Research of Network System Reconfigurable Model Based on the Finite State Automation

Shenghan Zhou and Wenbing Chang
School of Reliability and System Engineering, Beihang University, Beijing, China
Email: Changwenbing@263.net

Abstract—Since the network analysis model based on the system state exists the issues of network survivability safety, fault tolerance and dynamic ability are adapted to the environment changes, in this paper, network system model based on the finite state automation has reconfigurable quality. The model first puts forward the concept of reconfigurable network systems and reveals its robustness, evolution and the basic attributes of survivability. By establishing a hierarchical model of system state, the system robust behavior, evolution behavior and survival behavior are described. Secondly, network topology reconfigurable measurement as an example, puts forward the quantitative reconfigurable metrics. At last, the example verification. Experiments show that the proposed reconfigurable quantitative indicators of reconfigurable resistance model for [1.391, 1.140, 1.591] prove that the network is an efficient reconfigurable network topology, which can effectively adapt the dynamic changes in the environment.

Index Terms—Information Network; Robustness Indicators; Evolution Indicators; Measurement

I. INTRODUCTION

Information network in the political, economic and social life plays an irreplaceable role, however, in the process of network operation often threatened by fault and unpredictable emergencies, typical floods, fires, earthquakes, tsunamis and other natural disasters, terrorist attack, the hacker attack, computer malicious code, operator error or destruction and such abnormal events caused by human factors, will give people's production and life bring great influence and loss [1]. On the other hand, as the network scale expanding, network structure is increasingly complex, the rapid development of network technology, and the current new application, new demand changing, all need network system can adapt and respond to environmental change. Therefore, the construction of high reliability and can be self-healing network infrastructure, build a strain of reconfigurable network system, is becoming the focus of attention [2-5].

The core of the challenge faced by Reconfigurable networks is mainly the "change" (change or evolution) (especially unpredictable emergencies), in particular is required to construct the network system of reconfigurable resistance, can be efficient allocation of resources available for quick response and adapt to the change [6]. Reconfigurable network system's building, need to study the sensing, execution, communication,

control, calculated from the device in the system level to system level of structure and dynamic characteristic, refactoring to issue involves wide level, is complex, and related research is rarely. At home and abroad, has been carried out for reconfigurable system research includes hardware based on chip technology of reconfigurable computing, in response to the reconfigurable manufacturing of market demand changes, oriented programmable wireless communication technology and software engineering of reconfigurable software design, etc. [7-12].

Although these studies in single aspects, such as computing and communications, for the whole reconstruction of the network system provide enabling technology, but has not formed a complete system, the basic theory of reconfigurable quality and the key problem is not clear and consistent description, also lack of system modeling and analysis of reconfigurable [13-15].

Analysis of the modeling of reconfigurable is important to the study of network system of reconfigurable management, and design and build the basis and premise of reconfigurable network system). At first, this paper puts forward the concept of reconfigurable network systems and basic properties. In the system state based hierarchical structure, in view of the reconfigurable has robustness, evolution and survival of the attribute to rich, the model is put forward based on the finite state automata (FSM) reconfigurable analysis model. Then the measure of the network topology reconstruction can be quantitative analyzed. Finally summarizes the full text and research system of the reconfigurable network.

This paper mainly carries out the development and innovative work in the following aspects:

(a) Based on the system state in the analysis model of network security, network fault tolerance and survivability dynamic ability to adapt to the environment changes is not strong, in this paper, based on the finite state automata network system model of reconfigurable. The model first puts forward the concept of reconfigurable network systems, reveals its robustness, evolution and the basic attributes of survivability. By establishing a hierarchical model of system state, and then describe the system robust behavior, evolution behavior and survival behavior. Secondly, network topology reconfigurable measurement as an example,

puts forward the quantitative metrics of reconfigurable, evaluation is considered to be a measure of the reconfigurable respectively by robust d, evolutionary survival and product structure measurement of three-dimensional space. Metric values of reconfigurable corresponding to 3 d vector of the three dimensional space, the robustness, evolution and survivability index indicators.

(b) In order to further validation in this paper, based on the finite state automata, the correctness and validity of network system reconfigurable model, for example, uses the ARPA network topology, based on the evolution of ARPA network robustness, and quantitative analysis of survivability index, the ARPA network of 3 d reconstruction can be quantitative indicators for [1.391, 1.140, 1.591], shows that ARPA network is an efficient reconfigurable network topology. Experiments show that: based on the finite state automata network system reconfigurable model can construct an efficient reconfigurable network topology, can effectively to adapt to the dynamic changes in the environment.

