 Symp. on Applications and the Internet Workshops. 2005.

[14] Shen D, Chen G, Cruz J B, Haynes J L, Kruger M, Blasch E. A Markov game theoretic approach for cyber situational awareness. In: Dasarathy BV, ed. Proc. of the Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications, Vol. 6571, 65710F. 2007.

[15] Ding Yong-sheng. A new scheme for computational intelligence:bio-network architecture, CAAI Transactions on Intelligent Systems. 2007, 2(2):26-30.

[16] Ding Yong-sheng. Design of a bio-network architecture based on immune emergent computation. Control and Decision , 2003 , 18(2):155-159.

Published by Atlantis Press, Paris, France.