TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 31/49 pp175-179
Volume 12, Number S1, July 2007

A Novel Formal Analysis Method of Network Survivability Based on Stochastic Process Algebra*

ZHAO Guosheng (赵国生)[1,2,**], WANG Huiqiang (王慧强)[2], WANG Jian (王 健)[2]

1. Center of Computer Network and Information, Harbin Normal University, Harbin 150001, China;
2. Institute of Computer Science and Technology, Harbin Engineer University, Harbin 150001, China

Abstract: Stochastic process algebras have been proposed as compositional specification formalisms for performance models. A formal analysis method of survivable network was proposed based on stochastic process algebra, which incorporates formal modeling into performance analysis perfectly, and then various performance parameters of survivable network can be simultaneously obtained after formal modeling. The formal description with process expression to the survivable network system was carried out based on the simply introduced syntax and operational semantics of stochastic process algebra. Then PEPA workbench tool was used to obtain the probability of system's steady state availability and transient state availability. Simulation experiments show the effectiveness and feasibility of the developed method.

Key words: formal analysis; stochastic process algebra; network survivability; performance analysis

Introduction

At present, survivability has been a new research direction of network security technology. The definitions of survivability have been introduced by previous researchers[1,2], which define survivability as the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents. The system is in the broadest possible sense, including networks and large-scale systems[3]. In the area of survivability, the formal modeling technology is the most important foundational work, which may carry out the precise description and formal analysis for the dynamic behavior of network system through the standard formal language. The final goal of formal modeling is to perform the qualitative and quantitative analysis for the network system described. However, so far this field is being at the exploration stage. The existing most formal modeling methods aim at local network or specific system[4]. The paradigm that can simultaneously unify the qualitative and quantitative analysis into the formal modeling has not been found in existing research.

The European reliability research group[5] firstly remarked on the facet of survivability formalization, starting the 'X-key application' project. Although the 'X' may be one all-embracing characteristic, the formal method developed by this project was only applied in the fault-tolerant field until now. Westmark[6] proposed a formal description template of survivability from the angle of the smallest rank of service capability provided by network system in face of threat. Knight and Sullivan[7] gave a kind of survivable formalization description with sextuple, which is not precise enough to support an engineering approach to the survivability analysis of actual network system. Ellison[8] took service as the center, descriptively defined the survivability using finite state machine (FSM). Park and Chandramohan[9] introduced UML language to carry on the formal description of the survivability. Koroma and Li[10] introduced Semi-Markov process to formalize the survivability, but he only defined the paradigm

Received: 2007-02-01

* Supported by the Specialized Research Fund for the Doctoral Program of Higher Education (No. 20050217007)

** To whom correspondence should be addressed.
E-mail: zhaoguosheng@hrbeu.edu.cn; Tel: 86-451-88060155

system not the abstract system. Above several typical formal modeling methods mostly belong to conceptual description, which are difficult to be applied in the qualitative or quantitative analysis of survivability if they do not have a great many following work to do.

In the analysis of survivability, the existing literatures are mostly either qualitative or quantitative analysis. CMU/SEI proposed a representative SSA[11] method, which firstly divided the system into a security nucleus that cannot be broken and a restorable part, in view of certain attack pattern, gave the corresponding resistance, recognition, and recovery strategy, but it is merely a qualitative analysis method. Moitra and Konda[12] have developed a set of simulation models, which may quantitatively analyze the defense mechanisms and viability of various networks. Kring[13] proposed a kind of analysis framework that can converts the question of survivability analysis into a typical graph question based on the question space transformation idea, but it is a kind of qualitative analysis yet. By viewing service as AND-OR structure，Guo and Ma[14] presented a quantitative analysis method for services survivability based on the concept of configuration.

Because the high-level stochastic modeling methods have perfect performances in the description of system behavior relations and algebraic characters[15], which can also integrate quantitative and qualitative analysis into formal description, they have been gradually widely applied in network security analysis. This paper firstly uses the high-level stochastic formal modeling method to formally model and analyze the survivability of network system.

1 Stochastic Process Algebra (SPA)

The syntax of SPA component, *P*, is represented as

$$P ::= \mathrm{Nil} \mid (a,\lambda).P \mid P+Q \mid P \|_L Q \mid P/L \mid A \qquad (1)$$

Prefix, $(a,\lambda).P$: This represents the process *P* becomes a new one ofter an action, a . The time taken to perform a is described by an exponentially distributed random variable with parameter λ . The rate parameter may also take the value Nil, which makes the action passive in a cooperation.

Choice, *P*+*Q*: A race is entered into between components P and *Q*. If P evolves first, then any behavior of *Q* is discarded and vice-versa. This is often called competitive choice.

Hiding, P/L : Actions in the set *L* that emanate from the component P are rewritten as silent Γ-actions. The actions in *L* can no longer be used in cooperation with other components.

Constant, *A*: It is convenient to be able to assign names to patterns of behavior associated with components. Constants are components whose meaning is given by a defining equation. For example, $A \overset{\text{def}}{=} (a,r)$. A performs *a* at rate *r* forever.

Cooperation, $P \|_L Q$: P and *Q* run in parallel and synchronies over the set of actions in the set *S*. If P is to evolve with an action $a \in S$, it must first wait for Q to reach a point where it is also capable of producing an a-action, and vice-versa. In cooperation, the two components then jointly produce an a-action with a rate that reflects the slower of the two components.

2 Formal Modeling

One of the main advantages of stochastic process algebras is that it allows the creation of highly modular model descriptions. It may also accurately describe process behaviors and mutual relationships among system modules. Obviously, using stochastic process algebras to formalize the survivable network system is suitable. The structure of survivable network system usually involves a service request module and a server module that provides different services to relevant users as redundant way. So, in our research, we can consider our survivable system as the parallel composition of two components or processes (as shown in Fig. 1). System initial state can be illuminated as

$$\text{System} := \text{Request} \|_A \text{Server} \qquad (2)$$

where $\boldsymbol{A} := \{\text{key\_job}, \text{non\_key\_job}, \text{fail}\}$.

The process request represents the system loads caused by the different service quest, which the legal users and the attackers claim. The mainframe itself is modeled by the server process.

2.1 Request module modeling

Referring to the definition of survivability described by CMU/SET[3], we divided the service requests submitted to system into the key service request and the non-key service request. Moreover, we also take the attack request as a part of request module. So, the request module may be described as