A General Framework for Network Survivability Testing and Evaluation

Chunlei Wang
Tsinghua University/Department of Computer Science, Beijing, China
Email: wcl08@mails.tsinghua.edu.cn

Liang Ming, Jinjing Zhao and Dongxia Wang
National Key Laboratory of Science and Technology on Information System Security, Beijing, China
Email: mingliang78@yahoo.com.cn, misszhaojinjin@sina.com, dongxiawang@126.com

***Abstract*—The survivability of network is of vital importance with respect to the normal operation of information infrastructure. The current research works in the area of network survivability generally aimed at the definitions and quantifications of specific survivability attributes or metrics for distinct network objects. Unfortunately, there is a lack of research concerning how to model, test and evaluate the survivability of network in a consistent manner, and it is helpful to the unification of network survivability testing and evaluation and the promotion of related research works in the area of network survivability. Furthermore, the requirements for network survivability testing and evaluation are variable among different application domains. Therefore, a flexible mechanism to support the customizable testing and evaluation of network survivability is needed. In this paper, we propose a unified framework for network survivability testing and evaluation which is extensible and customizable. The customization method of network survivability measurement model and the general process of network survivability testing and evaluation are analyzed in detail. The testing of network survivability is performed based upon specific network survivability measurement model, and the associated test scheme containing a set of test cases are generated. The evaluation of network survivability is performed based upon the quantification results of network survivability metrics, and multiple criteria decision making method is utilized to evaluate network survivability. The experimental results show the generality and practicability of the framework and the effectiveness of proposed network survivability test model and evaluation method.**

***Index Terms*—network survivability, testing and evaluation framework, survivability model, survivability testing, survivability evaluation**

I. INTRODUCTION

With the rapidly development of network information techniques and the widely application of Internet, modern society becomes ever more dependent upon the continuously operations of network information systems. Therefore, the survivability of network is of vital importance with respect to the normal operations of information infrastructures. The goal of network survivability is to maintain the fundamental network system services in the face of faults/failures and to support the fulfillment of organization missions. The generally accepted definition of information system survivability was introduced by Ellison et al. [1]:

Survivability: the ability of a network computing system to provide essential services in the presence of attacks and failures, and recover full services in a timely manner.

Generally, the increased impact of network system vulnerabilities makes the testing and evaluation of network survivability under fault/failure events essential in network planning, design, implementation, and verification. In recent years, several organizations have achieved important progress in network survivability research and have proposed several new analysis methods. However, the definitions and quantification forms of network survivability these methods depend upon are complicated and divergent, and the unified and normalized framework for network survivability testing and evaluation which is convenient for implementation has not been proposed.

The measurement of network survivability usually refers to the quantitative metrics of network survivability. The provision of appropriate survivability metrics is the basis for objectively evaluating the survivability of network [2]. Due to the complexities of network systems, it is relatively difficult to model and analyze the intentional attacks and the methods for systematically analyzing and scientifically abstracting network survivability data are scarce. In this paper, we propose a flexible and extensible framework for network survivability testing and evaluation based upon the currently research outcomes of network survivability, and analyze the customization of network survivability measurement model and the process of network survivability testing and evaluation in detail. The contribution of this paper provides a feasible research approach for the normalization of network survivability testing and evaluation and the promotion of network survivability research.

The organization of this paper is as follows. In Section II, we propose the general framework for network survivability testing and evaluation, describe the

doi:10.4304/jnw.6.6.831-840

relationships between the framework and the multi-layered network needs to be evaluated (e.g. TCP/IP network), and show the customization of network survivability measurement model, and then summarize a general process of network survivability testing and evaluation. In Section III and IV, we describe the testing and evaluation methods of network survivability respectively. The framework and associated methods are illustrated and discussed in detail through experimental analysis in Section V. Finally, in Section VI we review related work, and in Section VII we draw conclusions and figure out future work.

II. Network Survivability Testing and Evaluation Framework

From the analysis of network survivability research works, we found that the survivability testing and evaluation that researchers concerns are relevant to specific application domains. Therefore, different network survivability measurement models need to be established. In addition, researchers would propose pertinent survivability metrics and associated quantification methods on different application backgrounds. In research and development practices, we found that the quantitative testing and evaluation of network survivability needs to consider a large amount of technical problems, and it requires that survivability testing and evaluation be performed through a unified approach which could accurately reflect the essence of network survivability. For instance, how to select appropriate survivability metrics as needed when quantifying the survivability of network, and how to choose reasonable quantitative evaluation methods based upon the characteristics of measured network objects in the survivability testing and evaluation system. The proper settlement of these problems is the precondition for accurately evaluating and effectively improving network survivability.

As we can see, for the evaluation of network survivability, considering one aspect separately could easily neglect other aspects, thus negatively impacting on the holistic assessment effects of network survivability. However, it is impractical to propose a general and accurate definition for quantitatively evaluating the survivability of network system owing to the diversity of survivability characteristics. We consider that the integrity of network survivability evaluation should be emphasized based upon the research works on various network survivability testing and evaluation methods. And the metrics, the models, and the testing and evaluation methods of network survivability should be synthesized in a holistic manner.

Meanwhile, the testing and evaluation of network survivability should be extensible and convenient for user extensions against different characteristics and object types from each domain. This paper proposes an extensible framework for network survivability testing and evaluation based upon the above analysis, which is applicable to a wide range of network system architectures, applications, fault/failure types, and desired survivability metrics and can be used to derive quantitative measures proposed by different network survivability measurement models.

The purpose of network survivability testing and evaluation framework is to construct the measurement model of network survivability, normalize the process of network survivability testing and evaluation, and provide specific testing and evaluation methods based upon practical requirements, as shown in Fig. 1. This framework is customizable and extensible, which reflects the required general architecture of network survivability testing and evaluation systems. The framework shown in Fig. 1 provides support for the typical measured network such as TCP/TP network, and the measured network could perform network survivability analysis and optimization using the information about network survivability evaluation information provided by the framework, such as routing backup and reconstruction based upon network connectivity [17].

