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

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. 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 of 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.
In contrast, we consider the same problem in continuous-time setting and develop a CTSMC model. Based on the EMC approach, we derive not only the steady-state probability of the CTSMC and the steady-state system availability but also the MTTSF. In addition to the difference between CTSMC and DTSMC, there are no work on the statistical estimation algorithm on the optimal switching time from an automatic detection mode to a manual detection mode for intrusions, into the SITAR. The statistical estimation scheme proposed here can be used for scheduling of mode change under the incomplete knowledge of intrusion-detection time under autonomic mode control [7]. In other words, it provides an adaptive control scheme of intrusion-detection function within an intrusion tolerant system. In COTS (commercial-off-the-shelf) distributed servers like SITAR, the intrusion-detection function equipped for a proactive security management is not perfect and is often switched to a manual detection mode, in order to detect intrusions/vulnerable parts more speedy (see [14,23]). Then this algorithm would be quite useful because it is not so easy to identify the transition probability in the real-time operation of SITAR. This paper is the complete version of our conference paper [4] with the detailed mathematical proofs and extensive simulation results.

3. SITAR

The SITAR is a COTS distributed server with an intrusion tolerant function [22] and consists of five major components; proxy server, acceptance monitor, ballot monitor, adaptive reconfiguration module, and audit control module. Since the usual COTS server is vulnerable for an intrusion from outside, an additional intrusion tolerant structure is introduced in the SITAR. Fig. 1 shows the configuration of SITAR. It can be checked that the part denoted by a dotted square can function as an intrusion tolerance to the vulnerable end servers $S_1, S_2, \ldots, S_i$, where $P_i$, $B_i$ and $A_i$ in the functional blocks are the logical functions to be executed to satisfy a given service request.

Proxy servers represent public access points for the intrusion tolerant services being provided (e.g. a decision support system for military command and control, or a transaction processing system for an E-commerce site). All requests come into one of the proxy servers depending on the service needs. The proxy server enforces the service policy specified by the current intrusion tolerant strategy. The policy determines which COTS servers the request should be forwarded to, and how the results from these servers should be adjudicated to arrive at the final response. A new request by the proxy server to the appropriate COTS servers is made on behalf of the original client, as depicted by the thin lines from the proxy servers to the COTS servers. Relevant ballot monitors and acceptance monitors are also informed of this decision.

When the responses (signified by the thick lines from right to left) are generated by the COTS servers, they are first processed by the acceptance monitors. The acceptance monitors apply certain validity check to the responses, forwarding them to the ballot monitors along with an indication of the check result. The acceptance monitors also detect signs of compromise on the COTS servers and produce intrusion triggers for the adaptive reconfiguration module. The ballot monitors serve as “representatives” for the respective COTS servers and decide on a final response through either a simple majority voting or Byzantine agreement process. The actual process taken will depend on the current level of detected security threat. The final response is forwarded to the proxy servers to be delivered to the remote client. The adaptive reconfiguration module receives intrusion trigger information from all other modules, evaluates intrusion threats, the tolerance objectives, and the cost/performance impact, and generates new configurations for the system. Since it is assumed that any individual component can be compromised, the backup adaptive reconfiguration module is provided to guard against the adaptive reconfiguration module becoming a single point of failure.
The audit control module provides means for auditing the behavior of all the other components in the intrusion tolerant system. All system modules maintain audit logs with signature protection. These logs can be verified through the audit control module. Additional diagnostic tests can be conducted through the audit control module. Intrusion triggers are distributed among three sets of modules. The triggers in the acceptance monitors are responsible for detecting compromised COTS servers. The triggers in the proxy servers are for detecting external attacks, and the triggers in the audit control will help the security administrator to monitor the secure operation of all the new functional blocks in our architecture through active auditing.

Madan et al. [9,10] described the stochastic behavior of SITAR by means of CTSMC and gave its embedded DTMC representation. Fig. 2 depicts the block diagram of SITAR behavior under consideration. Let $G$ be the normal state in which the COTS server can protect itself from adversaries. However, if a vulnerable part is detected by them, a state transition occurs from $G$ to the vulnerable state $V$. Further if adversaries attack the vulnerable part, the state moves to the attack state $A$. On the other hand, if the vulnerable part is detected by vulnerability identifiers such as benign users, the vulnerable state $V$ goes back to the normal state $G$ again.

In the attack state $A$, two possible states can be taken. If the problem caused by the attack cannot be resolved and the containment of the damaged part fails, the corresponding event can be regarded as a security failure, and the initialization/reconfiguration of the system is performed as a corrective maintenance (repair) at $DL$. After completing it, the system state makes a transition to $G$ again and becomes as good as new. While, if the intrusion/attack are detected, then the state goes to $C$. In the state $C$, one of two instantaneous transitions without time delay, which are denoted by dotted-lines in Fig. 2, can occur, i.e., if the damaged part by attacking is not so significant and does not lead to a serious security failure directly, the system state makes a transition from $C$ to $MC$ with probability $1-p$ ($0 \leq p \leq 1$), and the damaged part can be contained by means of the fail safe function. After the containment, the system state moves back to $G$ by masking the damaged part.

