Quantitative Evaluation of Intrusion Tolerant Systems Subject to DoS Attacks via Semi-Markov Cost Models

Toshikazu UEMURA and Tadashi DOHI

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

Abstract. In this paper we quantitatively evaluate the security of intrusion tolerant systems with preventive maintenance subject to DoS (Denial of Service) attacks. More specifically, we develop two semi-Markov cost models and describe the stochastic behavior of two intrusion tolerant systems with different preventive maintenance policies. The optimal preventive maintenance schedules are analytically derived to minimize the long-run average costs. We further perform the sensitivity analysis of the model parameters through numerical experiments. The results obtained here would be also useful to design ubiquitous systems subject to external malicious attacks.

Key words: DoS attack, information security, intrusion tolerance, preventive maintenance, long-run average cost, semi-Markov models

1 Introduction

Recently, since a huge number of information systems are connected by public network like internet and can be accessed by many unspecified people, we often encounter the serious problems on accidental and malicious threats. Once the security intrusion happens, it may lead to not only the leak/destruction of information but also the computer system down. For malicious attackers, if the access right strengthens, the probability that the security intrusion happens will decrease, but the utilization on accessibility will be rather lost. Hence, when the information security systems are designed, it is quite important to take account of both intrusion detection function and intrusion tolerant function. The former strengthens the access right against malicious accesses, the latter tolerates the security intrusion at the minimum risk. In fact, a number of implication techniques of intrusion tolerance at the architecture level have been developed for several real systems [13],[14], e.g., distributed systems [1], middleware [15], database systems [16], server systems [3]. The above approaches are based on the redundant design at the architecture level on secure software systems. In other words, these methods can be categorized by a design diversity technique in secure system design and need much cost for the development. On the other hand, the

environment diversity technique by the temporal time redundancy is a low-cost security tolerance technique. The most plausible examples for applying the environment diversity technique are ubiquitous systems under unspecified operation environment. In this paper we focus on the security design of intrusion tolerant systems with preventive maintenance.

The quantitative evaluation of information security based on modeling is quite effective to validate the effectiveness of information systems with intrusion tolerance. Littlewood et al. [6] found the analogy between the security theory and the traditional reliability theory in assessing the quantitative security of operational software systems and proposed some quantitative security measures. Jonsson and Olovsson [5] discussed a quantitative method to study the attacker's behavior with the empirical data observed in experiments. Ortalo, Deswarte and Kaaniche [9] applied the privilege graph and the Markov chain to evaluate the vulnerability, and derived the mean effort to security failure. Singh, Cukier and Sanders [11] and Stevens et al. [12] considered probabilistic models to verify the intrusion tolerant systems against several attack patterns, and explained theoretically the detection mechanism of system vulnerability. Madan et al. [7], [8] dealt with an architecture with intrusion tolerance, called SITAR (Scalable Intrusion Tolerant Architecture) and described the stochastic behavior of the system by discrete-time semi-Markov process. They also derived the mean time length to security failure. Imaizumi, Kimura and Yasui [4] considered an intrusion tolerant system subject to DoS (Denial of Service) attacks (see e.g. [2]) and gave a continuous-time semi-Markov model. They formulated the long-run average cost and derived the optimal monitoring time of illegal access for minimizing it. Recently, VoIP (Voice over IP) network system [10] was modeled by the continuous-time Markov chains from the viewpoint of security design. In this way, several stochastic models have been developed with the aim of quantitative evaluation of information security.

In this paper we focus on the DoS attacks similar to Madan et al. [7], [8] and Imaizumi, Kimura and Yasui [4], and quantitatively evaluate the security of intrusion tolerant systems with preventive maintenance. In the DoS attacks, the attackers detect the vulnerabilities in server applications and make the network traffic increasing extremely by sending a large amount of illegal dada. To protect the information assets from such malicious threats, the preventive maintenance would be useful for tolerating the security faults. The typical example of preventive maintenance is the patch management. If the vendors can know the vulnerable parts in the server applications in advance, they can release the patch before the malicious attackers detect them. In fact, the full vendors or the computer emergency response team/coordination center (CERT/CC) are always monitoring the system vulnerabilities reported by benign users or themselves, even after releasing the applications. More specifically, we develop two semi-Markov cost models and describe the stochastic behavior of two intrusion tolerant systems with different preventive maintenance policies. The optimal preventive maintenance schedules are analytically derived to minimize the long-run average costs. In numerical examples, we derive the optimal preventive maintenance policies

and their associated ling-run average costs, and further perform the sensitivity analysis of the model parameters.