II. RECONFIGURABLE

Reconfigurable is not a new concept noun, but it had already appeared in the field of manufacturing systems and information systems. Although people put forward the concept of reconfigurable system already has a history, the international exploration of reconfigurable network has just begun, the understanding of the basic concepts and scientific issues is not deep. International reconfigurable representative is available at the moment of this paper: description of the reconfigurable system of the United States national aeronautics and space administration (NASA) refers to the function layer and physical layer has the adaptability, can automatic or remote control and efficient system of one or more goals. The system can not only handle the upfront design events or scenarios, but also deal with unknown uncertainty during the design phase scene; In the national science foundation (NSF) application plan mentioned in 07-561: reconfigurable refers to the abnormal situations in order to ensure the system to work normally, and change the system structure and operation ability to meet the demand of the system.

The autonomy reconfigurable of information infrastructure based on next generation, integrated equipment, network, software engineering and embedded reconfigurable system provided by the pervasive computing power.

Network system is reconstruction refers to the system can be flexible configuration available resources to adapt to environmental changes, ability to provide continuous and effective services. Reconfigurable network system is a comprehensive concept, should contain multiple attributes. To be specific: from the angle of system design, the need to provide Robustness (Robustness), make the system have certain resistance to failure and attack and tolerance; From the angle of system development requires evolution (Evolvability), make the system has the adaptability to the environment change and extensibility;

From the perspective of user requirements to guarantee the service availability and Survivability (Survivability), it is an important objective of system reconstruction. Different from the system robustness, evolution and survivability in the traditional sense dispersed, isolated concept and connotation of reconfigurable network system will be under the goal of adaptive environmental change integration of the three basic attributes to form an organic whole.

As shown in figure 1, the reconfigurable network system of failure or attack response process can be divided into information acquisition, data processing and response to realize three parts. Among them, the information acquisition stage according to the system demand active external network environment information, system status information and alarm information, effective recognition network fault, analyze the running status of network system to master the current available resources distribution in the network, when and where the system how to refactoring support for information. Available resources reasonable scheduling and allocation is used to drive and coordination needed refactoring response behavior. According to the behavior characteristics of reconstructing response can be divided into: robust behavior, evolution behavior and survival behavior.

Robust behavior is the early stages of system response, mainly refers to the system takes advantage of the redundancy devices configured, redundant link resources such as spontaneous resistance and tolerance failure or attack behavior of system; Evolution behavior is the advanced stage of system response, is mainly refers to according to the emergency needs, can implement large span network structure and resource reconfiguration; Survival behavior is necessary to reconfigurable system, can work according to the system state for adaptive adjustment and the capability of fault recovery, etc.
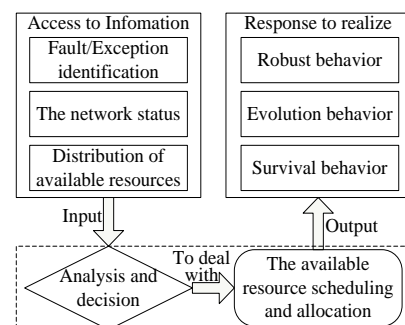

Figure 1.   Refractors process of the reconfigurable network

III. FSM RECONFIGURABLE MODEL

Based on the complexity, the openness and diversity of the network system, reconfigurable network system analysis and involved appropriate models focus on the modeling problem. Analysis method of the existing system characteristics, main boils down to set legal and state law.

Compared with the method of combination model, the model based on the state can express more complicated

relationship, such as random behavior, emergent behavior, etc. And compared with the general state of the system model, through the layered structure describes the state of the system model can effectively avoid the system state definitions and based on the analysis of state directly.

A. The Hierarchical Structure of the System State

Reconfigurable network system is determined by the system itself, not only is closely related with its surroundings. In this paper, starting from the relationship of system environment, through to the system input events (abnormal), examine the response of the system behavior (robust behavior and evolution behavior and living behavior, etc.), and then analyze the system of reconfigurable. In order to facilitate subsequent reconfigurable analysis, it is necessary to simplify the system properly, first used the following definitions and symbols:

Definition 1 the basic Service (Essential Service, *EsS*): system under abnormal environment still need to provide complete Service system is indispensable key function;

Definition 2 the Emergency services (Emergency Service, *EmS*): a system to meet the new requirements or special Service provided by the Emergency response. It is different from the conventional basic services, is the product of reconstructing system evolution.