Otherwise, i.e., if the containment of the damaged part with serious effects to the system fails, the state goes to $TR$ with probability $p$. We call this probability the triage probability in this paper. In the triage state $TR$, several corrective inspections are tried in parallel with services. If the system is diagnosed as security failure, the state moves to $F$, the service operation is stopped, and the recovery operation starts immediately. After completing the recovery from the failure, the system becomes as good as new in $G$. Otherwise, it goes to the so-called non-failure state denoted by $C_2$. Here, two states can be taken; it may be switched to the gracefully service degradation in $GD$ with probability $q$ ($0 \leq q \leq 1$), or the service operation is forced to stop and the corrective maintenance starts immediately.

The main differences from Madan et al. [9,10] are (i) an automatic intrusion-detection can be switched to a manual detection mode at any timing in $A$, although Madan et al. [9,10] did not take account of switching of automatic detection mode, (ii) in two states $C$ and $C_2$ instantaneous transitions are allowed in the present model, although Madan et al. [9,10] assumed random transitions with time delay. We define the time interval from $G$ to $G$ as one cycle and suppose that the same cycle repeats again and again over an infinite time horizon. For respective states, let $F_{i,j}(t)$ ($i, j \in \{G, V, A, DL, C, MC, TR, C_2, FS, GD, F\}$) denote the continuous transition probability distributions with probability density function (p.d.f.) $f_{i,j}(t)$ in CTSMC, where the mean is given by $\mu_{i,j}$ ($>0$).

In Fig. 3, we give the transition diagram of CTSMC. It is assumed that the automatic detection function in SITAR is switched just after $t_0$ ($\geq 0$) time unit elapses in an active attack state $A$ in CTSMC. More specifically, let $F_{A,DL}(t)$ be the
transition probability from $A$ to $DL$ which denotes the manual detection mode. When it is given by the step function, i.e., $F_{A,DL}(t) = 1$ \((t \geq t_0)\) and $F_{A,DL}(t) = 0$ \((t < t_0)\), the switching time from an automatic detection mode to a manual detection model is given by the constant time $t_0$ (decision variable). From the preliminary above, we formulate the steady-state system availability as a function of the switching time $t_0$ in the following section.

4. Probabilistic analysis

4.1. EMC approach

The embedded DTMC representation of CTS MC is illustrated in Fig. 4. Let $p_k$, $h_k$ and $\pi_k$ denote the steady-state probability of CTS M C in Fig. 3, the mean sojourn time and the steady-state probability of the embedded DT MC in Fig. 4, respectively, where $k \in \{G, V, A, DL, MC, TR, FS, GD, F\}$. From the definition, we can derive the steady-state probability $\pi_k$ of CTS M C by

\[
\begin{align*}
\pi_G &= h_G / \phi, \\
\pi_V &= h_V / \phi, \\
\pi_A &= p_A h_A / \phi, \\
\pi_{DL} &= p_A (1 - p_{MC} - p_{TR}) h_{DL} / \phi, \\
\pi_{MC} &= p_A p_{MC} h_{MC} / \phi, \\
\pi_{TR} &= p_A p_{TR} h_{TR} / \phi, \\
\pi_{FS} &= p_A p_{TR} p_{FS} h_{FS} / \phi, \\
\pi_{GD} &= p_A p_{TR} p_{GD} h_{GD} / \phi, \\
\pi_F &= p_A p_{TR} (1 - p_{FS} - p_{GD}) h_F / \phi,
\end{align*}
\]

where

\[
\phi = h_G + h_V + p_A [h_A + (1 - p_{MC} - p_{TR}) h_{DL} + p_{MC} h_{MC} \\
+ p_{TR} [h_{TR} + p_{FS} h_{FS} + p_{GD} h_{GD} + (1 - p_{FS} - p_{GD}) h_F]].
\]
4.2. CTSMC model

From the transition diagram of CTSMC in Fig. 3, we obtain

\[ p_A = \int_0^\infty F_{V,G}(t) dF_{V,A}(t), \quad (11) \]

\[ p_{MC} = p_{MC}(t_0) = (1 - p) F_{A,C}(t_0), \quad (12) \]

\[ p_{TR} = p_{TR}(t_0) = pF_{A,C}(t_0), \quad (13) \]

\[ p_{FS} = (1 - q) \int_0^\infty F_{TR,F}(t) dF_{TR,C_2}(t), \quad (14) \]

\[ p_{GD} = q \int_0^\infty F_{TR,F}(t) dF_{TR,C_2}(t), \quad (15) \]

where

\[ h_G = \mu_{G,V}, \quad (16) \]

\[ h_V = \int_0^t F_{V,C}(t) dF_{V,A}(t) + \int_0^\infty F_{V,A}(t) dF_{V,G}(t), \quad (17) \]