2 Model 1

2.1 Model Description

Figure 1 depicts the transition diagram of Model 1. Suppose that the server system starts operating at time $t = 0$ with Normal State; G. If attackers or hackers detect the vulnerability of a server application, the state makes a transition to Vulnerable State; V, where the transition time from G to V has the continuous cumulative distribution (c.d.f.) $F_0(t)$ with mean μ_0 (> 0). Once the malicious attack by an attacker begins, the system state changes to Attack State; A and the server operation stops for corrective maintenance, where the transition time from V to A is given by a random variable having the continuous c.d.f. $F_a(t)$ and mean μ_a (> 0). In this phase, if the minor corrective maintenance in a failure probable state is performed such as data recovery, the system can be recovered from the failure probable state to the normal one, and can become as good as new. The transition time from State A to State G is given by the generally distributed random variable with the c.d.f. $F_t(t)$ and mean μ_t (> 0). However, the system state may go to System Failure State; F before completing the minor corrective maintenance, where the transition time from A to F obeys the c.d.f. $F_f(t)$ with mean μ_f (> 0). Since this state is the system down state, the major recovery operation such as data initialization or system restart has to be carried out. The completion time to recover the server system from the system failure state is given by the non-negative continuous random variable with the c.d.f. $F_r(t)$ and mean μ_r (> 0).

On the other hand, if the vulnerable state V is detectable by vulnerability identifiers like a benign user, it may be effective to trigger the preventive maintenance before the vulnerabilities are detected by malicious attackers. As a plausible scenario on preventive maintenance, suppose that a benign user discovers the application vulnerability faster than the attackers, and discloses its information to the full vendor or the CERT/CC as well as his or her personal community. Then the patch management is an important issue for the vendor. When the development period of patch is relatively shorter, is the quick release of the patch really beneficial? If the vulnerable state is seldom detected, it would be better to release the patch from the vendor as soon as possible. However, if the similar vulnerable states may come repeatedly, the frequent release of patches may lead to the large overhead in operation. Define Preventive Maintenance State; M. If the preventive maintenance is triggered before the system becomes vulnerable, the system operation is stopped and the state goes to M from V. Without any loss of generality, define the transition time from V to A is distributed with the following c.d.f.:

$$F_m(t) = \begin{cases} 1 \ (t \geq t_0) \\ 0 \ (t < t_0). \end{cases} \tag{1}$$

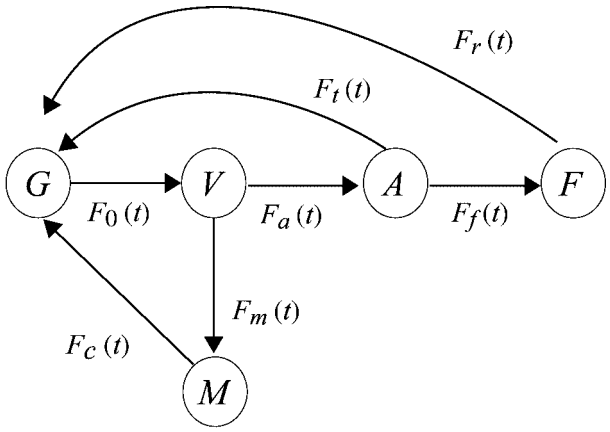

Fig. 1. Semi-Markov transition diagram of Model 1

This means that the preventive maintenance is performed at every t_0 time unit after the vulnerability is detected (this assumption is relaxed in the latter discussion). Once the preventive maintenance starts, it completes after the random time interval with the c.d.f. $F_c(t)$ and mean μ_c, so that the server system can be recovered similar to the state just before the vulnerability is detected. In the scenario of patch management, the time t_0 indicates a trigger to begin developing the patch. The same cycle repeats again and again over an infinite time horizon. Since the underlying stochastic process is a semi-Markov process, we can apply the standard technique to study it.