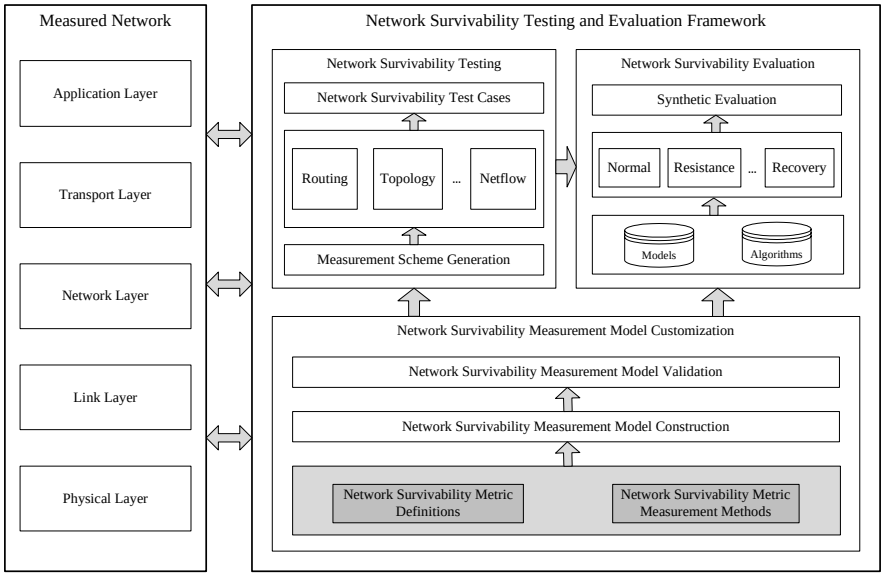


Figure 1. The architecture of network survivability testing and evaluation framework.

The framework for network survivability testing and evaluation mainly consists of the following three parts:

- *Customization of network survivability measurement model.* It is used for the definition of network survivability measurement model adaptable for specific domain requirements. The model can be customized based upon existed measurement model and specific measurement requirements from different domains. Meanwhile, the extensibility of model needs to be considered to support different domain applications. As a consequence, network survivability model construction is the groundwork of the whole framework and the extensible customization methods of network survivability measurement need to be provided to support the subsequent work.
- *Network survivability testing.* It is used for the testing and quantification of network survivability metrics based upon specific network survivability measurement model. This part needs to consider the characters in different stages in the survivable process, e.g. resistance, destroyed and recovery, and acquire the corresponding network survivability measurement data for calculation based upon the user requirements (e.g. network states, test scenes, test objects, and test methods, etc.), and finally obtains the quantification results of network survivability metrics.
- *Network survivability evaluation.* It is used for the evaluation of network survivability based upon the quantification results of network survivability metrics, and different network survivability evaluation models and algorithms can be utilized based upon the types of network to be measured and the distinct evaluation objectives.

A. Customization of Network Survivability Measurement Model

The establishment of network survivability measurement model is one of the most important foundations for performing various network survivability research works. The research works related to network survivability measurement model mainly focus on the definitions of network survivability model structure, that is, which survivability metrics the model should be composed of, and how to organize the corresponding metrics. In previous research works, researchers have proposed a great deal of metrics for quantifying network survivability, such as, network connectivity [17], Mean Time To Failure (MTTF) [18][19], Mean Time To Repair (MTTR) [18], etc. Aimed at different network measurement objects, researchers have proposed respective quantification metrics based upon the characteristics of the measured objects. For instance, the excess packet loss due to failures (ELF) is taken as the survivability performance metric of wireless ad-hoc network [16]. We roughly divide the proposed network survivability metrics as the following aspects by summarizing previous research works: robustness, availability, controllability, and adaptability, etc. Moreover, with the development of network survivability techniques, new metrics of network survivability would be proposed continuously. This kind of extensibility requirements need to be concerned when customizing network survivability model.

Furthermore, there probably have several quantification methods for the same network survivability metrics. For instance, the proposed quantification methods for network blocking probability [6] include the pure performance model based method, the pure availability model based method, and the performability measurement method. Each of the above three methods has respective application scenarios, so users probably expect to utilize several different quantification methods to measure network blocking probability, and synthetically compare and evaluate the quantification results under different measurement methods. That is, users may need to bind several quantification methods to specific network survivability metric when customizing network survivability model.

In this paper, we propose an extensible Network Survivability Measurement Model (NSMM) which consists of a set of measurement dimensions describing the capabilities of network survivability. The measurement dimensions can be nested, i.e. upper dimensions can be described by lower dimensions in detail. A measurement dimension of network survivability is composed of a set of network survivability metrics ultimately, and the metrics of network survivability are the atomic attributes of network survivability which is undividable. That is, the metrics of network survivability are the leaf nodes of network survivability model depicted as tree style, and the measurement dimensions are the branch nodes of the model.

A typical measurement model of network survivability is shown in Fig. 2. In this figure, each network survivability metrics can be bound with multiple quantification methods, one or several appropriate quantification methods can be selected based upon practical requirements and the quantification results of these methods can be examined when users need to measure specific survivability metric.

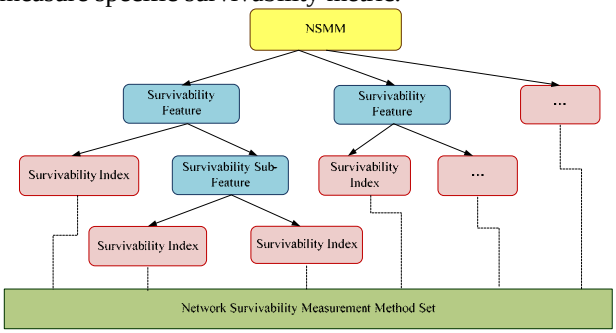


Figure 2. A typical network survivability measurement model.

We adopt 5-tuple to describe the above mentioned network survivability measurement model.

$NSMM =< FS, SFS, MS, VS, MM >$, which:

1) *FS* refers to the top level feature in *NSMM*, describing as the set of 2-tuple $< FN, FID >$, which: *FN* represents the name of feature, *FID* is the ID number of feature. The setup of this ID number is convenient for description and management, and there is a unique ID number for each feature and sub-feature.

2) *SFS* refers to the set of sub-features, describing as the set of 2-tuple $< FID, SFs >$, which: *FID* represents the feature name which is the parent of this set of sub-features, *SFs* refers to the set of 2-tuple $< SFID, SFN >$, which: *SFID* represents the ID number of sub-feature, and *SFN* represents the name of sub-feature.

3) *MS* refers to the set of survivability metrics, describing as the set of 3-tuple $< SFID, Metrics, \{MtdS\} >$, which: *SFID* represents the feature name which is the parent feature of this set of metrics, *Metrics* refers to the set of 2-tuple $< MID, MN >$, which: *MID* represents the ID number of metrics, and *MN* represents the name of metric. Therefore, the elements of *FS*, *SFS* and *MS* are combined to define the composition structure of *NSMM*. *MtdS* describes the measurement methods bound with this metric, which consists of 2-tuple $< MtdID, Context >$, which: *MtdID* represents the ID number of measurement method, and *Context* describes the scenario context corresponding to specific survivability measurement method.

4) *VS* refers to the set of 4-tuple $< MID, MtdID, Unit, Value >$ for describing the concrete values of the survivability metric, which: *MID* represents the ID number of metric in *NSMM* model, *MtdID* represents the ID number of quantification method, *Unit* represents the unit of metric value, *Value* represents the concrete value of corresponding metric identified by *MID*.