\[ h_A = h_A(t_0) = \int_0^{t_0} F_{A,C}(t) dt, \quad (18) \]

\[ h_{DL} = \mu_{DL,G}, \quad (19) \]

\[ h_{MC} = \mu_{MC,G}, \quad (20) \]

\[ h_{TR} = \int_0^\infty t F_{TR,F}(t) dF_{TR,C_2}(t) + \int_0^\infty t F_{TR,C_2}(t) dF_{TR,F}(t), \quad (21) \]

\[ h_{FS} = \mu_{FS,G}, \quad (22) \]
\[ h_{GD} = \mu_{GD,G}. \]  \hspace{1cm} (23) \\
\[ h_{F} = \mu_{F,G}. \] \hspace{1cm} (24)

and \( \bar{F}_{A,C}(t) = 1 - F_{A,C}(t) \). The steady-state system availability is defined as a fraction of time when the service can be provided continuously. Hence, the formulation of the steady-state system availability is reduced to the derivation of the mean sojourn time at each state. It should be noted that the system down states correspond to states DL, FS and F, so that the steady-state system availability is represented as a function of \( t_0 \) by

\[ AV(t_0) = \pi_G + \pi_V + \pi_A + \pi_{MC} + \pi_{TR} + \pi_{GD} = U(t_0)/T(t_0), \] \hspace{1cm} (25)

where

\[ U(t_0) = h_G + h_V + p_A \left[ h_A(t_0) + p_{MC}(t_0)h_{MC} + p_{TR}(t_0)(h_{TR} + p_{GD}h_{GD}) \right] \]

\[ = H_{G,V} + \int_{0}^{\infty} \bar{F}_{V,G}(t) dF_{V,A}(t) \left\{ \int_{0}^{t_0} \bar{F}_{A,C}(t) dt + \alpha F_{A,C}(t_0) \right\}. \] \hspace{1cm} (26)

\[ T(t_0) = U(t_0) + p_A \left[ \left( 1 - p_{MC}(t_0) - p_{TR}(t_0) \right) h_{DL} + p_{TR}(t_0) \left( p_{FS} h_{FS} + (1 - p_{FS} - p_{GD}) h_{F} \right) \right] \]

\[ = H_{G,V} + \int_{0}^{\infty} \bar{F}_{V,G}(t) dF_{V,A}(t) \left\{ \int_{0}^{t_0} \bar{F}_{A,C}(t) dt + \mu_{DL,G} F_{A,C}(t_0) + \beta F_{A,C}(t_0) \right\}. \] \hspace{1cm} (27)

\[ H_{G,V} = \mu_{G,V} + \int_{0}^{\infty} t\bar{F}_{V,G}(t) dF_{V,A}(t) + \int_{0}^{\infty} t\bar{F}_{V,A}(t) dF_{V,G}(t), \] \hspace{1cm} (28)

\[ \alpha = (1 - p)h_{MC} + p(h_{TR} + p_{GD}h_{GD}), \] \hspace{1cm} (29)

\[ \beta = \alpha + p \left( p_{FS} h_{FS} + (1 - p_{FS} - p_{GD}) h_{F} \right). \] \hspace{1cm} (30)

In the above expressions, \( \alpha \) and \( \beta \) mean that the mean up time and the total mean time from state C to G for one cycle, respectively.

### 4.3. Optimal switching time

Our next concern is to seek the optimal switching time, \( t_0^* \), maximizing the steady-state system availability \( AV(t_0) \) in Eq. (25). Taking the differentiation of \( AV(t_0) \) with respect to \( t_0 \) and setting equal to 0 yield the non-linear equation \( q(t_0) = 0 \), where

\[ q(t_0) = \left\{ 1 + \alpha r_{A,C}(t_0) \right\} T(t_0) - U(t_0) \left\{ 1 + (\beta - \mu_{DL,C}) r_{A,C}(t_0) \right\} \] \hspace{1cm} (31)

and \( r_{A,C}(t) = f_{A,C}(t)/\bar{F}_{A,C}(t) \) is the hazard rate of the transition time from state A to C. We make the following parametric assumptions:

(A-1) \( \alpha + \mu_{DL,G} < \beta \),

(A-2) \( \alpha \mu_{DL,G} < h_{G,V} (\beta - \alpha - \mu_{DL,C}) \).

From the definition it is evident that \( \alpha < \beta \). The assumption (A-1) implies that the sum of mean up time after state C and the mean corrective maintenance time is strictly smaller than the total mean time from state C to G. On the other hand, the assumption (A-2) seems to be somewhat technical but is needed to guarantee a unique optimal switching time. These assumptions were numerically checked and could be validated in many parametric cases. We characterize the optimal switching time maximizing the steady-state system availability as follows:

**Proposition 1.**

(1) Suppose that \( F_{A,C}(t) \) is strictly IHR (Increasing Hazard Rate) under the assumptions (A-1) and (A-2), i.e., \( dr_{A,C}(t)/dt > 0 \).