Definition 3 basic components (Essential Component, *EC*): refers to the resource unit of system which plays a role of supporting service system, according to degree of dependence on the system service, every basic component is a importance weights v

In this article the system status is decided by the performance of the system service, the service is provided by the system according to user requirements definition, services that the system requires can be composed of a services set { S_i }. Based on Workflow (Workflow) technology, the path between the servers to request as a pipeline, the transport of which is required to provide the service, the service flow.

Identified the resources unit come across by the service flow S_i, form the basic component set { EC_{ij} } the services needed, the basic components formed the participants of service flow.

According to the environment of system operation and performance of the services they offer, assuming failure probability of basic components EC_{ij}:

$$R_{ij} = \min(\varpi.y_{ij} + t, 1.2) \qquad (1)$$

T represents the failure probability of the basic components without considering the importance weights of basic components, α represents the threat coefficient of attack with related basic component EC_{ij} importance weights y_{ij}.

When $\varpi = 0$ represents random attack without considering the component's importance. The greater the value of α is, the greater the chance of important component of its deliberate attacks in the network service

system. In order to damage the system serve effectiveness and safety, the invaders will adopt a series of steps, intelligence gathering, long-range attack, get permissions, set the back door, etc. Therefore, this article use scenarios to describe the correlation of series events).

Definition 4 event scene (Event Scenario, *E*): to achieve a certain goal influencing system services, and take a series of events. Specifically, the scene can be divided into exception events Scenario (Abnormal Event $S_{ce-nario}$, *AE*) harm the system service and the response of recovery, refactoring, down the system service Event scene ($R_{e-sponse}$ Event Scenario, *RE*).

Event scenario describes the interaction of the network environment and network system. Among them, the AE represents incentives of environment on the system, through the analysis of consumption or damage the system resources (basic components) will affect system performance; RE system response to environmental changes, mainly through robust behavior, evolution behavior and living behavior to restore basic services, refactoring emergency services and degraded living services, etc.

According to the definition above, the system state is determined by system service performance, service and system performance depends on the basic components of system. It need exception event scene by attacking system basic components influence the service performance of the system and respond improve system performance through reconfiguration of the basic components in the system.

In the analysis of the system state, through the establishment of the system status hierarchy description that can effectively avoid the general state of the system based on state of the model definition and time constraint conditions known system state distribution of state transition analysis.
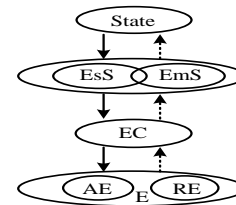

Figure 2. The hierarchical structure of the system state

Hierarchical structure of the system state as shown in figure 2, the analysis of the system state can press the arrow step by step, which will make direct state of the system definition and analysis of abnormal events situation, respond to events and their role in the definition of system analysis of the basic components, in turn, affects system performance.

B. The Analysis Process based on FSM

The following finite state automata (FSM) can be used to describe the basic network system (not refactoring network system):

$$T_0 = \left(R_0, \sum{}_0, \delta_0, k_0, K \right) \qquad (2)$$

where in, $R_0 = (R_0, R_1, ..., R_{M-1})$ represents that contains M state of the system state set, and the system state can be defined according to the operation condition of the system services:

$$\sum\nolimits_0 = (E_0, E_1, ..., E_{N-1}) \qquad (3)$$

Represent a set that contains N scenarios; δ_0 means state transfer functions, depending on the input event scene, by the state transition function $\delta_0 : R_0 \times \sum\nolimits_0 \to Q_0$ decided vicissitude from the current state of the system to the next system state; R_0 represents the initial status of the system, $R_0 \in R_0$; F represents stable state of the system, the system steady state can be any state in the R_0, so $F \in R_0$.
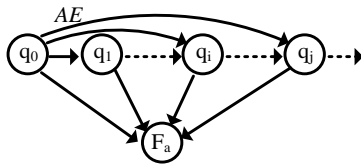

Figure 3.   Basic system state transition diagrams

Basic network system in case of any attack or failure, the relationship between the system state transitions is shown in figure 3. The system state arrange from left to right, from high to low, q_0 for the system normal working condition, $F_a \in F$ for system paralysis (failure). Abnormal events scene AE can be treated as incentives of the network system, the system state transfer as the response of a system, the characteristics of basic network system state transfer reflects when the system in case of any attack or failure, process of service performance gradually reduce until the system operation.

