Progress and Research of Network System Survivability Scheme with Cooperative Information Management

Qingliang Wang, LiFang Zhai, Zheng-Tao JIANG, Yunbing Hou

1 China University of Mining & Technology (Beijing), Beijing, China, 100190
2 Dalian Jiaotong University, Dalian, China, 032302
3 School of Computer Science, Communication University of China, Beijing, 100024
Email: zlf_dl@yahoo.cn

Abstract—Research progress of network survivability during the last few years were briefly introduced, including definitions, methods, qualitative and quantitative survivability evaluation, etc. Technical measures of survivability were summarized. Cooperative survivability and further possible research problems were investigated. Based on the idea of machine learning, survivability information can be got from other systems, and were utilized by the local system to enhance local survivability in time. Some research aspects on cooperative network survivability were summarized. Peers in a system collaborate with each other, which can improve the survivability of the whole systems.

Index Terms—Survivability analysis, System environment, Key service, Machine learning, Cooperative survivability

I. INTRODUCTION

The main goal of early network is to provide simple function that can guarantee the availability of quality of service. The requirements and dependence on network expand the system failure caused by invasion or other external factors [1]. The destructibility of network failure primarily is caused by two factors: One is that real world relies more on information networks; the second is the vulnerability of information networks itself. Security mechanism in face of the new problems exposes more vulnerability, and it is extremely difficult to ensure that the system is not damaged. The existing security and reliability mechanism mostly concentrate on the research of taking measures before successfully attack [2]. Therefore it is necessary to ensure that the system remains to provide key functions after being attacked, which is important to improve the dependability of network services.

Network survivability began to attract widespread attention in the early 90s. B. A. Hollway et al first proposed the concept of "survivability" of information systems in 1993 [3]. Based on related research fields (such as safety, fault tolerance, reliability, etc), they introduced new ideas that system can recover key functions and continue to provide users with acceptable quality of network service. At present, the life cycle model of software development has not got enough attention in system survivability. It is usually regarded as an independent plan or extra feature. Systematically study on the mechanism of survivability contributes immensely to integrate all aspects of attribute in system [4].

Early studies often take survivability as an additional subordinate attribute, and did not pay enough attention to it. Therefore, improving the survivability of network system often gets half the results with twice effort.

In China, concerns on network survivability increases gradually year by year. Figure 1 shows a rough statistics of the number of research projects on network survivability supported by the National Natural Science Foundation during the years of 2003 to 2007[5].

![Figure 1. NSF network survivability research in China.](image)

During the last three years (08, 09, 10), there are 2, 5 and 4 research projects respectively closely relating to network survivability. At present survivability research mainly includes the following aspects: accurate definition of survivability, survivability system structure and its characteristics, the realization of the survivability mechanism, system analysis and quantitative evaluation, network survivability protection technology, etc. This manuscript summarizes and analyzes the above aspects of network survival research progress and existing problems, and further investigates on coordinate system survival mechanisms method to improve the dependability of network services.
II. SURVIVABILITY DEFINITION AND ARCHITECTURES

Early researches about survivability were based on graph theory [6]. Currently there are many different definitions on survivability.

R. J. Ellison defines survivability as the ability of systems to finish the key task when it suffers from an attack, failure or accident [7], and points out four principles of survivability: 1) Resisting intrusion; 2) Identification (of the consequences of intrusion); 3) Recovery (of key services after successful attacks); 4) Adaptability (to improve the survivability of their own systems with knowledge getting from former intrusion events). In 1993, P. G. Neumann defines the survivability of network systems, namely in any adverse conditions, computer communication systems continue to meet the demand of users, including safety, reliability, real-time response and correctness, etc [8].

S. Jha et al defined survivability as an ability that systems maintain key services under abnormal events, such as failure, invasion, etc [9]. From these definitions of the survivability, we can see that what survivability most concerns about is to deal with the consequences of attack and to appropriately control the system. To accurately describe survivability, survivability grading standard as for systems are needed.

S. D. Moitra etc think survivability as the degree of systems that can resist single or multiple attacks and can still run in a certain state level after being attacked. They give a quantitative definition:

SURV = The performance level of a new state / Normal performance level.

This definition introduced another important problem that is how to grade the performance [10].

Another problem on survivability is to identify the key services and support key attributes of these services.