Define the one-step transition probability of Model 1 and its Laplace-Stieltjes transform (LST) by $Q_{ij}(t),\ i,j \in \{G,V,A,F,M\}, i \neq j$ and $q_{ij}(s) = \int_0^\infty \exp\{-st\}dQ_{ij}(t)$, respectively. Then it is evident to obtain

$$q_{GV}(s) = \int_0^\infty \exp\{-st\}dF_0(t), \tag{2}$$

$$q_{VM}(s) = \int_0^\infty \exp\{-st\}\overline{F}_a(t)dF_m(t), \tag{3}$$

$$q_{VA}(s) = \int_0^\infty \exp\{-st\}\overline{F}_m(t)dF_a(t), \tag{4}$$

$$q_{AG}(s) = \int_0^\infty \exp\{-st\}\overline{F}_f(t)dF_t(t), \tag{5}$$

$$q_{AF}(s) = \int_0^\infty \exp\{-st\}\overline{F}_t(t)dF_f(t), \tag{6}$$

$$q_{FG}(s) = \int_0^\infty \exp\{-st\}dF_r(t), \tag{7}$$

$$q_{MG}(s) = \int_0^\infty \exp\{-st\}dF_c(t), \tag{8}$$

where in general $\overline{\psi}(\cdot) = 1 - \psi(\cdot)$.

Next we define the recurrent time distribution from State G to State G again by $H_{GG}(t)$. Then the LST of the recurrent time distribution is given by

$$\begin{aligned} h_{GG}(s) &= \int_0^\infty \exp\{-st\} dH_{GG}(t) \\ &= q_{GV}(s) q_{VA}(s) q_{AG}(s) + q_{GV}(s) q_{VA}(s) q_{AF}(s) q_{FG}(s) \\ &\quad + q_{GV}(s) q_{VM}(s) q_{MG}(s). \end{aligned} \tag{9}$$

Suppose that the system state is G at time $t = 0$ with probability one. We define the transition probability from G to $j \in \{G, V, A, F, M\}$ at an arbitrary time t (> 0) and its LST by $P_{Gj}(t)$ and $p_{Gj} = \int_0^\infty \exp\{-st\} dP_{Gj}(t)$, respectively. Then, we have

$$p_{GG}(s) = \overline{q}_{GV}(s) \overline{h}_{GG}(s), \tag{10}$$

$$p_{GV}(s) = q_{GV}(s) \left[\overline{q}_{VA}(s) - q_{VM}(s) \right] / \overline{h}_{GG}(s), \tag{11}$$

$$p_{GA}(s) = q_{GV}(s) q_{VA}(s) \left[\overline{q}_{AG}(s) - q_{AF}(s) \right] / \overline{h}_{GG}(s), \tag{12}$$

$$p_{GF}(s) = q_{GV}(s) q_{VA}(s) q_{AF}(s) \overline{q}_{FG}(s) / \overline{h}_{GG}(s), \tag{13}$$

$$p_{GM}(s) = q_{GV}(s) q_{VM}(s) \overline{q}_{MG}(s) / \overline{h}_{GG}(s). \tag{14}$$

It is not so easy to take the inversion of the above LSTs in Eqs.(10)–(14) . Instead, by taking the limitation, we can derive the limitting transition probability $P_j = \lim_{t \to \infty} p_{G,j}(t)$, $j \in \{G, V, A, F, M\}$, i.e.,

$$P_G = \frac{\mu_0}{\mu_0 + \int_0^{t_0} \overline{F}_a(t) dt + \alpha F_a(t_0) + \beta F_a(t_0) + \mu_c \overline{F}_a(t_0)}, \tag{15}$$

$$P_V = \frac{\int_0^{t_0} \overline{F}_a(t) dt}{\mu_0 + \int_0^{t_0} \overline{F}_a(t) dt + \alpha F_a(t_0) + \beta F_a(t_0) + \mu_c \overline{F}_a(t_0)}, \tag{16}$$

