Journal of Computer and System Sciences 78 (2012) 1751–1774

Contents lists available at SciVerse ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

An adaptive mode control algorithm of a scalable intrusion tolerant architecture ☆

Tadashi Dohi *, Toshikazu Uemura

Department of Information Engineering, Graduate School of Engineering, Hiroshima University, 1-4-1 Kagamiyama, Higashi-Hiroshima 739-8527, Japan

ARTICLE INFO

Article history:
Received 31 January 2011
Received in revised form 31 May 2011
Accepted 28 October 2011
Available online 26 May 2012

Keywords:
Adaptive mode control
Intrusion tolerance
SITAR
System availability
MTTSF
Semi-Markov modeling
EMC approach
Statistical estimation
Non-parametric algorithm
Security/dependability analysis

ABSTRACT

In this paper we consider an intrusion tolerant system with two detection modes; automatic detection mode and manual detection mode for intrusions, which is called SITAR (Scalable Intrusion Tolerant Architecture), and describe the dynamic transition behavior by a continuous-time semi-Markov chain (CTSMC). Based on the embedded Markov chain (EMC) approach, we derive the steady-state probability of the CTSMC, the steady-state system availability and the mean time to security failure (MTTSF). Especially, we show necessary and sufficient conditions to exist the optimal switching time from an automatic detection mode to a manual detection mode, which maximizes the steady-state system availability. Next, we develop an adaptive mode control scheme to estimate the optimal switching time without specifying the associated probability distribution function, whose idea behind is based on a statistically non-parametric algorithm by means of the total time on test concept. Numerical examples through a comprehensive simulation study are presented for illustrating the optimal switching of detection mode, and investigating the asymptotic property of the resulting adaptive mode control scheme.

1. Introduction

Because Internet is highly vulnerable to Internet epidemics, a lot of attacking events compromise a huge number of host computers rapidly and cause DoS around the Internet. Such epidemics result in extensive widespread damage costing billions of dollars, and countering the propagating worms in time becomes an increasingly emergency issue on the Internet security. The computer network security is designed in several layers. Among them, the security approaches taken in the system layer are quite effective to protect the information resource from various network attack incidents and to realize secure computing environments in our daily life.

Although traditional security approaches which may be categorized into *intrusion-detection approaches* establish proactive barriers such as a firewall, unfortunately, the efficiency of a single barrier is not still enough to prevent attacks from sophisticated new skills by malicious attackers. As the result, the number of network attack incidents is tremendously increasing still now on. In contrast to pursue the nearly impossibility of a perfect barrier unit, the concept of *intrusion tolerance* is becoming much popular in recent years. An intrusion tolerant system can avoid severe security failures caused by intrusion and/or attack, and can provide intended services to users in a timely manner even under attack. This is inspired from traditional techniques commonly used for tolerating accidental faults in hardware and/or software systems, and can provide

☆ This paper is an extended version of the conference paper (Dohi and Uemura, 2010, [4]) presented at The 7th International Conference on Autonomic and Trusted Computing (ATC 2010), Xi'an, China, October 26–29, 2010.

* Corresponding author. Fax: +81 82 422 7025.
E-mail address: dohi@rel.hiroshima-u.ac.jp (T. Dohi).

0022-0000/$ – see front matter © 2012 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.jcss.2011.10.022

the system dependability which is defined as a property of a computer-based system, such that reliance can justifiably be placed on the service it delivers [1].

Much efforts in security have been focused on specification, design and implementation issues. In fact, several implementation techniques of intrusion tolerance at the architecture level have been developed for real computer-based systems. For an excellent survey on this research topic, see Deswarte and Powell [2]. Since the above methods can be categorized by a design diversity technique in secure systems and need much cost for the development, the effect on implementation has to be evaluated carefully and quantitatively. To assess quantitatively security/dependability effects of computer-based systems, reliability/performance evaluation techniques with stochastic modeling are quite effective.

Littlewood et al. [8] applied fundamental techniques in reliability theory to assess the security of operational software systems and proposed some quantitative security measures. Jonsson and Olovsson [6] also developed a quantitative method to study attacker's behavior with the empirical data observed in experiments. Ortalo, Deswarte and Kaaniche [11] used both privilege graph and continuous-time Markov chain (CTMC) to evaluate system vulnerability, and derived the mean effort to security failure. Uemura and Dohi [13,15] focused on the typical DoS (Denial of Service) attacks for a server system and formulated an optimal patch management problem via continuous-time semi-Markov chains (CTSMCs).