D. Medhi studied the survivability of large-scale heterogeneous information system that is composed of different services. They focused especially on network physical attacks. The ultimate aim of the study is to optimize network resources, and minimize network congestion when facing with a serious attack [11]. D. Medhi divides survivability technology into three categories: prevention, network design, communication management and recovery. This classification helps to deploy specific survival mechanisms. He points out that the survivability of the network design often refers to the survivability strategy during the network design stage, but in practice diversity is usually replaced by redundancy to improve the network survivability.

W. Li et al introduced a new web service to support continuous operation in the event of failure or suffered from security attacks. The technology they used is replication mechanism and N-Modular Redundancy. Mechanism Updating was not discussed in that web service, so its application will be limited [12].

H. Shrobe etc. described a middleware system AWDRT on the application of new and legacy information survivability. "AWDRT" stands for structure difference, packaging, diagnosis, recovery, adaptive software and trust modeling [13]. AWDRT diagnoses the damaged resources and inputs this assessment to its trust model. Finally, once the abnormal behavior was found, it enables rollback and redundant data to recover the target system. AWDRT recovery mechanism continuously provides service from the fail point of application, but it did not distinguish time-sensitive service mechanism. In addition, AWDRT predefined an expected behavior model of the designers’ target system to test abnormal behaviors. With the continual emergence of new applications, behavior patterns will be continuously updated. AWDRT will consider many behaviors as abnormal behaviors, so it affects the accuracy of detection.

III. SURVIVABILITY REALIZATION MECHANISM AND METHODS

Survivability is not a new concept; it is trying to integrate traditional separate technologies together to ensure that the system has an ability to provide critical services even in accident environments. Survivability concerns on the performance of the whole system, but it needs to consider functions provided by various components. This brings the complexity of definition, implementation, analysis and description of the environment. It is also a reason that the survivability research progress is comparatively slow.

The current technical measures to protect the survivability mainly include:

- **Physical isolation**: to prevent any possible test and intrusion;
- **Authentication**: to ensure that only authorized users can access system (such as passwords, identity, certificate, biological recognition, etc.);
- **Access control**: to ensure that anyone who enters the system members have appropriate permissions (such as access control list, application-oriented access control policy);
- **Encryption**: to prevent unauthorized reading of data;
- **Message filtering**: to prevent the inflow of illegal data;
- **Survivability encapsulation**: to control the number of abnormal behaviors;
- **Defensive code**: guarantee the code without defects and mistakes; check the return value before calling other interfaces and functions;
- **Detection**: to find abnormal behavior entering the system;
- **Integrity check**: to detect data modification;
- **Tolerance**: to guarantee the normal operation of system’s key services when suffer invasion (such as fault tolerance, intrusion tolerance);
- **System diversification**: increasing the difficulty of capturing all systems;
- **Functional separation**: to reduce or eliminate the relationship of logical dependencies between services;
- **Critical service and non-critical service separation**: to reduce key service’s dependence on non-critical service;
- **Component redundancy**: to avoid the damage of the whole system by a component’s destruction;
Data replication: to ensure the availability of data after being destroyed;
System rollback and recovery: the system can return to normal state when problems occur;
New invasion activity identification: to identify new intrusion activities and take defense strategies. If there is a suspicious behavior, it immediately verifies its credibility.

The above technologies are now commonly used to ensure the survivability of network systems, but their realizations are different. Therefore, to realize system’s survivability, one first needs to distinguish critical services from non-critical services, to distinguish critical attributes and non-critical attributes, and to define the minimum quality level of these attributes and key objectives. The key attributes need to include the specified time, the accurate time required etc. These different attributes’ indexes also need to be balanced in considering money expense.

R. J. Ellison etc proposed network analysis method (SNA) to analyze distributed network system’s survivability [14]. The steps of their method include system tasks, system architecture definition, the definition of key capabilities, damaging ability definition, the survivability analysis of structure weaknesses. In the process of planning the network system and its structure, they use a systematic method to achieve and enhance the survivability of network system.

Generally speaking, the existing survivability research on network system is mainly about warning and response mechanism, and it still needs further improvement in the following research areas:

① Survivability systems’ abnormal behavior detection mechanism needs to distinguish malicious behaviors from normal behaviors.
② Rank and classification mechanism classifies malicious behaviors and evaluates severity (influence degree, scale and duration, event correlation, etc).
③ Service management module analyzes different level of services influenced by malicious behavior;
④ Policy enforcement mechanisms adopt different strategies of the survivability according to the type of malicious behavior, the extent and criticality of the affected services.