(i) If \( q(0) > 0 \) and \( q(\infty) < 0 \), then there exists a unique optimal switching time \( t_0^* \) (\( 0 < t_0^* < \infty \)) satisfying \( q(t_0^*) = 0 \). The corresponding steady-state system availability \( AV(t_0^*) \) is given by

\[ AV(t_0^*) = \frac{1 + \alpha r_{A,C}(t_0^*)}{1 + (\beta - \mu_{DL,C}) r_{A,C}(t_0^*)}. \] \hspace{1cm} (32)
(ii) If \( q(0) \leq 0 \), then the optimal switching time is \( t_0^* = 0 \) and the corresponding maximum steady-state system availability is given by

\[
AV(0) = \frac{H_{G,V}}{H_{G,V} + \mu_{DL} p_A}.
\]  

(iii) If \( q(\infty) \geq 0 \), then the optimal switching time is \( t_0^* \to \infty \) and the corresponding maximum steady-state system availability is given by

\[
AV(\infty) = \frac{H_{G,V} + (\mu A, C + \alpha) p_A}{H_{G,V} + (\mu A, C + \beta) p_A}.
\]

(2) Suppose that \( F_{A,C}(t) \) is DHR (Decreasing Hazard Rate) under the assumptions (A-1) and (A-2), i.e., \( dr_{A,C}(t) \leq 0 \). If \( AV(0) > AV(\infty) \) then \( t_0^* = 0 \) otherwise \( t_0^* \to \infty \).

Since \( t_0 \) is a timing from \( A \) to \( DL \) in Fig. 3, the policy \( t_0^* \to \infty \) means that it is always optimal not to switch to the manual detection mode. On the other hand, the policy \( t_0^* = 0 \) implies that it is optimal to switch to the manual detection mode just after state moves to the attack state.

4.4. MTTSF analysis

Next, we derive MTTSF [10,18,19]. Let \( X_a \) and \( X_t \) denote the absorbing states and the transient states in CTSMC. Let

\[
P = \begin{bmatrix} Q & C \end{bmatrix}
\]

be the whole transition probability matrix, where \( Q \) and \( C \) denote the transient and the absorbing probability matrices for \( X_a = \{DL, FS, GD, F\} \) and \( X_t = \{G, V, A, MC, TR\} \) in Fig. 4:

\[
Q = \begin{bmatrix} G & V & A & MC & TR \\ G & 0 & 1 & 0 & 0 & 0 \\ V & 0 & 0 & 0 & 0 & 0 \\ A & 0 & 0 & 0 & 0 & 0 \\ MC & 1 & 0 & 0 & 0 & 0 \\ TR & 0 & 0 & 0 & 0 & 0 \end{bmatrix}
\]  

and

\[
C = \begin{bmatrix} DL & FS & GD & F \\ G & 0 & 0 & 0 & 0 \\ V & 0 & 0 & 0 & 0 \\ A & 0 & 0 & 0 & 0 \\ MC & 0 & 0 & 0 & 0 \\ TR & 0 & 0 & 0 & 0 \end{bmatrix}.
\]

In Eq. (35), \( O \) and \( I \) are the zero matrix whose elements are 0 and the identity matrix, respectively. In Eqs. (36) and (37), it means that \( \bar{p}_A = 1 - p_A, \bar{p}_{MC} + \bar{p}_{TR} = 1 - p_{MC} - p_{TR} \) and \( \bar{p}_{FS} + \bar{p}_{GD} = 1 - p_{FS} - p_{GD} \). Using the mean visit number \( V_i \) and the mean sojourn time \( h_i \) in state \( i \), MTTSF is defined by

\[
\text{MTTSF} = \sum_{i \in X_t} V_i h_i,
\]

where \( V_i \) is the solution of the following simultaneous linear equations:

\[
V_i = q_i + \sum_{j} V_j q_{ji} \quad i, j \in X_t,
\]

and \( q_{ji} \) denotes the elements of \( Q \). For the initial probability vector in Eq. (39), we set

\[
q = [q_0] = [1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0].
\]

Finally, solving Eq. (39) yields the mean visit number:
\[ V_G = \frac{1}{p_A p_{MC}(t_0)} , \quad V_V = V_G , \quad V_A = p_A V_G , \quad V_{MC} = p_{MC}(t_0) V_A , \quad V_{TR} = p_{TR}(t_0) V_A \]

and leads to the analytical derivation of MTTSF.

5. Adaptive mode control algorithm

If the transition probability distribution functions in Fig. 3 are completely known, it is possible to seek the security/dependability measures with the optimal mode switching time. However, in general, it is not so easy to identify the transition behavior of the operational server systems and to know the corresponding probability distribution functions. As the most plausible scenario, suppose that the transition probability distribution functions \( F_{i,j}(t) \) \((i, j \in \{G, V, A, DL, C, MC, TR, C_2, FS, GD, F_i\})\) are unknown, but that the associated transition time data in each transition from state \( i \) to \( j \) are available. Since only the functions \( p_{MC}(t_0) \) and \( p_{TR}(t_0) \) in Eqs. (12) and (13) depend on the decision variable \( t_0 \), it is worth mentioning that the other quantities in Eqs. (11) and (14)-(24) can be estimated directly from the underlying transition time data. So, from Eqs. (12) and (13), it is evident to know that a statistical estimator of \( F_{A,C}(t) \) is needed to estimate the steady-state system availability and MTTSF.