5) *MM* refers to the set of 4-tuple $< MtdID, MtdN, MID, MtdDesc >$, which is the set of available measurement methods in network survivability measurement framework. In this 4-tuple, *MtdID* represents the ID number of measurement method (each method has its unique ID number), *MtdN* represents the name of measurement method, *MID* represents the ID number of survivability metric which corresponds to the measurement method indentified by *MtdID*, *MtdDesc* is the description of measurement method.

From the above definition, we propose an extensible network survivability measurement model, and the model could be customized based upon the characteristics of different domains. Moreover, the measurement model could be used to guide the testing and evaluation of network survivability.

B. Network Survivability Testing and Evaluation Process

As shown in previous sections, many metrics could be used to describe network survivability, e.g. network connectivity, network blocking probability, MTTF, etc. Usually, narrow survivability definitions tend to specify one or a set of closely related metrics upon which the quantification work is performed [20]. However, the evaluation of network survivability covers extensive factors from specific network objects to users' requirements and expectations for satisfying different evaluation objectives, and the quantifications of these metrics often performed in a case by case manner.

In the framework, we propose a general process of network survivability testing and evaluation based upon the customization of network survivability measurement model. The process can be applied to a variety of network survivability models covering different survivability metrics, as well as the new metrics that will appear in the future.

In general, the testing and evaluation of network survivability can be summarized in the following 6-step process, and the process supports the iteration of survivability testing and evaluation, as shown in Fig. 3.

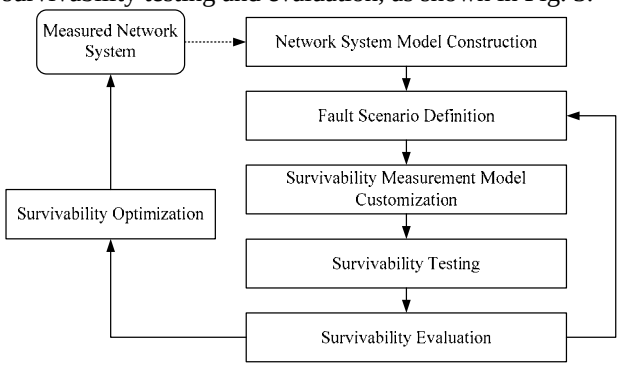


Figure 3. The general process of network survivability testing and evaluation.

Step 1. Construct the measured network system model. The concerns of network survivability are the capabilities of measured network providing proper services. Therefore, it needs to construct the network system model for survivability testing and evaluation based upon network topology, network objects and network services. The network system model can be defined as the following form: $NSM =< TP, \{NO\}, \{NS\} >$, which: *TP* represents the topology of measured network, $\{NO\}$ represents the set of network objects, and $\{NS\}$ represents the set of network services.

Step 2. Define fault scenarios. Network survivability mainly considers the effects caused by stochastic fault events and intentionally malicious events, so the relationships among these events must be seriously concerned. Therefore, we represent these associated events with common intentions in network survivability testing and evaluation by means of fault scenarios, which can be defined as the following form: $FS = \{NS, P, \{E\}, \{NO\}, desc\}$, which: *NS* represents the affected network services, *P* represents the weight value of severity, $\{E\}$ represents the set of atomic events of the fault scenario which determines the several key steps of *FS*, $\{NO\}$ represents the set of network objects

involved by the fault scenario, *desc* represents the description of fault scenario.

Step 3. Customize network survivability measurement model. The appropriate network survivability metrics and associated quantification methods are selected based upon the network system model constructed by step 1 and the fault scenarios defined by step 2, and the survivability measurement model suitable for the measured network is customized which mainly emphasizes the relationships among network system model, fault scenarios and network survivability metrics.

Step 4. Perform the testing of network survivability. To test network survivability, the associated test scheme containing a set of test cases must be generated based upon the customized survivability measurement model. The involved network objects and network services are tested based upon the fault scenario, the corresponding test data are obtained from measured network, and the quantification results of network survivability metrics are calculated based upon the measurement methods.

Step 5. Perform the evaluation of network survivability. Usually, the evaluation of network survivability attributes is performed in a hierarchical manner, e.g. resistance, destroyed, recovery, etc. And the evaluation of different survivability attributes corresponds to the test results of different survivability metrics which utilize different survivability evaluation models and algorithms.

Step 6. Perform the optimization of network survivability. The network management policies for the optimization of network survivability can be designated based upon user requirements and network operation environment. The configuration and topology of network can be optimized based upon the evaluation results of network survivability and pre-configured policies so as to achieve better network survivability.

III. NETWORK SURVIVABILITY TESTING

According to the network survivability testing and evaluation framework described in Section II, we need to get the values of the customized survivability metrics by network survivability test. In this section, we will describe how to make a network survivability test and set up test cases for given survivability metrics in detail.

Compared with ordinary test, network survivability test should consider much more problems, even the great difference of each phase during a network surviving process. So there is a lot of work needs to be done to study the principle of survivable network's operation. And there are also some problems nowadays in network survivability test, such as insufficient test cases, unsatisfying test results, and low testing efficiency. In order to address these problems, in this section we propose a test model based on the evolvement process of survivable network, by considering the characteristics of network states in different phases of surviving process. Finally, survivability testing is performed in accordance with the test model.

According to the characteristics of network states in different phases of the survivable process, we set up a Test Model based on the Evolvement Process of Survivable Network (TMEPSN) [21].

In TMEPSN, there are six components, which are test scenes, network states, survivability metrics, test objects, adjusting policies, and test methods. The corresponding notations for the above six components are described as follows:

1) S : refers to a set of network states, let $S=\{s_1,s_2,s_3,s_4,s_5\}$ where s_1, s_2, s_3, s_4, s_5 denotes normal, resistance, destroyed, recovery, and adaptation state respectively.

2) E_OBJT : refers to a set of scene factors in target component, for example, E_OBJT ={ $Normal\_Traffic$, $Topology$, $Security\_Mechanism$, Bug, …}.

3) E_ATTK : refers to a set of scene factors in attack component, for example, E_ATTK ={ $Attack\_Traffic$, $Attack\_Tool$, $Attack\_Path$, …}.

4) E_TEST : refers to a set of scene factors in test component, for example, E_TEST ={ $Test\_Traffic$, $Test\_Position$, $Sensor\_Property$, …}.

5) E : refers to a total set of test scenes described by component E_OBJT, E_ATTK and E_TEST. Namely, $E=E\_OBJT\times E\_ATTK\times E\_TEST$.

6) M : refer to a set of survivability metrics, let M ={ m_1, m_2, m_3, …, m_i ,…, m_n } where m_i denotes a test metric, and n is the number of test metrics.