Later, the same authors [14] considered a secure design of an intrusion tolerant database system [20,23] with a control parameter to switch an automatic detection mode to a manual detection mode after receiving an attack, and described its stochastic behavior by a CTSMC. Park et al. [12] considered an $M/G/1$ queueing model to model an intrusion tolerant server. Uemura et al. [17] also considered the stochastic behavior of an IMS-based VoIP network system with intrusion tolerance. In this way considerable attentions have been paid to stochastic modeling in security/dependability evaluation of computer-based systems.

In this paper we consider an existing system architecture with intrusion tolerance, called SITAR (Scalable Intrusion Tolerant Architecture). The SITAR was developed in MCNC Inc. and Duke University [22]. The main purpose of this paper is to describe the SITAR with two detection modes; automatic detection mode and manual detection mode by a CTSMC and derive the optimal switching time, which maximizes the steady-state system availability in a continuous time. We also develop a statistically non-parametric algorithm to estimate the optimal switching time without specifying the associated probability distribution function, based on the total time on test concept [3].

The remaining part of this paper is organized as follows: Section 2 describes the related work with this paper. In Section 3 we overview the SITAR and describe the fundamental stochastic behavior of it [9,10]. Section 4 takes the embedded Markov chain (EMC) approach and obtains the representation of an embedded discrete-time Markov chain (DTMC) in the steady state for the CTSMC model. We derive the steady-state probability in the CTSMC by using the mean sojourn time and the steady-state probability in the embedded DTMC. Next we formulate the maximization problem of steady-state system availability in continuous time and show necessary and sufficient conditions to exist the optimal switching time from an automatic detection mode to a manual detection mode. In addition to the availability analysis we analytically derive the mean time to security failure (MTTSF) along with the EMC approach.

In Section 5, we develop a statistically non-parametric algorithm to estimate the optimal switching time, where the total time on test concept is useful to obtain the resulting estimator. We translate the underlying optimization problem on analysis to a graphical one, and derive an estimator of the optimal switching time with the complete sample of the transition time data to an automatic detection mode. Numerical examples are presented in Section 6 for illustrating the optimal switching of detection mode and investigating the asymptotic property of the resulting estimator. Here, we develop a simulator to examine the convergence property of estimators of the optimal switching time and its associated dependability measures. Finally the paper is concluded with some remarks in Section 7. All proofs for mathematical propositions are give in Appendix A.

2. Related work

Madan et al. [9,10] consider the security evaluation of SITAR and proposed a CTSMC model to describe the dynamic stochastic behavior. More precisely, they investigated effects of the intrusion tolerant architecture under some attack patterns such as DoS attacks. Based on the EMC approach, they derived not only the steady-state probability of the CTSMC and the steady-state system availability but also the MTTSF. However, they assumed in their model that all transition times are random variables. Uemura et al. [18] introduced a preventive maintenance time such as a patch release time for the SITAR and showed that releasing a security patch at a suitable (constant) timing enables to improve the steady-state system availability effectively. Though their model is a special case of [10] with a deterministic transition time, introduction of the optimal patch release policy by maximizing the steady-state system availability is a new idea. Wang et al. [21] developed a stochastic reward nets (SRNs) model for the SITAR. Fujimoto et al. [5] also considered the similar model as [18] by means of Markov regenerate stochastic Petri nets (MRSPNs) which belong to a wider class of stochastic process than CTSMCs.

On the other hand, recently, the same authors [16,19] introduced an additional control parameter, called the switching time from an automatic detection mode to a manual detection mode for intrusions, into the SITAR, and showed that the similar effect to increase the steady-state system availability can be obtained by controlling the switching time. However, it is worth noting that they assumed the discrete-time operation of the SITAR and developed a discrete-time semi-Markov chain (DTSMC) model. The basic idea on switching from an automatic detection mode to a manual detection mode of vulnerability is due to [14,23] in the context of an intrusion tolerant database system.