In fact, most of the network system through the redundant equipment and link, under the condition of the gateway and subnet failure, can also maintain the basic communication and services, has certain robustness. There are a lot of indexes to measure the network system robustness, including in the field of network security, the most concerned about is the system for the tolerance of random fault and deliberate attacks.

System robustness is described by using FSM as shown in figure 4 (a), the system state, q_{i-1}, q_i and q_j corresponding system service performance reduce in turn RE_{i-1} and RE_{j-1} to represent the response incident scene under the action of the system robustness, dotted line is shown in state transfer $q_i \times RE_{i-1} \to q_i$ and $q_i \times RE_{j-1} \to q_i$, describes the response process of the system fault tolerance, restore service.

Network system evolution refers to the system response to environmental changes and the capability of adaptive reconfiguration structure and resources. In the process of system evolution, can be extended to generate emergency services to meet the specific requirements of the environmental changes.

As shown in figure 4 (b), q_i' is generated the new state in the process of system evolution response, according to the emergency services definition provided by system evolution extension. State transfer $q_i \times RE_{j-1} \to q_i$ embodies the system through the role of the response to an event scene evolution stage production meet the demand of system especially the evolution behavior.

Network survivability is refers to the system when subjected to random failure or malicious attacks, can continue to provide service for users' "survival" ability, this is an important target of system reconstruction. Abnormal events in the scenario, system can still provide elegant relegation service, is the outstanding performance of the system can survive, using FSM description as shown in figure 4 (c). Fa' is a graceful degradation in system working condition, the basic service before complete failure is considered to be a system exists some failure state of the system. RE_d is degraded service condition and respond to events, turned to the Fa' state transition $q_i \times RE_{j-1} \to d \to Fa'$ and $q_i' \times RE_{j-1}' \to d \to Fa'$ embodies the survivability response behavior of system to provide the degraded service.

(a) State transition diagram under the action of robustness

(b) State transition diagram under the action of an evolutionary

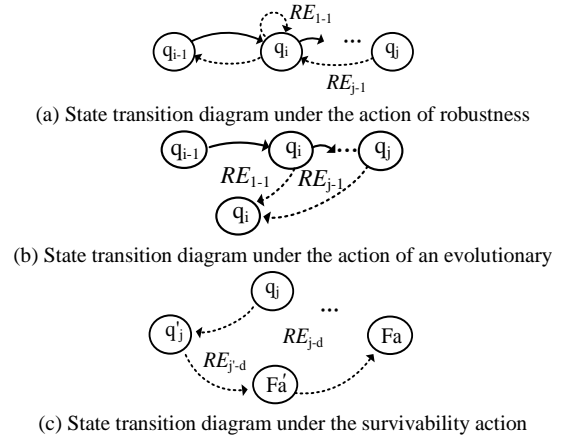(c) State transition diagram under the survivability action

Figure 4.   State transition diagram of different attribute system

C. The Reconfigurable Analysis Model based on FSM

Robustness, evolution and survivability is basic attribute of reconfigurable network system, which embodies the reconfigurable system robustness has some fault tolerance and resilience of primary reconfigurable quantity; Evolutionary embodies the reconfigurable system has expansibility and flexibility of advanced reconfigurable ability and survivability embodies the important target to reconstruct the network system. Integrate the reconfigurable network system model of robustness, evolution and survivability, it can be described as:

$$RM = (Q, \sum, \delta, q_0, F) \qquad (4)$$

The Q is the system state, and the system state decides according to the service performance of the system

provides, namely the service focus provided by the system contain which basic services and emergency services; $\sum = \left(AE_0 ..., AE_i ...; RE_0 ..., RE_i ... \right)$ Is a collection of abnormal situation and response events scene; Q_0 for the system normal working state; Fa' for graceful degradation of the system working status (partial failure); Fa' for system paralysis (complete failure). For event scene Σ, get by the state transition function $\delta : Q \times \sum \to Q$ and then, coming into next state.