To achieve the goal of providing critical services continuously, the primary task of survival mechanisms is to reduce the impact of failure and to recover system function, rather than to identify reasons for failure. In addition the composition of the system also has significant impact on survivability, such as power law network has the ability to resist random destruction, but weak ability on targeted destruction. Random network has the ability to resist the intended destruction, but weak ability on random destruction.

For single-link failures, the most direct and reliable method is doubling network resources, but the price of this approach is very high. In [15], based on linear programming theory, H. Kervin proposed the communication strategy to resist single link failure from the topology and scale perspective. The basic idea of it is to design necessary topology structure. This method enables the network to support all communications requirements and to guarantee full recovery of connections. Under the assumption of unit load price and certain configuration expense in each link, it satisfies all communication demand with the minimum cost. To realize problem decomposition process one must know the whole connections and failing connection topology. It needs global connection information if connection relationship is changed [15].

IV. SURVIVABILITY EVALUATION AND ANALYSIS METHOD

A. Qualitative Analysis

H. Kalyoncu etc defined the survivability measurement through the minimum possibility of connections. They defined dependence recursively by deleting edges of undirected graphs and changing corresponding probability [16].

Different environment determines different demand of the survivability. For different attacks, requirements for survivability and the type of recovery is different. In addition, if the same attack aimed at different target, the consequence is not the same. Defining different weights of key services will help the implementation of survival mechanisms [17].

The same system towards different attackers needs different survival properties. According to different environment one can quantitatively define different probability survivability.

A. Zolfaghari etc discussed the expectations and demand of users, pause (run interruption) and survival analysis frameworks. They pointed out that performance goals of survivability will help ensure network performance at a given failure scene at least not degenerate below the predetermined degree. Interruption of the operation was classified into three levels: catastrophic, severe, mild [18].

S. Jha etc investigated the impact of attacks in the graph generated by model checking. This method can be used for reliability analysis, waiting and cost-benefit analysis [9]. They pointed out that survivability analysis is very different from other domains’ analysis technique: First, survivability pays attention on system service; Second, survivability analysis need to handle multidimensional system services, such as functions, fault tolerance, and reliability; In addition, survivability analysis should be service-related. S. Jha described the probability of events using Bayesian networks. By identifying a group of “key” element automatically they calculated the reliability and latency and maximized the survivability in certain conditions.

B. Quantitative Analysis

L. Cloth etc used model checking method and continuous-time markov process to estimate survivability. According to their research, survivability can be recovered under certain conditions. The advantage of this method is that it can be used to calculate some
survivability's parameters, but it also has the disadvantage that the system must list all the atomic states [19].

W. Molisz etc mainly discussed survivability functions of the IP network in the typical routing protocol, and they defined survivability as a probability function describing the percentage of data stream transforming after failure. The survivability attributes include percentage of stream after the failure, the corresponding p-percentile values, and the probability of worst-case, and they also described the survivability function and the corresponding algorithms [20].

H. Kang investigated the survivability of military communication networks quantitatively based on their topology. They supposed that wireless network contact only has two kinds of state: damage or undamaged, each time only a contact is damaged. The benefit of their scheme is to measure the survivability of topological network by means of quantitative methods. The more physical network hops means the worse connecting it is [21].

According to the differences of levels of survivability and cost, system designer should design rational recovery ability according to real situation and specific requirements at the design stage.

Survivability capacity can be described as the level of recovery, the time required for total recovery, the time required for recovery to a specific level, etc. The same restoring result with different recovery methods resulting different resources demand. As in Figure 2, the horizontal axis shows time of recovery, the vertical axis indicates service recovery rate, different recovery curves indicates different energy or source requirements.

Not all systems require the same survivability. One should determine the appropriate system survivability according to actual needs, operating environment, and fund. Therefore, the survivability mechanism design includes idle equipment capacity deployment meeting certain restores constraint condition.

It is difficult to build an integrated survivability protection system. "bucket effect" causes that any management’s decision defect will lead to whole failure of protection system. How to reduce management’s complexity and how improve management’s efficiency is becoming a promising research issue of network survivability.