Before developing a statistical estimation algorithm for the optimal switching time, we translate the underlying problem \( \max_{0 \leq t_0 < \infty} AV(t_0) \) to a graphical one. Define the scaled total time on test (TTT) transform [3] of the probability distribution \( F_{A,C}(t) \) by

\[ \phi(\gamma) = \frac{1}{\mu_{A,C}} \int_0^{F_{A,C}^{-1}(\gamma)} \bar{F}_{A,C}(t) \, dt , \]

where

\[ F_{A,C}^{-1}(\gamma) = \inf\{t_0; F_{A,C}(t_0) \geq \gamma\} , \quad 0 \leq \gamma \leq 1 . \]

It is well known that \( F_{A,C}(t) \) is IHR (DHR) if and only if \( \phi(\gamma) \) is concave (convex) on \( \gamma \in [0, 1] \) [3]. After a few algebraic manipulations, we have the following result.

**Proposition 2.** Suppose that the assumptions (A-1) and (A-2) are satisfied. Obtaining the optimal switching time \( t_0^* \) maximizing the steady-state system availability \( AV(t_0^*) \) is equivalent to obtaining \( \gamma^* (0 \leq \gamma^* \leq 1) \) such as

\[ \max_{0 \leq \gamma \leq 1} \frac{\phi(\gamma)}{\gamma^* + c_2} , \]

where

\[ c_1 = \frac{H_{G,V}}{p_A \mu_{A,C}} + \frac{\alpha \mu_{DL,G}}{\mu_{A,C}(\alpha - \beta + \mu_{DL,G})} (> 0) , \]

\[ c_2 = \frac{\mu_{DL,G}}{\beta - \alpha - \mu_{DL,G}} (> 0) . \]

From the above result, it is seen that the optimal switching time \( t_0^* = F_{A,C}^{-1}(\gamma^*) \) is determined by calculating the optimal point \( \gamma^*(0 \leq \gamma^* \leq 1) \) maximizing the tangent slope from the point \((-c_2, -c_1)\) to the curve \((\gamma, \phi(\gamma)) \in [0, 1] \times [0, 1] \) in the two-dimensional plane. This geometrical procedure seems to be very useful to determine the optimal switching time on the graph, instead of solving the non-linear equation in Eq. (31). In addition, it would be interesting to perform graphically the sensitivity analysis of model parameters on the optimal switching time, because the sensitivity can be checked visually and its educational effect to understand the optimal mode control is beneficial.

Next, suppose that the optimal switching time has to be estimated from an ordered complete (uncensored) observation \( 0 = x_0 < x_1 < x_2 < \cdots < x_n \) of the transition times from an absolutely continuous distribution \( F_{A,C}(t) \), which is unknown. Then the scaled TTT statistics [3] based on this sample are defined by \( \psi_{ij} = \psi_j/\psi_n \), where

\[ \psi_j = \sum_{k=1}^{j} (n-k+1)(x_k - x_{k-1}) , \quad j = 1, 2, \ldots, n ; \quad \psi_0 = 0 . \]
Since the empirical distribution function \( F_{nj} \) corresponding to the sample data \( x_j \) \((j = 0, 1, 2, \ldots, n)\) is given by
\[
F_{nj} = \begin{cases} 
  j/n & \text{for } x_j \leq x < x_{j+1}, \\
  1 & \text{for } x_n \leq x,
\end{cases}
\]
the resulting polygon by plotting the points \((F_{nj}, \phi_{nj})\) \((j = 0, 1, 2, \ldots, n)\) and connecting them by line segments is called the scaled TTT plot \([3]\). In other words, the scaled TTT plot can be regarded as a numerical counterpart of the scaled TTT transform.

The following result gives an autonomic mode control algorithm based on the non-parametric estimator for the optimal switching time.

**Proposition 3.**

(i) Suppose that the optimal switching time has to be estimated from \( n \) ordered complete sample \( 0 = x_0 \leq x_1 \leq x_2 \leq \cdots \leq x_n \) from an absolutely continuous distribution \( F_{A,C}(t) \), which is unknown. Then, a non-parametric estimator of the optimal switching time \( t^*_0 \) which maximizes \( AV(t_0) \) is given by \( x_{j^*} \), where
\[
j^* = \left\{ j \mid \max_{0 \leq j \leq n} \frac{\phi_{nj} + c_1}{f/n + c_2} \right\}
\]
and \( \mu_{A,C} \) in Eq. (49) is replaced by \( \sum_{k=1}^{n} x_k/n \).