State transition of reconfigurable system is shown in figure 5, the system state from high to low in turn arranged $\{ q_0, q_1', q_1 ..., q_i' ..., Fa', q_i ..., q_j ..., Fa \}$, $\{ q_1', q_i' \}$ is generated new state of grade system evolution response, Fa' is survival grade response the graceful degradation of working condition. Solid arrows shown in AE_i indicate the system under the action of abnormal events scene state transition; the loop line shown in RE_{i-1} reflects the system robustness under the action of the tolerance of the response of the situation of abnormal events, points line arrow shown in RE_{j-1}' shows the system robustness to system service recovery; short dotted arrow shown in RE_{i-1}' embodies the sexual response under the action of system evolution scenario generation evolution of emergency services; the status change shown in RE_{j-d}, it turn to Fa' reflected the survivability of the system.
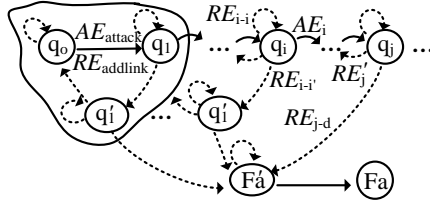

Figure 5.   State transition diagram of reconfigurable system

Compared with the analysis model in previous network based on the system state, although in this paper, the analysis of the process is also based on the transfer of the system state, effectively avoids the direct definition of the system state and the probability calculation of state transition.

D. Quantitative Analysis of Reconfigurable Quality

Quantitative analysis of the reconfigurable is an important content of the reconfigurable network system research. Reconfigurable is a comprehensive concept, with multiple attributes, directly to the quantitative analysis of reconfigurable itself is very difficult. Based on the analysis of the basic properties and reconfigurable model, this section has quantitative robustness, evolution and survivability's metrics and then a quantitative analysis of reconfigurable system. The following is a quantitative attribute index.

1) Robustness Index

Robustness reflect the system under a variety of incentives of the abnormal events, can still provide the required basic service ability, emphasized on the basis of

using limited resources to maintain the service performance of the system. The system robustness with the state corresponding service system efficiency after robustness effect and the state corresponding service system efficiency before robustness effect, the corresponding service efficiency ratio, R.

$$R = \frac{J_f / R_f}{J_{f0} / R_{f0}} \tag{5}$$

Among them, the ratio of the system service capacity (output) and consume resources R (input) represent system service efficiency. J_f / R_f represents system service efficiency after robustness effect, J_{f0} / R_{f0} represents system service efficiency before robustness effect. Based on the hierarchical structure of the system status, system service capacity can be represent for $J = \sum_i s_i . v_{si}$, among them, v_{si} represents the importance weight of basic service Si is remains effective; Consume resources can be represented as $R = \sum_i \sum_j EC_{ij-vij}$, among them, vij represents the basic components EC_{ij} importance weights which is depended on basic service S_i; From the definition of the system robustness index R for a network system has good robustness, its robustness index should be greater than or equal to 1.

2) Evolution Indicators

System evolution quantity reflects the reconfiguration of the system resource's ability to meet the demand of system service at a certain evolution cost. System evolution with the evolution after state the corresponding service system efficiency and the evolution before state the corresponding service system efficiency ratio, remember to Δz.

$$\Delta z = \frac{J_z / C_z}{J_0 / C_0} = \frac{J_z / J_0}{C_z / C_0} \tag{6}$$

Among them, J_z represents system service ability after the evolution, J_0 represents the system service ability before evolution function; C_z represents resources consumed in the evolution configuration, C_0 represents resources consumed without carrying out the evolution configuration.

By definition, when $J_z \succ J_0$, $\Delta z \geq 1$, represents evolutionary configuration in the situation of the cost is not high to get higher network performance, this case has good evolution; $J_z \succ J_0$, $C_z \succ C_0$, $0 \prec \Delta z \prec 1$ represents evolution efficiency is not obvious, and the price is higher, makes little sense to evolution of configuration of this kind of circumstance; Other situations also need to according to the requirements of system evolution (focus on the price or performance) or add new indicators to analyze.