7) B : refers to a set of test objects, let B ={ b_1, b_2, b_3,…, b_i, …} where b_i denotes a test object.

8) W : refers to a set of test methods, let W ={ w_1, w_2, w_3, …, w_i, …} where w_i denotes a test method.

9) P : refers to a set of adjusting policies, let P ={ p_1, p_2, …, p_i, …, p_n } where p_i denotes an adjusting policy directly corresponding to the survivability metric m_i. And n is the number of adjusting policy.

In order to describe the network survivability test formally based on TMEPSN in the network survivability testing and evaluation framework, we need a number of definitions for network survivability test.

Definition 1: Network survivability test whole set A is defined by

$$A=E\times S\times B\times M\times P\times W$$

where E, S, B, M, P, and W are sets of test scenes, network states, test objects, survivability metrics, adjusting policies, and test methods respectively.

Definition 2: Network survivability test a, and $a\in A$ is a network survivability test for some problem. $a=(e,s,b,m,p,w)$

where $e\in E$, $s\in S$, $b\in B$, $m\in M$, $p\in P$, $w\in W$, and we can use $e=e(a)$, $s=s(a)$, $b=b(a)$, $m=m(a)$,

$p = p(a)$, $w = w(a)$ represents the values of e, s, b, m, p, w respectively.

Definition 3: Network survivability test subset A_k is a network survivability test set about problem k. $A_k = \{a_1, a_2, ..., a_i, ...\}_k$, $A_k \subset A$, where a_i is a network survivability test for problem k.

Based on each component of test model, network survivability test subset can be divided into the following types: network survivability test subset based on test scenes, network survivability test subset based on network states, network survivability test subset based on test objects, network survivability test subset based on test metrics, and network survivability test subset based on test methods. Here, we only need network survivability test subset based on test metrics for the requirements of Network Survivability Testing and Evaluation Framework.

Definition 4: *M*-based network survivability test function f_M, is a type of network survivability test based on test metrics, and $f_M : M \to A$. For any m in M, there exists a subset A_m in A correspondingly. Namely, $\forall m \in M$, there exists $A_m \subset A$, which answers for $f_M(m) = A_m$. A_m is the *m*-based network survivability test subset, also called as a case of *M*-based network survivability test.

As we have got a set of customized network survivability metrics, considering an *M*-based network survivability test in Definition 4, we can get the relationships among six components in a given test A_m shown in Fig. 4.

Choosing proper test method is a key in network survivability test. Considering network survivability test whole set A, we can define an assigning function as below.

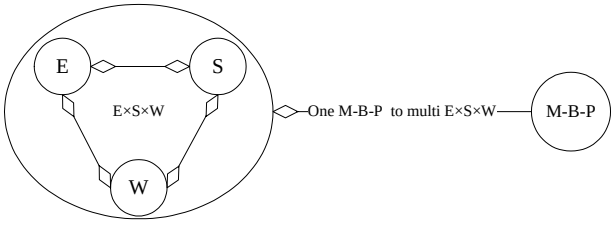


Figure 4. Relationships among six components in a given test A_m

Definition 5: Assigning function of survivability test method is $F : E \times S \times B \times M \times P \to \psi(W)$. Assigning function $F(e, s, b, m, p) = \{w\}$ means that we can get a proper test method $w \in W$, by using some test scene $e \in E$, some network state $s \in S$, some test object $b \in B$, some test metric $m \in M$, and some adjusting policy $p \in P$.

Assigning function of survivability test method is achieved by constraints based on the relationship matrix of the six components. With assigning function, we can produce network survivability test subsets.

Definition 6: Distance of two survivability tests a_1 and a_2 is $\lambda = |a_1 - a_2|$, which denotes the Euclidian Distance of survivability tests vectors a_1 and a_2, where $a_1 = (e_1, s_1, b_1, m_1, p_1, w_1)$, $a_2 = (e_2, s_2, b_2, m_2, p_2, w_2)$.

By calculating the distance λ, we can make several survivability tests with shorter distances performing in parallel, and make other survivability tests with larger distances performing in series, which can enhance the test efficiency and resource.

Now we can make survivability testing in the light of the test model in four steps as follows:

Step 1. Describe test requirements with six basic components in the test model TMEPSN. We should list the contents of each component formally, for example, $M = \{SRT, TST, NLD, TRT\}$ represents test metric set with four metric, i.e. Service Response Time, Threat Sensing Time, Network Link Degree, and Topology Reconstruction Time respectively.

Step 2. Get constraint functions from the relationships among the six components shown in Fig. 4. We should list all the mapping relationships in Fig. 4 for given test requirement.

Step 3. Produce all the assigning functions of test methods by using the constraints described above in the form of Definition 5.

Step 4. Set up test cases in the form of Definition 3 by using the assigning functions of test methods. What's more, we can consider making parallel test to improve the test efficiency.

IV. NETWORK SURVIVABILITY EVALUATION

The network survivability evaluation method is the course of getting the rank preference order of each alternative according to the evaluation measurements based on the test result of every survivability metrics. This is a typical Multiple Criteria Decision Making Problem (MADM) [24].

MADM deals with the problem of choosing an option from a set of alternatives which are characterized in terms of their attributes. MADM is a qualitative approach due to the existence of criteria subjectivity. It requires information on the preferences among the instances of an attribute, and the preferences across the existing attributes. The aim of the MADM is to obtain the optimum alternative that has the highest degree of satisfaction for all of the relevant attributes.

A MADM problem can be concisely expressed in a matrix format, in which columns indicate attributes considered in a given problem; and in which rows list the competing alternatives. Specifically, a MADM problem with m alternatives $(A_1, A_2, ..., A_m)$ that are evaluated by n attributes $(C_1, C_2, ..., C_n)$ can be viewed as a geometric system with m points in n-dimensional space. An element $X_{i,j}$ of the matrix indicates the performance rating of the i th alternative, A_i, with respect to the j th attribute, C_j, as shown in Eq. (1):

$$D = \begin{array}{c} \\ A_1 \\ A_2 \\ A_3 \\ \cdots \\ A_m \end{array} \begin{array}{c} \begin{array}{ccccc} C_1 & C_2 & C_3 & \cdots & C_n \end{array} \\ \begin{bmatrix} x_{11} & x_{12} & x_{13} & \cdots & x_{1n} \\ x_{21} & x_{22} & x_{23} & \cdots & x_{2n} \\ x_{31} & x_{32} & x_{33} & \cdots & x_{3n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ x_{m1} & x_{m2} & x_{m3} & \cdots & x_{mn} \end{bmatrix} \end{array} \quad (1)$$

Typically, a network attack process can be divided into five steps: normal, resistance, destroyed, recovery, and adaptation. In order to make a reasonable and scientific decision to the network survivability, every attack step should be evaluated. After getting the network statements on each attack step of each alternative, a final decision can be drawn. To make the evaluation result of each attack step and each alternative into one criterion, the TOPSIS evaluation method is adopted.