$$P_A = \frac{\alpha F_a(t_0)}{\mu_0 + \int_0^{t_0} \overline{F}_a(t) dt + \alpha F_a(t_0) + \beta F_a(t_0) + \mu_c \overline{F}_a(t_0)}, \tag{17}$$

$$P_F = \frac{\beta F_a(t_0)}{\mu_0 + \int_0^{t_0} \overline{F}_a(t) dt + \alpha F_a(t_0) + \beta F_a(t_0) + \mu_c \overline{F}_a(t_0)}, \tag{18}$$

$$P_M = \frac{\mu_c \overline{F}_a(t_0)}{\mu_0 + \int_0^{t_0} \overline{F}_a(t) dt + \alpha F_a(t_0) + \beta F_a(t_0) + \mu_c \overline{F}_a(t_0)}, \tag{19}$$

where

$$\alpha = \int_0^\infty t \overline{F}_t(t) dF_f(t) + \int_0^\infty t \overline{F}_f(t) dF_t(t), \tag{20}$$

$$\beta = \mu_r \int_0^\infty \overline{F}_t(t) dF_f(t). \tag{21}$$

In Eqs.(20) and (21), α and β imply the mean transition time from State A to the subsequent state and the mean transition time from State A to State G

through State F, respectively. From the results above, the semi-Markov model here is ergodic and the related stationary measures like the long-run average cost exist.

2.2 Optimal Preventive Maintenance Policy

Define the following cost parameters:

c_{m} (> 0): preventive maintenance cost per unit time
c_{t} (> 0): minor recovery cost per unit time
c_{r} (> 0): major recovery cost per unit time.
Then, the long-run average cost for the steady state in Model 1, $C_1(t_0)$, is formulated by

$$\begin{aligned} C_1(t_0) &= \lim_{t\to\infty} \frac{\mathrm{E}[\text{total cost during } (0,t]]}{t} \\ &= c_{\mathsf{m}} P_{\mathsf{M}} + c_{\mathsf{t}} P_{\mathsf{A}} + c_{\mathsf{r}} P_{\mathsf{F}} = U_{\mathsf{c1}}(t_0)/T_1(t_0), \end{aligned} \tag{22}$$

where

$$U_{\mathsf{c1}}(t_0) = c_{\mathsf{m}}\mu_{\mathsf{c}}\overline{F}_{\mathsf{a}}(t_0) + c_{\mathsf{t}}\alpha F_{\mathsf{a}}(t_0) + c_{\mathsf{r}}\beta F_{\mathsf{a}}(t_0), \tag{23}$$

$$T_1(t_0) = \mu_0 + \int_0^{t_0} \overline{F}_{\mathsf{a}}(t)dt + \alpha F_{\mathsf{a}}(t_0) + \beta F_{\mathsf{a}}(t_0) + \mu_{\mathsf{c}}\overline{F}_{\mathsf{a}}(t_0). \tag{24}$$

We make the following parametric assumptions:

(A-1) $c_{\mathsf{m}}\mu_{\mathsf{c}} < c_{\mathsf{t}}\alpha + c_{\mathsf{r}}\beta$,
(A-2) $\beta > \mu_{\mathsf{c}}$.

Assumption (A-1) means that the sum of both mean recovery costs from the failure probable state and the system failure state is always greater than the mean preventive maintenance cost. Also, Assumption (A-2) implies that the mean time to recover the system after a system failure is always greater than the mean time required by the preventive maintenance. These two assumptions are needed to motivate the optimal preventive maintenance policy considered here. Then, we can characterize the optimal preventive maintenance policy minimizing the long-run average cost in Model 1 as follows.