(ii) The estimator given in (i) is strongly consistent, i.e. \( x_{j^*} \) converges to the (real but unknown) optimal solution \( t^*_0 \) uniformly with probability one as \( n \to \infty \), if a unique optimal switching time exists.

6. Numerical examples

6.1. Preliminaries

In this section we derive the optimal switching time \( t^*_0 \) characterized in Section 3 and quantify two security measures; steady-state system availability and MTTSF. Suppose the following parametric circumstance: \( \mu_{G,V} = 72, \mu_{V,G} = 15, \mu_{V,A} = 24, \mu_{DL,G} = 15, \mu_{MC,G} = 12, \mu_{TR,F} = 6, \mu_{TR,C_2} = 8, \mu_{FS,G} = 30, \mu_{GD,G} = 40 \) and \( \mu_{F,G} = 48 \). Also we suppose that \( f_{A,C}(t) \) is the gamma p.d.f. with shape parameter \( k \) and scale parameter \( d \):
\[
f_{A,C}(t) = \frac{t^{k-1}d^{-k} \exp(-t/d)}{\Gamma(k)},
\]
where \( \Gamma(\cdot) \) denotes the standard gamma function. Especially we concern the following four cases:

(i) Case 1: \( p = 0 \), i.e., the system state makes a transition from \( C \) to \( MC \) with probability one.
(ii) Case 2: \( p = 0.5 \) and \( q = 0.5 \).
(iii) Case 3: \( p = 1 \) and \( q = 0 \), i.e., the service operation at \( C_2 \) is forced to stop with probability one.
(iv) Case 4: \( p = 1 \) and \( q = 1 \), i.e., the gracefully degradation can be observed with probability one.

It is evident from Fig. 2 that Case 1 is an unrealistic case because the attack can be always masked perfectly and the system down does not occur with probability one. In this situation, it is evident to see that the mode switching from an automatic mode to a manual model is not needed, and that the optimal switching time should be always \( t^*_0 \to \infty \). Case 3 and Case 4 correspond to the scenario where the probability that the containment with a fail safe function is triggered is extremely small, and should be considered as the worst case scenario. Especially, Case 4 denotes the case where the fail-secure function does not also work. This is corresponding to the well-known DoS attack with \( G, V, A, DL, TR, GD \) and \( F \), where the states \( MC \) and \( FS \) can be regarded as a security failure state under the DoS attack circumstance \([9,10]\).

In Figs. 5 and 6, we illustrate the behavior of steady-state system availability and MTTSF, respectively. From these figures, we know that Case 3 with many service stops gave lower system availability and MTTSF, and that their decreasing rate was remarkable. Except in Case 1, it is seen that the steady-state system availability is a unimodal function of \( t_0 \), but that MTTSF is a monotonically increasing function in each case. From this fact, increasing the optimal switching time leads to increasing MTTSF which can be regarded as a system lifetime, so that the automatic detection model can work to extend MTTSF. However, if we focus on the availability, there exists an optimal mode switching time maximizing it in the sense of long-run operation.

6.2. Sensitivity analysis

We derive the optimal switching time which maximizes the steady-state system availability for varying failure parameters \((k, d)\). Tables 1 and 2 present the optimal switching time and its associated system availability with varying \( k \) and \( d \) for...
Table 1
Dependence of steady-state system availability on parameter $k$ in continuous-time operation.

<table>
<thead>
<tr>
<th>$k$</th>
<th>Case 1</th>
<th>Case 2</th>
<th>Case 3</th>
<th>Case 4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$t_0^*$</td>
<td>$\Delta (%)$</td>
<td>$t_0^*$</td>
<td>$\Delta (%)$</td>
</tr>
<tr>
<td>1</td>
<td>$\infty$</td>
<td>1</td>
<td>0</td>
<td>0.9337</td>
</tr>
<tr>
<td>2</td>
<td>$\infty$</td>
<td>1</td>
<td>0</td>
<td>1.4240</td>
</tr>
<tr>
<td>3</td>
<td>$\infty$</td>
<td>1</td>
<td>0</td>
<td>5.0032</td>
</tr>
<tr>
<td>4</td>
<td>$\infty$</td>
<td>1</td>
<td>0</td>
<td>9.1387</td>
</tr>
<tr>
<td>5</td>
<td>$\infty$</td>
<td>1</td>
<td>0</td>
<td>13.4647</td>
</tr>
</tbody>
</table>

Case 1–Case 4, where $d = 4$ is fixed in Table 1, $k = 3$ is fixed in Table 2, and ‘$\Delta$’ denotes the increment (%) from the non-switching time case ($t_0 \rightarrow \infty$). It can be shown that the steady-state system availability could be improved, especially, up to 10.6% in Case 3. The main reason why this observation could be obtained was the existence of services frequently stopped in Case 3. In Table 2, it can be seen that controlling the switching time is quite effective, especially, in Case 3. As the value of $d$ increases more and more, i.e., the time to detection of intrusions is much longer, the steady-state system availability monotonically increases.
the function of each module of our simulator in the following:

We develop a simulator is considered as the security failure state, MTTSF decreases arbitrarily by controlling the switching time. Although we out Monte Carlo simulations, we check the convergence of the estimator of the optimal switching time derived in Section 4. Through-
Step 4 (Evaluation): Calculate estimates of model parameters updated in Step 2 and of the optimal switching time \( t^*_0 \) in Step 3. From these values, we calculate estimates of the maximum system availability \( AV(t^*_0) \) and MTTSF \( MTTSF(t^*_0) \). We repeat these steps (Step 2–Step 4) by 800th cycle.