3) Survivability Index

Viability of the system under abnormal environment can use the rate of time change of d_J / d_t system service

performance to measure. Within the time period T, system survivability index Λ is defined as the action of system service performance degradation rate before the survivability respond to events and the action of system service performance degradation rate after the survivability respond to events,

$$\wedge = \frac{dJ_0 / d_t}{dJ_R / d_t} \qquad (7)$$

Among them, dJ_0 / d_t represents decline rate of system service performance before the survivability, dJ_R / d_t represents decline rate of system service performance after the survivability. According to the definition of system survivability index $\wedge$, has better survivability for a reconfigurable network topology, its survivability index should be greater than 1.
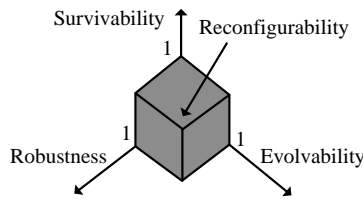

Figure 6.   Reconfigurable metric space

E. Reconfigurable Measurement

Reconfigurable of network system are needed to measure from multiple targets, multiple perspectives, based on the basic attribute of reconfigurable above, the analysis of robustness, the evolution and survivability index, evaluation is considered to be a measure of the reconfigurable respectively by robust d, evolutionary survival and product structure measurement of three dimensional space.

Reconfigurable measurement for corresponding to the three dimensional space of three dimensional vectors, the component are robustness index indicators, evolution and survivability index, expressed as $[R \, \overline{\Delta z}, \wedge]$. Among them, the index R and $\left\{\overline{\Delta z}\right\}$ are seen type (8) and (9), within the time period w, respectively get by type (5) and (6) update. As shown in figure 6, in metric space of the network system reconfigurable indicators, weight index w, $\overline{\Delta z}$ and $\wedge$ values greater than 1 unit cube on the lateral area of the reconfigurable measurement is efficient.

$$\overline{R} = 1 / w. \sum\nolimits_{w=i-w}^{w} R(w) \qquad (8)$$

$$\overline{\Delta z} = 1 / w. \sum\nolimits_{w=i-w}^{w} \Delta z(w) \qquad (9)$$

IV.   EXPERIMENT AND ANALYSIS

In recent years a large number of studies have shown that the characteristics owned by network is decides by the network topological. The following specific network

topology is the quantitative analysis of the reconfigurable network topology. ARPA network as shown in figure 7 (a) is Europe and the United States common trunk network topology, including 21 nodes and 26 connections are the uniform network, and most node degree is 2.

(a) ARPA network topology
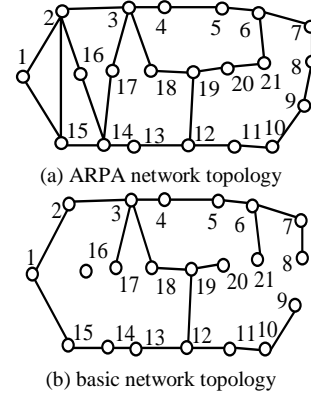

(b) basic network topology

Figure 7.   Examples for network topology

Assuming that basic network topology with the size of ARPA network the GT is the minimum connected tree structure generated by 21 nodes and 20 side shown in figure 7 (b) of article. Compared with the topology GT, ARPA network topology under the condition of removing any node or malicious removed key nodes at random, won't make the network is not connected, pertaining to the ARPA network for a single node failure by robust. However, as the network environment deterioration, if consider removing multiple nodes at the same time, such as maliciously v_3 and v_{12}, remove node will result in no network connectivity, network performance fell sharply.

According to the established reconfigurable analysis models, assuming that the system state set corresponding to the network topology in abnormal environment $G(n,m)$ (n number of nodes, m said the number of edges), among them, the part of the state transition relationship is shown in figure 8 (see figure 5 dotted box wife figure). The state q0 corresponding figure $G_{ARPA}(22,27)$, q_1 figure corresponding chart $G_{ARPA} - \{v_3\}(20,21)$ after removing the node v_3 , q_1' corresponding to add edge set $E'\{(v_1,v_4),(v_{16},v_{17})\}$ evolution generated figure GARPA+E'(20,24), abnormal events scene AE_{attack} represents removed degree of ARPA network Information center (Information $C_{en-trality}$, one of malicious attacks on the largest node vitamin c_k^i, and can be described as $q_0 \times AE_{attack} \rightarrow q_1$ state transition; the answering event scene $RE_{addlink}$ represents the evolution response behavior of adding edge set E , realize the state transition $q_1 \times RE_{addlink} \rightarrow q_1'$.