Theorem 1: (1) Suppose that the c.d.f. $F_{\mathsf{a}}(t)$ is strictly IFR (Increasing Failure Rate) under the assumptions (A-1) and (A-2). Define the non-linear function:

$$\begin{aligned} q_{\mathsf{c1}}(t_0) = (c_{\mathsf{t}}\alpha + c_{\mathsf{r}}\beta - c_{\mathsf{m}}\mu_{\mathsf{c}})r_{\mathsf{a}}(t_0)T_1(t_0) \\ -\{1 + (\alpha + \beta - \mu_{\mathsf{c}})r_{\mathsf{a}}(t_0)\}U_{\mathsf{c1}}(t_0), \end{aligned} \tag{25}$$

where $r_{\mathsf{a}}(t) = (dF_{\mathsf{a}}(t)/dt)/\overline{F}_{\mathsf{a}}(t)$ is the failure rate.

(i) If $q_{c1}(0) < 0$ and $q_{c1}(\infty) > 0$, then there exists a unique optimal preventive maintenance time t_0^* $(0 < t_0^* < \infty)$ satisfying $q_{c1}(t_0^*) = 0$. The minimum long-run average cost is then given by

$$C_1(t_0^*) = \frac{(c_t\alpha + c_r\beta - c_m\mu_c)r_a(t_0^*)}{1 + (\alpha + \beta - \mu_c)r_a(t_0^*)}. \tag{26}$$

(ii) If $q_{c1}(0) \geq 0$, then $t_0^* = 0$, i.e., it is optimal to trigger the preventive maintenance just after the vulnerability is detected. Then the minimum long-run average cost is given by

$$C_1(t_0^*) = C_1(0) = \frac{c_m\mu_c}{\mu_0 + \mu_c}. \tag{27}$$

(iii) If $q_{c1}(\infty) \leq 0$, then $t_0^* \to \infty$, i.e., it is optimal not to perform the preventive maintenance even after the vulnerability is detected. Then the minimum long-run average cost is given by

$$C_1(t_0^*) = C_1(\infty) = \frac{c_t\alpha + c_r\beta}{\mu_0 + \mu_a + \alpha + \beta}. \tag{28}$$

(2) Suppose that the c.d.f. $F_a(t)$ is DFR (Decreasing Failure Rate) under the assumptions (A-1) and (A-2). If $C_1(0) < C_1(\infty)$, then $t_0^* = 0$ otherwise $t_0^* \to \infty$.

Proof: Differentiating the function $C_1(t_0)$ with respect to t_0 and setting it equal to zero imply $q_{c1}(t_0) = 0$. Further differentiation of $q_{c1}(t_0)$ yields

$$\frac{q_{c1}(t_0)}{dt_0} = \frac{dr_a(t_0)}{dt}\Big\{(c_t\alpha + c_r\beta - c_m\mu_c)T_1(t_0) - (\alpha + \beta - \mu_c)U_{c1}(t_0)\Big\}. \tag{29}$$

If $F_a(t)$ is strict IFR, from the assumptions (A-1) and (A-2), it is obvious that the right-hand-side of Eq.(29) takes a positive value for an arbitrary t_0 and that the function $q_{c1}(t_0)$ is an increasing function of t_0. From this, the long-run average cost $C_1(t_0)$ is a quasi-convex function of t_0, so that if $q_{c1}(0) < 0$ and $q_{c1}(\infty) > 0$, then there exists a unique optimal solution t_0^* $(0 < t_0^* < \infty)$ which satisfies $q_{c1}(t_0^*) = 0$. In the cases of $q_{c1}(0) \geq 0$ and $q_{c1}(\infty) \leq 0$, the long-run average cost $C_1(t_0)$ becomes increasing and decreasing in t_0, and the optimal solution is given by $t_0^* = 0$ and $t_0^* \to \infty$, respectively. If $F_a(t)$ is DFR, the long-run average cost $C_1(t_0)$ is a quasi-concave function of t_0, and the result is trivial.