Step 5 (Measurement): The procedure from Step 1 to Step 4 generates only one sample path of an estimate \( \hat{t}^*_0, AV(\hat{t}^*_0) \) or MTTSF(\( \hat{t}^*_0 \)). To evaluate the temporal behavior of these estimates, it is needed to assess the quality of estimation with many samples. From the law of large numbers, it can be expected that these sample behaviors approach to the corresponding real solutions on \( t^*_0, AV(t^*_0) \) or MTTSF(\( t^*_0 \)). Hence, we execute 100 times simulation runs from Step 1 to Step 4, and calculate the arithmetic means of 100 estimates of \( t^*_0, AV(\hat{t}^*_0) \) or MTTSF(\( \hat{t}^*_0 \)) in each cycle.

In Figs. 8–16, we plot the convergence of estimates of the optimal switching time and its related dependability measures, where the cases with 50 and 100 sample paths are calculated with the arithmetic means of the estimates at each cycle, and the a dotted line of all figures is a real solution. It can be observed that the resulting estimates show smoothed curves as the number of samples increases. In fact, in Figs. 8, 11 and 14, the temporal behavior of estimates on \( t^*_0 \) with only one sample fluctuates in Case 2, Case 3 and Case 4, and the resulting estimates do not approach to the real optimal solutions. However, when the number of samples increases, they tend to converge to a certain level. On the other hand, the steady-state system availability and MTTSF approach to the corresponding solutions, and the convergence speed becomes much faster when the number of samples increases. These results imply that it is not sufficient to monitor the operational transition behavior of only one SITAR system. So, it is desired to operate multiple SITAR systems in parallel and monitor the on-line transition behavior in order to get the mode control strategy with higher accuracy.

It may be interesting to know that the convergence depends on each case under consideration. For instance, in Case 1, it is found that \( \hat{t}^*_0 \) converges at around 700–800 cycles, but \( AV(\hat{t}^*_0) \) and MTTSF(\( \hat{t}^*_0 \)) do at around 150–200 and 300–400 cycles, respectively. On the other hand, it is seen that \( \hat{t}^*_0 \) in Case 3 and Case 4 does not converge even at 800th cycle. While, \( AV(\hat{t}^*_0) \) (MTTSF(\( \hat{t}^*_0 \)) in Case 3 and Case 4 converges to the corresponding solutions at around 300–400 and 600–700 cycles (300–400 and 400–500 cycles). In this way, a large amount of statistical data are needed to estimate the real optimal mode switching time and its associated dependability measures. The lesson learned from the simulation study is negative to get the real but unknown optimal mode switching control if the SITAR system is operated independently. In other words, this problem would be resolved by a good deal of parallelism of server management.

7. Conclusion

In this paper we have considered a CTSMC model of an intrusion tolerant system by introducing the switching time from an automatic detection mode to a manual detection mode. We have derived the optimal switching time analytically so as to maximize the steady-state system availability and obtained MTTSF. Also, we have developed a statistical estimation algorithm of the optimal switching time. The lesson learned from numerical examples was that the optimal switching could improve the system availability/MTTSF effectively in some cases. Hence, it has been shown that the combination between
Fig. 8. Asymptotic behavior of \( \hat{t}_0^* \) in Case 2.
Fig. 9. Asymptotic behavior of $AV(\hat{t}_0^*)$ in Case 2.
Fig. 10. Asymptotic behavior of MTTSF($\hat{\tau}_0^*$) in Case 2.
Fig. 11. Asymptotic behavior of $\hat{t}_0^*$ in Case 3.

(a) one sample path.

(b) 50 sample paths.

(c) 100 sample paths.
Fig. 12. Asymptotic behavior of $AV(\hat{t}_0^*)$ in Case 3.

(a) one sample path.

(b) 5 sample paths.

(c) 100 sample paths.
Fig. 13. Asymptotic behavior of MTTSF($\hat{t}_0$) in Case 3.
Fig. 14. Convergence on $\hat{t}_0$ in Case 4.
Fig. 15. Convergence on $AV(\hat{i}_0^*)$ in Case 4.
Fig. 16. Convergence on MTTSF($\hat{t}_0^*$) in Case 4.
an intrusion tolerance architecture and a control of detection mode for intrusions was quite effective to manage the critical computer-based systems. Also, we have made a challenge to estimate asymptotic optimal mode switching strategy and executed a simulation study. When the transition time data can be obtained from the multiple SITAR operations in parallel, e.g., 50 or 100 parallel operations, it is possible to estimate the optimal model switching time accurately. In the future, it will be expected to improve the convergence speed of the estimate proposed in this paper. Then, the kernel-based estimation may be useful to improve the estimation accuracy and the convergence speed.