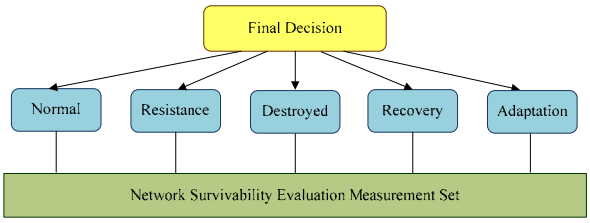


Figure 5. A typical network survivability evaluation model.

TOPSIS (Technique for Order Preference by Similarity to Ideal Solution) have been applied to solve a variety of applications, and are proven methodology in solving MADM problems [25].

The evaluation procedure is defined as follows:

Step 1: Build the decision matrixes for every attack course and calculate normalized rating for each element in the decision matrixes by Eq. (2):

$$r_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1}^{m} x_{ij}^2}} \quad i = 1,...,m, \quad j = 1,...,n \quad (2)$$

Step 2: Calculate weighted normalized ratings for every element in the three decision matrixes. The weighted normalized value $v_{i,j}$ is calculated by Eq. (3).

$$v_{ij} = w_i r_{ij} \quad i = 1,...,m, \; j = 1,...,n \quad (3)$$

Step 3: Identify positive ideal (A^*) and negative ideal (A^-) solutions for every attack course. The A^* and A^- are defined in terms of the weighted normalized values, as shown in Eq. (4) and (5), respectively:

$$A^* = \{v_1^*, v_2^*, \ldots, v_j^*, \ldots, v_n^*\} = \left\{\left(\max_i v_{ij} \mid j \in J_1\right), \left(\min_i v_{ij} \mid j \in J_2\right) \mid i = 1,...,m\right\} \quad (4)$$

$$A^- = \{v_1^-, v_2^-, \ldots v_j^-, \ldots, v_n^-\} = \left\{\left(\min_i v_{ij} \mid j \in J_1\right), \left(\max_i v_{ij} \mid j \in J_2\right) \mid i = 1,...,m\right\} \quad (5)$$

Where J_1 is a set of benefit attributes (larger-the-better type), and J_2 is a set of cost attributes (smaller-the-better type).

Step 4: Calculate separation measures. The separation (distance) between alternatives can be measured by the n-dimensional Euclidean distance in every decision matrix. The separation of each alternative from the positive ideal solution, A^*, is given by Eq. (6):

$$S_i^* = \sqrt{\sum_{j=1}^{n} (v_{ij} - v_j^*)^2}, \quad i = 1,...,m \quad (6)$$

Similarly, the separation from the negative ideal solution, A^-, is given by Eq. (7):

$$S_i^- = \sqrt{\sum_{j=1}^{n} (v_{ij} - v_j^-)^2}, \quad i = 1,...,m \quad (7)$$

Step 5: Calculate similarities to ideal solution in every decision matrix. This is defined in Eq. (8):

$$C_i^* = \frac{S_i^-}{S_i^* - S_j^-}, \quad i = 1,...,m \quad (8)$$

Note that $0 \leqslant C_i^* \leqslant 1$,where $C_i^* = 0$ when $A_i = A^-$, and $C_i^* = 1$ when $A_i = A^*$.

Step 6: Build the decision matrix for the final decision. This is defined in Eq. (9):

$$E = \begin{bmatrix} C_{S1,1} & C_{S2,1} & C_{S3,1} & C_{S4,1} & C_{S5,1} \\ C_{S1,2} & C_{S2,2} & C_{S3,2} & C_{S4,2} & C_{S5,1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ C_{S1,m} & C_{S2,m} & C_{S3,m} & C_{S4,m} & C_{S5,1} \end{bmatrix} \quad (9)$$

Step7: Redone the Step3 to Step 5 again for matrix E, and calculate rank preference order. Choose an alternative with maximum C_i^* or rank alternatives according to C_i^* in descending order.

V. Case Studies

In this section, we perform an experiment to test and evaluate the survivability of network under different scenarios and to validate the generality and practicability of the framework proposed in this paper.

A. Requirement of the Test Case

In the experiment, a network system with six basic components in the test model TMEPSN is described. Because of the importance of test metrics, we focus on analyzing the *M*-based network survivability test and its description mechanisms. We will discuss its *M*-based network survivability test.

Based on the test model TMEPSN and Definition 4, network survivability test subset A_m can be obtained from *M*-based network survivability test function $f_M : M \to A$. Function f_M can be resolved

by assigning function f in Definition 5 and relationships in Fig. 4, then we can get A_m.

$E=\{e_1,e_2\}$, which represents the set of test scenes with two test scenes e_1 and e_2 shown in Table I, which includes target aspect, attack aspect, and test aspect.

TABLE I.
TWO TEST SCENES E1AND E2

Scene	Target aspect				Attack aspect	Test aspect
	Node number	***Network link degree***	***Routes***	***Services***		
e_1	100	20	20000 pieces of BGP routes	50 Web services	none	test component deployed on one node
e_2	100	20	20000 pieces of BGP routes	50 Web services	one kind of worm virus attacking network connection	test component deployed on one node

$S=\{s_2,s_3,s_4\}$, which represents network state set with three network states, i.e. resistance, destroyed, and recovery respectively. The criterion of resistance is 80% of node link degree≥10, and that of destroyed states is 80 % of node link degree<10, and that of recovery is 80% of node link degree≥10.

$B=\{b_1,b_2,b_3\}$, which represents test object set with three test objects, i.e. web service, threat, topology respectively.

$M=\{SRT,TST,NLD,TRT\}$, which represents test metric set with four metric, i.e. Service Response Time, Threat Sensing Time, Network Link Degree, and Topology Reconstruction Time respectively.

$P=\{p_{SRT},p_{TST},p_{NLD},p_{TRT}\}$, which represents adjusting policy set with four policies respectively, corresponding to Service Response Time, Threat Sensing Time, Network Link Degree, and Topology Reconstruction Time.

$W=\{w_1,w_2,w_3,w_4,w_5,w_6\}$, which represents test method set with six methods, i.e., *SRT*-method based on real network, *TST*-method based on real network, *NLD*-method based on model analysis, *NLD*-method based on real network, *TRT*-method based on model analysis, and *TRT*-method based on real network.

According to the relationships among the six components in Fig. 4, we can get such constraint function in Table II. Because M, B, and P are regarded as a whole, we use M instead of them.