3 Model 2

3.1 Model Description

In Model 1 it was assumed that the vulnerable state V could be detectable by the vulnerability identifiers and that the development of the patch could be

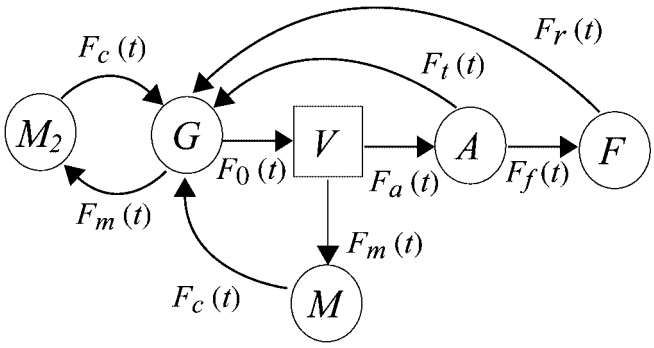

Fig. 2. MRGP transition diagram of Model 2.

started after the time t_0 measured from the vulnerable state V elapsed. However, this assumption can not be always validated, because the vendor can not know the detection timing of vulnerabilities by malicious attackers. To resolve this problem, we consider another stochastic model referred as Model 2 in Fig.2. That is, the preventive maintenance is triggered at the periodic time interval measured from State G. In Fig.2, the circles and the square denote regeneration points and a non-regeneration point, respectively, so that the underlying stochastic process is reduced to a Markov regenerative process (MRGP) which belongs to the wider class than the semi-Markov processes.

However, as well known, the MRGP can be translated to the usual semi-Markov process by changing the definition of the underlying states. Figure 3 illustrates the translated semi-Markov transition diagram of the MRGP in Fig.2, where we define two new states:

Normal State; G^0
Preventive Maintenance State; M^0

and the Stieltjes convolution operator by '$*$', i.e.,

$$F_0 * F_a(t) = \int_0^t F_0(t-x)dF_a(x). \tag{30}$$

Similar to the previous discussion, we define the one-step transition probability and its LST by $Q_{ij}(t),\ i,j \in \{G^0, A, F, M^0\}, i \neq j$ and $q_{ij}(s) = \int_0^\infty \exp\{-st\}\, dQ_{ij}(t)$, respectively. Then it is immediate to see that

$$q_{G^0A}(s) = \int_0^\infty \exp\{-st\}\overline{F}_m(t)dG(t), \tag{31}$$

$$q_{AG^0}(s) = \int_0^\infty \exp\{-st\}\overline{F}_f(t)dF_t(t), \tag{32}$$

$$q_{G^0M^0}(s) = \int_0^\infty \exp\{-st\}\overline{G}(t)dF_m(t), \tag{33}$$

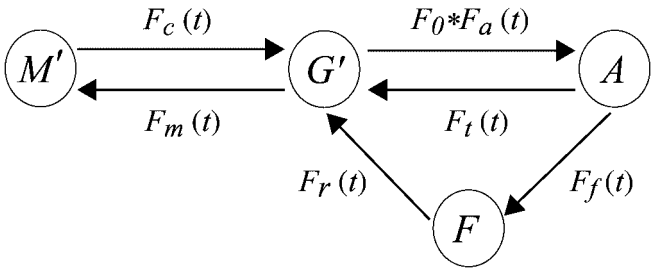

Fig. 3. Translated semi-Markov transition diagram of Model 2.

$$q_{M'G'}(s) = \int_0^\infty \exp\{-st\} dF_c(t), \tag{34}$$

$$q_{AF}(s) = \int_0^\infty \exp\{-st\} \overline{F}_t(t) dF_f(t), \tag{35}$$

$$q_{FG'}(s) = \int_0^\infty \exp\{-st\} dF_r(t), \tag{36}$$

where $G(t) = F_0(t) * F_a(t)$.

For the recurrent time distribution from State G' to State G' again, $H_{G'G'}(t)$, we obtain the LST:

$$\begin{aligned} h_{G'G'}(s) &= \int_0^\infty \exp\{-st\} dH_{G'G'}(t) \\ &= q_{G'M'}(s) q_{M'G'}(s) + q_{G'A}(s) q_{AG'}(s) \\ &\quad + q_{G'A}(s) q_{AF}(s) q_{FG'}(s). \end{aligned} \tag{37}$$