The following analysis the robustness of ARPA network topology, evolution and survivability measure and the analysis of ARPA network reconfigurable quantify. For convenience of analysis, assuming that the connection of topology at the same price as 1, connecting n section point, requires at least $n-1$ the edge, if

connected side is more than $n-1$, will increase the corresponding network resources. The redundancy of the network structure can be defined as the excess number of edges in the graph (the actual number of edges with minimum connected the difference between the number of edges of the tree) with the ratio of the number of edges in same size completely diagram. Removed node or edge from the network, often affect the shortest path between nodes and change of the connection degree; make the efficiency of network change. Average network efficiency (Eave) under the random failure can be used to the said the function of the network topology efficiency. Therefore, the robustness of ARPA network topology index can be represented as RF_{at}.
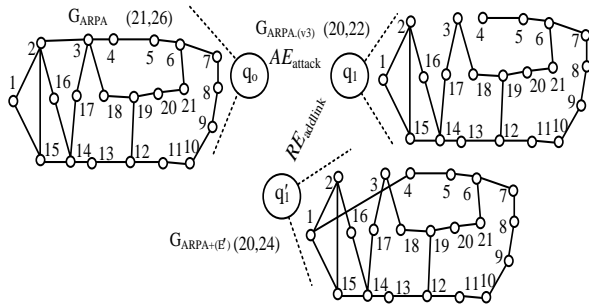

Figure 8.   Diagram of ARPA network state transition

$$(ARPA) = \frac{E_{ave}(ARPA)}{E_{ave}(G_z)} = 1.410$$

Evolution indicators measure of ARPA network after removing nodes v3, before the evolution of network diagram $G_{ARPA-\{V_3\}}$ and after evolution the generated network diagram GARPA+E' is consider the average efficiency ratio of the network under network resource consumption. The indicators for the evolution

$$\Delta e_{NT}(ARPA) = \frac{E_{ave}(G_{ARPA+E})}{E_{ave}(G_{ARPA-\{V_3\}})} \cdot \frac{G_{ARPA-\{v_3\}}(20,21)}{C_{APRA+E'}(20,25)} = 1.142$$

ARPA network survivability measure with basic network topology with GT and ARPA network in exceptional cases, the ratio of the network survival adaptability (T) declined to describe. Figure 9 shows the ARPA network and GT survival adaptability increased with the increase of removing node number change (statistics) of 10 groups of experimental data, can be observed from the table, the ARPA network is better than the GT survival adaptability, at random to remove node in the initial period ($Num = [0,3]$), the survival of GT adaptability's decline rate obviously bigger than $APRA$ network. In general, in most of the network, failure probability of two or more nodes at the same time is very small, so we only consider removing a few nodes. So consider reduced network adaptive survival ratio in the initial period can fully reflect the survival adaptability situation of network topology. ARPA network survivability index can be approximately expressed as ΔNT.

$$(ARPA) = \frac{\Delta T(G_T)}{\Delta T(ARPA)} = 1.591$$
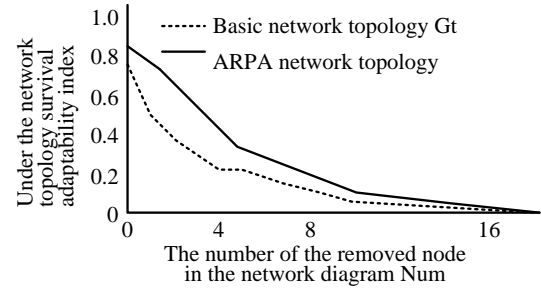

Figure 9.   Survival adaptability of ARPA and basic network G_T

Based on quantitative analysis of $APRA$ network robustness, evolution and survivability index above shows that 3 d reconstruction of $APRA$ network can be quantitative indicators for $[1.391,1.140,1.591]$, $APRA$ network is an efficient network topology which can be heavy construct.

V.   CONCLUSION

Reconfigurable research of network system is as a new direction based on the network safety, fault tolerance and survivability research in such fields, are receiving more and more attention. It is different with previous analysis model of the system network based on the state, this paper analysis of reconfigurable although also be based on the system state description, through the establishment of the state of the system hierarchy, effectively avoid the direct definition of the state of the system and the calculation of the system state transition probability. With the introduction of abnormal situations and response events scene of different levels on the relationship between the environment - system for dynamic description and analysis, reflects the reconfigurable network system dynamic ability to adapt to the environment changes

This paper carries out the network system reconfigurable analysis model based on FSM which based on the formal description and modeling for abnormal reconfigurable system robust behavior under the network environment, evolution behavior and survival behavior. To achieve the quantitative evaluation of the system reconfigurable, in the analysis of the measurement network topology reconfigurable, on the basis of the proposed network system of reconfigurable metrics. Metrics of reconfigurable make the network system analysis model with the quantitative analysis of application prospects.