The survivability strategies should change according to the circumstance and attacks. To support this change, special learning methods are needed to get outside information.

V. COLLABORATIVE SURVIVABILITY MECHANISM WITH LEARNING SKILLS

With the exponentially increase of complexity of the distributed networks, it is difficult to cope with dynamic network security threats. This requires integrated information and technologies to build cooperative systems. The methods and strategies can be learned from other systems.

This section is intended to overcome the existing survivability mechanisms’ shortcomings in knowledge collection, behavior learning, and discuss the corporative mechanisms for survivability. The strategies of ‘learning form others’ for survivability may become a kind of method for increasing the dependability of network.

A. Component Functions for Collaborative Survivability

Currently, the integrity, intrusion detection, alarm and reliable mechanisms are often separated from each other. Such systems cannot find their bugs until they were successfully attacked. The learning ability and knowledge reasoning is the key method for prevent new intrusions.

According to the function of learning components and their relationship, Survival system can be divided into the following modules (Figure 3):

Sensing component: Detecting abnormal changes in the environment, and send outside data to the analysis component;

Abnormal analysis component: to analyze abnormal information from the sensing components and information gathering component, then it sends the analysis data and processing suggestions to management component;

System environment analysis: to analyze system surroundings and application background, and classifies threat attributes and severity levels by characteristics of environment;

System risk assessment: to analyze the possibility of threats based on knowledge reasoning and system defects, and sends the analysis data to management component;
Restriction analysis: it provides complete survivability solutions for survivability mechanism based on the basis of resources, economical and technological conditions;

Management component: it is composed of information processing components and order processing components. Information processing components deals with information received from the analysis components and ranks the severity of incidents. Order processing component sends the corresponding commands to the Execution components based on the severity of the incident;

Survivability control: to choose survivability strategies (such as risk voiding, risk tolerating) based on the knowledge of success/failure cases;

Measures implementation: to guarantee that the system provides key service, and gradually recovers all services;

Execution component: to execute each instruction and to allocate resources according to the order;

Notification component: to notify the appropriate components of other entities to take corresponding defensive measures;

Information collection component: collecting influence of events and corresponding survivability processing methods, and analyzing the correlation between these events’ characteristics and the local components, and send corresponding information to analysis components.

B. Collaborative Survivability Mechanism Description

In the network environment, any single system can not recognize all the threats by itself. Threat discovery by methods of cooperation is a necessary complement for improving survivability. It mainly includes the following several models:

Send/Receive mode:
Sensing component captures information if it recognizes abnormal changes in the environment. Local survival mechanisms put out solutions according to the previous local/collacting successful/fail cases, to ensure continuous service and timely recovery. Then it sends the description of threats and the corresponding successful strategies to other systems. These systems combine this information with local actual conditions to take necessary measures to improve their own survivability.

Active request mode:
When local service suffers from potential threats, its survival mechanism collects similar threats and related measures from other systems. Then it optimizes its survival strategies and improves its own survivability ability.

Defect repairing mechanism:
In order to improve the whole network’s survivability, an entity scans its own defects, and repairs the drawback of the system, and shares protection information with other entities.

The whole collaborative survivability cycle can be divided into the following several stages:
1. Evaluating system resources and potential risks;
2. Identifying the task, key attributes and system environment;
3. Identifying the resources that support the tasks and key attributes;
4. Forecasting potential emergency or risks, analyzing risk characteristics and corresponding measures (if necessary, send active request);
5. To develop appropriate emergency measures according to available threat/measures information and local constraints;
6. Improving local survivability strategies;
7. To inform other related entities with threat characters and corresponding measures.

C. Multi-system Learning and Symbol Computation for Cooperative Survivability Schemes

Symbol notion and definition:

Definition 1. Disjunctive normal form for functions. The symbol $\lor$ denotes the union of functions or information of different systems.

Definition 2. Function set. $\Omega(X)$ denotes the full set of functions to be investigated. $A(X)$ represents the set of functions of system $A$ that belong to $\Omega(X)$. $A(x)$ represents the function $x$ of system $A$.

Definition 3. Function inclusion. $A(X) \subseteq B(X)$ denotes that all functions of system $A$ belong to $B$.