Given the initial state G' at time $t = 0$, the LSTs of transition probabilities $P_{G'j}(t)$, $j \in \{G', A, F, M'\}$ at an arbitrary time t (> 0) are given by

$$p_{G'G'}(s) = \overline{q}_{G'A}(s) - q_{G'M'}(s) \overline{h}_{G'G'}(s), \tag{38}$$

$$p_{G'A}(s) = q_{G'A}(s) \overline{q}_{AG'}(s) - q_{AF}(s) \overline{h}_{G'G'}(s), \tag{39}$$

$$p_{G'F}(s) = q_{G'A}(s) q_{AF}(s) \overline{q}_{FG'}(s) / \overline{h}_{G'G'}(s), \tag{40}$$

$$p_{G'M'}(s) = q_{G'M'}(s) \overline{q}_{M'G'}(s) / \overline{h}_{G'G'}(s). \tag{41}$$

In a fashion similar to Model 1, it can be seen that the limitting transition probabilities $P_j = \lim_{t\to\infty} p_{G',j}(t)$, $j \in \{G', A, F, M'\}$ are given by

$$P_{G'} = \frac{\int_0^{t_0} \overline{G}(t) dt}{\int_0^{t_0} \overline{G}(t) dt + \alpha G(t_0) + \beta G(t_0) + \mu_c \overline{G}(t_0)}, \tag{42}$$

$$P_A = \frac{\alpha G(t_0)}{\int_0^{t_0} \overline{G}(t) dt + \alpha G(t_0) + \beta G(t_0) + \mu_c \overline{G}(t_0)}, \tag{43}$$

$$P_{\mathrm{F}} = \frac{\beta G(t_0)}{\int_0^{t_0} \overline{G}(t)dt + \alpha G(t_0) + \beta G(t_0) + \mu_{\mathrm{c}} \overline{G}(t_0)}, \tag{44}$$

$$P_{\mathrm{M}^0} = \frac{\mu_{\mathrm{c}} \overline{G}(t_0)}{\int_0^{t_0} \overline{G}(t)dt + \alpha G(t_0) + \beta G(t_0) + \mu_{\mathrm{c}} \overline{G}(t_0)}. \tag{45}$$

3.2 Optimal Preventive Maintenance Policy

In Model 2, the long-run average cost $C_2(t_0)$ is formulated as

$$\begin{aligned} C_2(t_0) &= \lim_{t\to\infty} \frac{\mathrm{E}[\text{total cost during } (0,t]]}{t} \\ &= c_{\mathrm{m}} P_{\mathrm{M}^0} + c_{\mathrm{t}} P_{\mathrm{A}} + c_{\mathrm{r}} P_{\mathrm{F}} = U_{\mathrm{c2}}(t_0)/T_2(t_0), \end{aligned} \tag{46}$$

where

$$U_{\mathrm{c2}}(t_0) = c_{\mathrm{m}} \mu_{\mathrm{c}} \overline{G}(t_0) + c_{\mathrm{t}} \alpha G(t_0) + c_{\mathrm{r}} \beta G(t_0), \tag{47}$$

$$T_2(t_0) = \int_0^{t_0} \overline{G}(t)dt + \alpha G(t_0) + \beta G(t_0) + \mu_{\mathrm{c}} \overline{G}(t_0). \tag{48}$$

We give the following result to characterize the optimal preventive maintenance policy for Model 2, without the proof.

Theorem 2: (1) Suppose that the c.d.f. $F_{\mathrm{a}}(t)$ is strictly IFR under the assumptions (A-1) and (A-2). Define the non-linear function:

$$\begin{aligned} q_{\mathrm{c2}}(t_0) = &(c_{\mathrm{t}}\alpha + c_{\mathrm{r}}\beta - c_{\mathrm{m}}\mu_{\mathrm{c}}) r_{0\mathrm{a}}(t_0) T_2(t_0) \\ &- \{1 + (\alpha + \beta - \mu_{\mathrm{c}}) r_{0\mathrm{a}}(t_0)\} U_{\mathrm{c2}}(t_0), \end{aligned} \tag{49}$$

where $r_{0\mathrm{a}}(t) = (dG(t)/dt)/\overline{G}(t)$ is the failure rate.