REFERENCES

[1] Z. Pei and Z. Zhenxiang, "A framework for personalized service website based on TAM," *in the international conference on service systems and service management.* vol. 2 Troyes, France: IEEE, 2006, pp. 1598-1603.

[2] Jiaping Liu, A. Stolyar, M. Chiang, H. V. Poor, "Queue back-pressure random access in multihop wireless networks: optimality and stability," *IEEE Transactions on Information Theory*, vol. 55, no. 9, pp. 4087-4098, 2009. http://dx. doi. org/10. 1109/TIT. 2009. 2025563

[3] Jing Chen, Tong Li, Ruiying Du, et al. "Efficient reliable opportunistic network coding based on hybrid flow in wireless network," *China Communications*, vol. 8, no. 4, pp. 125-131, 2011.

[4] M. Teltzrow and A. Kobsa, "Impacts of User Privacy Preferences on Personalized Systems: A Comparative Study," *Designing personalized user experiences in E-Commerce,* vol. 5, pp. 315-332, 2004.

[5] Mu Yong-min, ZHENG Yu-hui, ZHANG Zhi-hua et al. The algorithm of infeasible paths extraction oriented the function calling relationship. *Chinese Journal of Electronics*, 2012, 21(2): 236-240.

[6] Nagurney A, Yu M, Qiang Q. Supply chain network design for critical needs outsourcing. *Regional Science,* 2011, 90(1): 123-142.

[7] M. Dostál and Z. Eichler, "Fine-Grained Adaptive User Interface for Personalization of a Word Processor: Principles and a Preliminary Study," *Communications in Computer and Information Science,* vol. 173, pp. 496-500, 2011. http://dx. doi. org/10. 1007/978-3-642-22098-2_99

[8] Yafei Hu, Fangmin Li, and Xinhua Liu. "Network Coding Based Link Scheduling for QoS Provisioning in Multi-radio and Multi-channel Wireless Mesh Networks", *Journal of Communications,* vol. 7(4), pp: 899-908, 2012.

[9] *Bo Yang, Chung-Huang Yang, Yong Yu, Dan Xie,* A Secure Scalar Product Protocol and Its Applications to Computational Geometry. *Journal of Computers*, Vol 8, No 8 (2013), 2018-2026

[10] D. Rigas and K. Al-Omar, "A Controllability and Customization Approach to Personalized Web Content," *International Journal of Education and Information Technologies* vol. 4, pp. 33-40, 2010.

[11] M. Lillibridge et aI., "Sparse Indexing, Large Scale, Inline Deduplication Using Sampling and Locality," *in proceedings of 7th USENIX Conference on File and Storage Technologies, USENIX Association, San Francisco, California, 2009*, pp. 111-123.

[12] Ronasi, Keivan, Vincent W. S. Wong, and Sathish Gopalakrishnan. "Distributed Scheduling in Multihop Wireless Networks with Maxmin Fairness Provisioning," *IEEE Transactions on Wireless Communications,* vol. 11, no. 5, pp. 1753-1763, 2012. http://dx. doi. org/10. 1109/TWC. 2012. 030812. 110493

[13] *Bin Zhou, Rongbo Zhu, Ying Zhang, Linhui Cheng,* An Efficient Data Fingerprint Query Algorithm Based on Two-Leveled Bloom Filter. *Journal of Multimedia,* Vol 8, No 2 (2013), 73-81

[14] R. Ahlwede, N. Cai, S. R. Li, R. W. Yeung, "Network information flow," *IEEE Transactions on Information Theory,* vol. 46, no. 4, pp. 1204-1216, 2000. http://dx. doi. org/10. 1109/18. 850663

[15] Takahiro Matsuda, Taku Noguchi, Tetsuya Takine, "Survey of Network Coding and its applications," *IEICE Transactions on Communications*, vol. E94-B No. 3, 2011.