Note: In Table II, when $W\rightarrow S$ in destroyed state, network is not connected, so we cannot use w_4, i.e. *NLD*-method based on real network, to test the metric *NLD*. What's more, we can only metric *TRT* when network is in recovery state as the meaning of Topology Reconstruction Time.

TABLE II.
CONSTRAINT FUNCTION

***M→E*:**	***E→S*:**
$L(SRT)=\{e_1, e_2\}$	$L(e_1)=\{s_2,s_3,s_4\}$
$L(TST)=\{e_2\}$	$L(e_2)=\{s_2,s_3,s_4\}$
$L(NLD)=\{e_1,e_2\}$	***W→S*:**
$L(TRT)=\{e_1,e_2\}$	$L(w1)=\{s_2,s_3,s_4\}$
***W→E*:**	$L(w2)=\{s_2,s_3,s_4\}$
$L(w1)=\{e_1,e_2\}$	$L(w3)=\{s_2,s_3,s_4\}$
$L(w2)=\{e_2\}$	$L(w4)=\{s_2,s_4\}$
$L(w3)=\{e_1,e_2\}$	$L(w5)=\{s_3\}$
$L(w4)=\{e_1,e_2\}$	$L(w6)=\{s_3\}$
$L(w5)=\{e_1,e_2\}$	***M→S*:**
$L(w6)=\{e_1,e_2\}$	$L(SRT)=\{s_2,s_3,s_4\}$
***M→W*:**	$L(TST)=\{s_2,s_3,s_4\}$
$L(SRT)=\{w_1\}$	$L(NLD)=\{s_2,s_3,s_4\}$
$L(TST)=\{w_2\}$	$L(TRT)=\{s_4\}$
$L(NLD)=\{w_3,w_4\}$	
$L(TRT)=\{w_5,w_6\}$	

B. Description of the Test Case

By using the constraint above, we can produce all of the assigning functions of test methods.

$F(e_1,s_2,b_1,SRT,p_{SRT})=\{w_1\}$,
$F(e_1,s_3,b_1,SRT,p_{SRT})=\{w_1\}$,
$F(e_1,s_4,b_1,SRT,p_{SRT})=\{w_1\}$,
$F(e_2,s_2,b_1,SRT,p_{SRT})=\{w_1\}$,
$F(e_2,s_3,b_1,SRT,p_{SRT})=\{w_1\}$,
$F(e_2,s_4,b_1,SRT,p_{SRT})=\{w_1\}$,
$F(e_2,s_2,b_2,TST,p_{TST})=\{w_2\}$,
$F(e_2,s_3,b_2,TST,p_{TST})=\{w_2\}$,
$F(e_2,s_4,b_2,TST,p_{TST})=\{w_2\}$,
$F(e_1,s_2,b_3,NLD,p_{NLD})=\{w_3,w_4\}$,
$F(e_1,s_3,b_3,NLD,p_{NLD})=\{w_3\}$,
$F(e_1,s_4,b_3,NLD,p_{NLD})=\{w_3,w_4\}$,
$F(e_2,s_2,b_3,NLD,p_{NLD})=\{w_3,w_4\}$,
$F(e_2,s_3,b_3,NLD,p_{NLD})=\{w_3\}$,
$F(e_2,s_4,b_3,NLD,p_{NLD})=\{w_3,w_4\}$,
$F(e_1,s_2,b_4,TRT,p_{TRT})=\phi$,
$F(e_1,s_3,b_4,TRT,p_{TRT})=\{w_5,w_6\}$,
$F(e_1,s_4,b_4,TRT,p_{TRT})=\phi$,
$F(e_2,s_2,b_4,TRT,p_{TRT})=\phi$,
$F(e_2,s_3,b_4,TRT,p_{TRT})=\{w_5,w_6\}$,
$F(e_2,s_4,b_4,TRT,p_{TRT})=\phi$.

By using the assigning functions of test methods, we can make these network survivability test subsets described as follows.

$A_{m_1}=f_M(SRT)=\{(e_1,s_2,b_1,SRT,p_{SRT},w_1),(e_1,s_3,b_1,SRT,p_{SRT},w_1),(e_1,s_4,b_1,SRT,p_{SRT},w_1),(e_2,s_2,b_1,SRT,p_{SRT},w_1),(e_2,s_3,b_1,SRT,p_{SRT},w_1),(e_2,s_4,b_1,SRT,p_{SRT},w_1)\}$;

$A_{m_2} = f_M(TST) = \{(e_2, s_2, b_2, TST, p_{TST}, w_2), (e_2, s_3, b_2, TST, p_{TST}, w_2), (e_2, s_4, b_2, TST, p_{TST}, w_2)\}$;

$A_{m_3} = f_M(NLD) = \{(e_1, s_2, b_3, NLD, p_{NLD}, w_3), (e_1, s_2, b_3, NLD, p_{NLD}, w_4), (e_1, s_3, b_3, NLD, p_{NLD}, w_3), (e_1, s_4, b_3, NLD, p_{NLD}, w_3), (e_2, s_2, b_3, NLD, p_{NLD}, w_3), (e_2, s_2, b_3, NLD, p_{NLD}, w_4), (e_2, s_3, b_3, NLD, p_{NLD}, w_3), (e_2, s_4, b_3, NLD, p_{NLD}, w_3), (e_2, s_4, b_3, NLD, p_{NLD}, w_4)\}$;

$A_{m_4} = f_M(TRT) = \{(e_1, s_3, b_4, TRT, p_{TRT}, w_5), (e_1, s_3, b_4, TRT, p_{TRT}, w_6), (e_2, s_3, b_4, TRT, p_{TRT}, w_5), (e_2, s_3, b_4, TRT, p_{TRT}, w_6)\}$.

These above described network survivability test subsets mean how to make tests with six kinds of component information. For example, equation A_{m_3} means, with adjusting policy p_{NLD}, when network is in scene e_1 and in resistance state, survivability measure *NLD* of network topology can be tested by means of w_3 and w_4; and in destroyed state, *NLD* can be tested by means of w_3; and in recovery state, NLD can be tested by means of w_3; and when network is in scene e_2 and in resistance state, *NLD* can be tested by means of w_3 and w_4; and in destroyed state, *NLD* can be tested by means of w_3; and in recovery state, *NLD* can be tested by means of w_3 and w_4.

What's more, we can also calculate the distance of survivability tests λ in test subset A_{m_3}. As a consequence, we can make survivability tests $(e_2, s_3, b_1, SRT, p_{SRT}, w_1)$, $(e_2, s_3, b_2, TST, p_{TST}, w_2)$, and $(e_2, s_3, b_4, TRT, p_{TRT}, w_6)$ performing in parallel because of their shorter inside distances.

We choose a small network environment with three different configurations, and measure the values of survivability metrics under the same network attack. The testing results are shown in Table III, IV and V.