So one has the follows properties:
1) $\Phi \subseteq A(X)$;
2) If $A(X) \subseteq B(X)$, $B(X) \subseteq C(X)$, then $A(X) \subseteq C(X);$ 
3) If $A(X) \subseteq B(X)$, $B(X) \subseteq A(X)$, then $A(X) = B(X)$.

Definition 4. Survival information inclusion. $A(X)$ or $A_i(X)$ represents that $A$ or $A_i$ provides survival information about $X_i \subseteq X$.

Note: when the function $x$ of system $B$ is attacked (denotes $B_a(x)$), then to recover the normal function $B(x)$, $B$ needs information on $A(x)$. Here it is supposed that $B$ can utilize full information of $A(x)$.

Theorem 1. For the function $x \in X$ and attack $a$, the sufficient condition for recovering $B_a(x)$ from $B(x)$ is $\exists A_i$ and $n \in \mathbb{Z}^+$, such that $x \in \lor_{A_i(X)} A_i(X)$

Proof. Under the condition that $B$ has global learning ability, $B$ can find $A_i(x)$ from the set $\Psi$. So $B$ can recover to $B_a(x)$.

In fact, the probability to recover $B_a(x)$ is closely related to its communication capability and the size of set $\Psi$. The more convenience of $B$ to communicate with other system node, the more opportunities for $B$ to get survival information of $x$.

In order to recover the service $x$, the quality of this cooperative scheme can be evaluated as:

$$\eta_x = \frac{\#\{ \lor_{A_i(X)} A_i(x) | x \in A_i(X) \}}{\#\{ \lor_{A_i(X)} A_i(x) \}}$$

Under the condition of $x \in \lor_{A_i(X)} A_i(x)$, the more sets $A_i(X)$ such that $x \in A_i(x)$, the more chances to recover $B_a(x)$.
From theorem 1, to insure system survivability, one can improve the global communication capability (such as to shorten path length and increase clustering coefficient with small world) or construct necessary survival information set $\Psi$ that easy to achieve.

D. Issues in the Progress of Collaborative Survivability

Network collaborative survivability involves resources, environment, techniques, and other elements, while single attribute is not sufficient to solve this problem. Meanwhile, the industry of many famous manufacturers also aimed at various survival technologies, and developed different technical solutions [22]. They try to realize the unified management and deploy multiple products, thereby reduce the management cost and improve the overall protection strength. But the current work of integrated management and coordination monitoring research is still not perfect, and it still cannot meet the protection needs of complex network environment.

Academic research work focuses on collaborating different safety technologies to meet the need of specific survival, but lack of unified and integrated management. There is no dominant theories and techniques for survivability, so it is necessary to strengthen research in this area.

In view of limitations of the network collaborative survivability study, the following research issues needs to be strengthened:
1) to set up formal models for comprehensive survivability management monitoring, and describe integrated management and cooperation mechanism. And then to construct the theoretical foundation for integrating a variety of safe and reliable technologies;
2) to establish an effective integrated management and monitoring system architecture. In order to meet the requirements of integrated management, cooperative mechanism should be optimized from the perspective of the overall architecture;
3) to establish automatic adaptive monitoring mechanism among multiple systems. It should have the ability to solve the survival problems by automatic collaborative protection with dynamic changes of environment;
4) to design effective technology to support integrated management and collaboration in a complex system;
5) to improve the existing survivability monitor ability, and to investigate new monitor technologies meeting distributed computing environment.

It will be significant for enhancing collaborative protection and constructing integrated survivability management for network system.

VI. CONCLUSIONS

This paper systematically describes the survivability of the network in recent year. It summarized technical measures for improving survivability in the open environment, in which single functional mechanism(safety or reliability) is not sufficient to ensure a system. So it’s necessary to introduce research on the collaborative mechanism of survivability that will improve information sharing and self-repair ability. By optimizing the survivability mechanisms, it can improve the reliability and survivability of the whole network service system.

Compared with the growth of network scale and application, the research progress on system’s survivability is relatively slow. With the increasing of reliance on information and network systems, it is necessary to improve new collaborative theory models and technical realizations.

ACKNOWLEDGMENT

This research is supported by Beijing Municipal Natural Science Foundation(4112052), Beijing Municipal Special Fund for Cultural and Creative Industries(2009), National “211” Development Fund for Key Engineering Programs and Engineering Programming of Communication University of China.

REFERENCES