Acknowledgment

This research was supported by the Ministry of Education, Science, Sports and Culture, Grant-in-Aid for Scientific Research (C), Grant No. 21510167 (2009–2012).

Appendix A

Proof of Proposition 1. Further differentiation of the function \( q(t_0) \) leads to

\[
\frac{q(t_0)}{dt_0} = dF_{A,C}(t_0) \left\{ \alpha T(t_0) - (\beta - \mu_{DL,G})U(t_0) \right\}. \tag{55}
\]

If \( F_{A,C}(t) \) is strictly IHF under (A-1) and (A-2), the r.h.s. of Eq. (55) takes a negative value, that is,

\[
\alpha T(t_0) - (\beta - \mu_{DL,G})U(t_0) = (\alpha - \beta + \mu_{DL,G}) \left\{ H_{G,V} + \int_0^\infty F_{V,G}(t) dF_{V,A}(t) \right\} + \alpha \mu_{DL,G} \tag{56}
\]

is strictly negative. Hence, the function \( q(t_0) \) is a strictly decreasing function of \( t_0 \) and \( AV(t_0) \) is strictly quasi-concave in \( t_0 \). In this situation, if \( q(0) > 0 \) and \( q(\infty) < 0 \), then there exists a unique \( t_0^* \) \((0 < t_0^* < \infty)\) maximizing \( AV(t_0) \), which satisfies the non-linear equation \( q(t_0^*) = 0 \). If \( q(0) \leq 0 \) or \( q(\infty) \geq 0 \), then the function \( AV(t_0) \) decreases or increases, and the resulting optimal switching time becomes \( t_0^* = 0 \) or \( t_0^* \to \infty \). On the other hand, if \( F_{A,C}(t) \) is DHR, the function \( AV(t_0) \) is a quasi-convex function of \( t_0 \), and the optimal switching time trivially becomes \( t_0^* = 0 \) or \( t_0^* \to \infty \). \( \Box \)

Proof of Proposition 2. From the definition in Eq. (48), the steady-state system availability in Eq. (25) is represented as a function of \( \gamma \) by

\[
AV(t_0) = AV(F^{-1}_{A,C}(\gamma)) = H_{G,V}/\mu_{A,C} + p_A(\phi(\gamma) + (1 - \gamma) + (\beta/\mu_{A,C})\gamma) - H_{G,V}/\mu_{A,C} + p_A(\phi(\gamma) + (\mu_{DL,G}/\mu_{A,C})(1 - \gamma)) + (\beta/\mu_{A,C})\gamma) = 1 + \frac{H_{G,V}/\mu_{A,C} + p_A(\phi(\gamma) + (\beta - \mu_{DL,G})\gamma)}{H_{G,V}/\mu_{A,C} + (\beta - \mu_{DL,G})\gamma - \mu_{DL,G}/\mu_{A,C}}. \tag{57}
\]

Hence, it is obvious that maximizing Eq. (57) is equivalent to minimizing

\[
\frac{H_{G,V}/\mu_{A,C} + \mu_{DL,G} + \mu_{A,C}(\phi(\gamma) + (\beta - \mu_{DL,G})\gamma)}{(\alpha - \beta + \mu_{DL,G})\gamma - \mu_{DL,G}} = \frac{\mu_{A,C}}{\alpha - \beta + \mu_{DL,G}} \left\{ \beta - \mu_{DL,G} + \phi(\gamma) + c_1 \right\}. \tag{58}
\]

From the assumption (A-1), the proof of Eq. (48) is completed. From the assumption (A-2) and \( 0 < p_A < 1 \), we have Eqs. (49) and (50). \( \Box \)

Proof of Proposition 3. Since the estimators, \( \phi_{nj} \) and \( F_{nj} \) are the numerical counterparts of \( \phi(\gamma) \) and \( \gamma \), respectively, it is straightforward to hold Eq. (53) in (i) where the population mean \( \mu_{A,C} \) in Eq. (49) is replaced by the sample mean \( \sum_{k=1}^n x_k/n \). In (ii), it is well known that \( \phi_{nj} \) and \( F_{nj} \) are both strongly consistent estimators of \( \phi(\gamma) \) and \( \gamma \), respectively, i.e., \( \phi_{nj} \to \phi(\gamma) \) and \( F_{nj} \to \gamma \) uniformly with probability one as \( n \to \infty \). From the Glivenko–Cantelli theorem, the resulting estimator of the optimal switching time \( t_0^* \) is also strongly consistent [3]. The proof is completed. \( \Box \)

References