C. Evaluation Results

We can quantitatively evaluate network survivability based on the above testing results by using MADM-based network survivability evaluation method. Firstly, we can build the decision matrixes for every attack course as Table VI.

Then, we can calculate normalized rating for each element in the decision matrixes as Table VII.

We omit the following steps owing to the brevity of the paper. Finally, the sixth step ranks the solutions according to TOPSIS analysis results, which is:

Solution 1> Solution 3> Solution 2

Therefore, the survivability of the measured network under different scenarios is evaluated and the results can be adopted as the network design or optimization considerations.

TABLE III.
TESTING DATA OF NETWORK SURVIVABILITY METRICS UNDER SOLUTION 1

Metrics	Meaning	Value				
		s_1	s_2	s_3	s_4	s_5
SRT	Service Response Time	0.5s	2s	5s	1s	0.5s
TST	Threat Sensing Time	1s	2s	6s	2s	1s
NLD	Network Link Degree	20	16	6	18	20
TRT	Topology Reconstruction Time	-	-	-	2s	-

TABLE IV.
TESTING DATA OF NETWORK SURVIVABILITY METRICS UNDER SOLUTION 2

Metrics	Meaning	Value				
		s_1	s_2	s_3	s_4	s_5
SRT	Service Response Time	0.8s	4s	8s	4s	0.8s
TST	Threat Sensing Time	3s	4s	6s	4s	3s
NLD	Network Link Degree	20	16	6	18	20
TRT	Topology Reconstruction Time	-	-	-	5s	-

TABLE V.
TESTING DATA OF NETWORK SURVIVABILITY METRICS UNDER SOLUTION 3

Metrics	Meaning	Value				
		s_1	s_2	s_3	s_4	s_5
SRT	Service Response Time	0.6s	3s	5s	1s	0.6s
TST	Threat Sensing Time	1s	2s	6s	2s	1s
NLD	Network Link Degree	20	16	6	18	20
TRT	Topology Reconstruction Time	-	-	-	3s	-

TABLE VI.
DECISION MATRIX FOR NETWORK SURVIVABILITY METRICS

	SRT	*TST*	*NLD*	*TRT*
Solution 1	1.8	2.4	16	2
Solution 2	3.52	4	16	5
Solution 3	2.04	2.4	16	3

TABLE VII.
NORMALIZED DECISION MATRIX FOR TOPSIS ANALYSIS

	SRT	*TST*	*NLD*	*TRT*
Solution 1	0.4046	0.4575	0.57735	0.32444
Solution 2	0.79122	0.76249	0.57735	0.81111
Solution 3	0.45855	0.4575	0.57735	0.48666

VI. RELATED WORK

Current research works in the area of network survivability measurement mainly focus on the model of network survivability, the quantification methods of network survivability, the analysis methods of network survivability, and the quantitative assessment methods of network survivability, etc.

Survivability Models. Heegaard and Trivedi [3][4] developed both simulation and analytic models to assess the survivability of a network with virtual connections exposed to link or node failures. The modeling approaches are applied to both small and real-sized network examples. Jindal and Dharmaraja et al. [5] developed an analytical model to determine performance

oriented survivability metrics in terms of call blocking probabilities to quantitatively assess the effect of failures on cellular networks, which assumes Markovian property for the networks and the measures are obtained on solving the proposed Markov model. As an important part of survivability, Madan and Trivedi [22] analyzed quantification of intrusion tolerant systems using a Markov chain model to compute mean time taken to reach failed system states by attack-response graph.

Survivability Quantification Methods. Liu and Trivedi [6] proposed a general survivability quantification approach which is applicable to a wide range of system architectures, applications, failure/recovery behaviors, and desired metrics. Zhao and Wang et al. [8] proposed the PST-based (processing-storage-transmission) survivability system model and the algorithm of PST-based system survivability measure. Bowers and Delcambre et al. [9] introduced adaptation spaces to precisely and predictably specify the adaptation of a software component, and applied adaptation spaces to support Quality of Service and survivability of systems. Kang and Butler et al. [10] presented a new measure for survivability of military communication networks based upon topological structures, which can be used to evaluate and enhance the survivability of military communication networks. Zhang, Wang and Guo et al. [23] presented a survivability quantitative analysis model for network system based on attack graph, which indicated that survivability depends on network system itself, as well as the environment where it's running.

Survivability Analysis Methods. Amiri and Ghassemi-Tari et al. [11] presented a method for transient analysis of availability and survivability of a system with the standby components, and the Markov models, eigen vectors and eigen values are employed for analyzing the transient availability and survivability of the system. Zhao and Cui et al. [12] proposed an effective model for ad hoc network based on stochastic Petri nets, adopted a two-phase approach consisting of the steady-state availability analysis and the system transient performance ana1ysis, and provided a quantitative approach for analysis of the network survivability. Mead and Ellison et al. [13] describes the Survivable Network Analysis (SNA) method developed at the SEI's CERT Coordination Center, which focuses on preservation of essential system services that support the organizational mission.

Survivability Assessment Methods. The Integrated Survivability Assessment (ISA) methodology [14] provides a practical, simple process for assessing the survivability of integrated systems (systems of systems), systems, and/or subsystems with respect to the integrated threat spectrum and/or to individual threats. Keshtgary and Al-Zahrani et al. [15] proposed a composite model for survivability that consists of performance and availability analysis, and constructed a hierarchical model to evaluate the network survivability performance. Chen and Garg et al. [16] modeled the network survivability as a composite measure consisting of both network failure duration and failure impact on the network and proposed a quantitative approach to evaluate wireless ad-hoc network survivability.

VII. Conclusions and Future Work

In this paper, we presented a unified, extensible framework for network survivability testing and evaluation based upon the previous survivability research outcomes, elaborated the customization of network survivability measurement model and the general process of network survivability testing and evaluation. The testing and evaluation framework can be used for different anticipated quantification to obtain the comprehensive understanding of network survivability behaviors under various environments, quantitatively comparing the proposed different survivability architectures, and evaluating the survivability attributes of network. Network survivability testing is performed based upon specific network survivability measurement model, and network survivability evaluation is performed based upon the quantification results of network survivability metrics, and multiple criteria decision making method is utilized to evaluate network survivability.

Future work includes further elaborating the testing and evaluation framework and extending it to provide more network survivability metrics and associated testing methods, collecting the operation data of large scale network and quantitatively evaluating network survivability through multiple evaluation methods, and further validating the efficiency and practicability of the proposed network survivability testing and evaluation framework.

Acknowledgment

The authors would like to thank Prof. Yiqi Dai at Department of Computer Science, Tsinghua University, for providing the guidance of network survivability measurement model that has been used to construct network survivability testing and evaluation framework.

References

[1] R. J. Ellison, D. A. Fisher, R. C. Linger, et al., "Survivable Network Systems: An Emerging Discipline," Technical Report CMU/SEI-97-TR-013, Software Engineering Institute, Carnegie Mellon University, November 1997.

[2] R. Savola, "Towards a Security Metrics Taxonomy for the Information and Communication Technology Industry," Proceeding of International Conference on Software Engineering Advances, 2007.

[3] P. E. Heegaard and K. S. Trivedi, "Network survivability modeling," Computer Networks: The International Journal of Computer and Telecommunications Networking. Elsevier North-Holland, Inc. New York, USA, Volume 53, Issue 8, June 2009, pp. 1215-1234.

[4] P. E. Heegaard and K. S. Trivedi, "Survivability quantification of communication services," In The 38th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Anchorage, Alaska, USA, June 2008.

[5] V. Jindal, S. Dharmaraja, K. S. Trivedi, "Analytical survivability model for fault tolerant cellular networks supporting multiple services," In Proceedings of International Symposium on Performance Evaluation of

Computer and Telecommunication Systems (SPECTS 2006), IEEE Press, Los Alamitos, 2006, pp. 505-512.

[6] Y. Liu and K. S. Trivedi, "A general framework for network survivability quantification," In 12th GI/ITG Conference on Measuring, Modelling and Evaluation of Computer and Communication Systems together with 3rd Polish-German Teletraffic Symposium (MMB & PGTS 2004), VDE Verlag, 2004, pp. 369-378.

[7] Y. Liu and K. S. Trivedi, "Survivability quantification: The analytical modeling approach," International Journal of Performability Engineering, vol. 2(1), 2006, pp. 29-44.

[8] Q. Zhao, H. Q. Wang, G. S. Feng, "A method of processing-storage transmission model-based system survivability measure," Wuhan University Journal of Natural Sciences, Volume 12, Number 1, January 2007, pp. 143-146.

[9] S. Bowers, L. Delcambre, D. Maier, et al., "Applying adaptation spaces to support quality of service and survivability," In DISCEX '00, vol. 2, January 2000, pp. 271-283.

[10] Haizhuang Kang, C. Butler, Qingping Yang, Jiamo Chen, "A new survivability measure for military communication networks," In Proceedings of Military Communications Conference (MILCOM 98), vol.1, October 1998, pp.71-75.

[11] M. Amiri, F. Ghassemi-Tari, A. Mohtashami and J. S. Sadaghiani, "A Methodology for analyzing the transient availability and survivability of a system with the standby components in two cases: The identical components and the non-identical components," Journal of Applied Sciences vol.8(22), 2008, pp. 4105-4112.

[12] J. Zhao, G. Cui, H. W. Liu, H. Q. Wang, "Survivability analysis of wireless Ad hoc network using stochastic reward nets," Journal of Harbin Inistitute of Technology, vol. 15, No. 4, 2008, pp. 535-539.

[13] N. R. Mead, R. I. Ellison, R. C. Linger, T. Longstaff and J. McHugh, "Survivable Network Analysis Method," CMU/SEI-2000-TR-013, September 2000.

[14] G. L. Guzie, "Integrated survivability assessment," ARL-TR-3186, Survivability/Lethality Analysis Directorate, Army Research Laboratory, 2004.

[15] M. Keshtgary, F. A. Al-Zahrani, A. P. Jayasumana, "Network Survivability Performance Evaluation with Applications in WDM Networks with Wavelength Conversion," 29th Annual IEEE Conference on Local Computer Networks, Tampa, Florida, USA, November 2004.

[16] D. Y. Chen, S. Garg, and K. S. Trivedi, "Network survivability performance evaluation: A quantitative approach with applications in wireless ad-hoc networks," In Proceedings of the Fifth ACM International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM'02), Atlanta, GA, September 2002.

[17] M. Duque-Anton, F. Bruyaux, P. Semal, "Measuring the survivability of a network: connectivity and rest-connectivity," European Trans. Telecomunications, vol. 11(2), 2000, pp. 149-159.

[18] W. Fawaz, F. Martignon, K. Chen, G. Pujolle, "A Novel Protection Scheme for Quality of Service Aware WDM Networks," Communications, May 2005.

[19] E. Jonsson, "Towards an integrated conceptual model of security and dependability," In Proc. The First International Conference on Availability, Reliability and Security, IEEE Computer Society, 2006, pp. 646-653.

[20] S. C. Liew and K. W. Lu, "A framework for characterizing disaster-based network survivability" IEEE Journal on Selected Areas in Communications, vol. 12(1), January 1994, pp. 52–58.

[21] L. Ming, D. X. Wang, L. F. Zhang, C. L Wang, et al., "Research on Test Model of Network Survivability", Journal of Computational Information Systems, 2010,6(4), pp.1301-1309.

[22] B. B. Madan, K. S. Trivedi, "Security modeling and quantification of intrusion tolerant systems using attack-response graph", Journal of High Speed Networks, vol. 13(4), 2004, pp. 297–308.

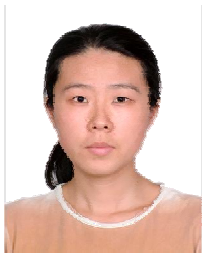
[23] L. J. Zhang, W. Wang, L. Guo, et al., "A Survivability Quantitative Analysis Model for Network System Based on Attack Graph", Proceedings of the Sixth International Conference on Machine Learning and Cybernetics, Hong Kong, 2007, pp. 3211–3216.

[24] T. Yang, C. C. Hung, "Multiple-attribute decision making methods for plant layout design problem", Robotics and Computer-Integrated Manufacturing vol. 23, 2007, pp. 126-137.

[25] K. P. Yoon, C. L. Hwang, Multiple attribute decision making. Thousand Oaks, CA: Sage Publication, 1995.

Chunlei Wang is a Ph.D. Candidate of Computer Science at Tsinghua University, Beijing, China. His research interests include network survivability, trusted network, software security, and program analysis. He received a Master in Computer Engineering from Academy of Equipment Command and Technology in 2002.

Liang Ming is an assistant researcher at National Key Laboratory of Science and Technology on Information System Security of China. His research interests include network survivability, network measurement, and software testing. He received a Ph.D. in Computer Engineering from Machine Engineering College in 2008.



JinJing Zhao is an assistant researcher at National Key Laboratory of Science and Technology on Information System Security of China. Her research interests include network survivability, Inter-domain routing system, complex system theory, and network security. She received a Ph.D. in Computer Science from National University of Defense Technology in 2007.

Dongxia Wang is a researcher at National Key Laboratory of Science and Technology on Information System Security of China. Her research interests include network survivability and network situation awareness. She received a Ph.D. in Computer Science from National University of Defense Technology in 1999.