(i) If $q_{\mathrm{c2}}(0) < 0$ and $q_{\mathrm{c2}}(\infty) > 0$, then there exists a unique optimal preventive maintenance time t_0^* $(0 < t_0^* < \infty)$ satisfying $q_{\mathrm{c2}}(t_0^*) = 0$. The minimum long-run average cost is then given by

$$C_2(t_0^*) = \frac{(c_{\mathrm{t}}\alpha + c_{\mathrm{r}}\beta - c_{\mathrm{m}}\mu_{\mathrm{c}}) r_{0\mathrm{a}}(t_0^*)}{1 + (\alpha + \beta - \mu_{\mathrm{c}}) r_{0\mathrm{a}}(t_0^*)}. \tag{50}$$

(ii) If $q_{\mathrm{c1}}(0) \geq 0$, then $t_0^* = 0$ and the minimum long-run average cost is given by

$$C_2(t_0^*) = C_2(0) = c_{\mathrm{m}}. \tag{51}$$

(iii) If $q_{\mathrm{c2}}(\infty) \leq 0$, then $t_0^* \to \infty$ and the minimum long-run average cost is given by

$$C_2(t_0^*) = C_2(\infty) = \frac{c_{\mathrm{t}}\alpha + c_{\mathrm{r}}\beta}{\mu_0 + \mu_{\mathrm{a}} + \alpha + \beta}. \tag{52}$$

(2) Suppose that the c.d.f. $F_{\mathrm{a}}(t)$ is DFR under the assumptions (A-1) and (A-2). If $C_2(0) < C_2(\infty)$, then $t_0^* = 0$ otherwise $t_0^* \to \infty$.

Table 1. Dependence of parameters (k, λ) on the long-run average cost.

		Model 1			Model 2		
(k,λ)	$t_0 \to \infty$	t_0^*	$C_1(t_0^*)$	reduction (%)	t_0^*	$C_2(t_0^*)$	reduction (%)
(2,5)	119.3280	0.0105	8.7717	92.6491	45.5572	49.6777	58.3689
(2,10)	113.3180	0.0421	8.7709	92.2600	48.2156	47.2078	58.3406
(2,15)	107.8850	0.0949	8.7695	91.8714	50.8743	44.9717	58.3151
(3,5)	116.2460	0.3344	8.7606	92.4637	53.1873	38.2400	67.1041
(3,10)	107.8850	0.9586	8.7397	91.8991	57.6474	35.4980	67.0964
(3,15)	100.6460	1.7782	8.7124	91.3435	62.1078	33.1228	67.0898
(4,5)	113.3180	1.2623	8.7245	92.3009	60.5449	31.6771	72.0459
(4,10)	102.9490	3.2492	8.6515	91.5963	67.0879	28.7700	72.0541
(4,15)	94.3177	5.6576	8.5651	90.9189	73.6312	26.3515	72.0609

In Section 2 and Section 3, we derived the optimal preventive policies for respective models with aperiodic and periodic preventive maintenance schedules, respectively. In the following section, we calculate numerically the optimal preventive schedules and their associated long-run average costs, and compare them quantitatively. Also, we perform the sensitivity analysis of model parameters and investigate the effect of preventive maintenance policy in the intrusion tolerant system.

4 Numerical Examples

Suppose that the c.d.f. $F_{\mathsf{a}}(t)$ is given by the gamma distribution with shape parameter k (> 0) and scale parameter λ (> 0):

$$F_{\mathsf{a}}(t) = t^{\mathsf{k}-1}\frac{\exp\{-t/\lambda\}}{\Gamma(k)\lambda^{\mathsf{k}}} \tag{53}$$

and that the other transition probabilities are given by the exponential distributions, where the other model parameters are assumed as $\mu_0 = 168$, $\mu_{\mathsf{f}} = 4$, $\mu_{\mathsf{c}} = 3$, $\mu_{\mathsf{t}} = 5$, $c_{\mathsf{r}} = 2500$, $c_{\mathsf{m}} = 500$ and $c_{\mathsf{t}} = 750$.

Table 1 presents the dependence of distribution parameters (k, λ) on the optimal preventive maintenance policies and their associated long-run average costs. From this result, it would be effective to perform the preventive maintenance based on the optimality criterion. Comparing the case without the preventive maintenance, the effect of 91%∼92% (60%∼70%) cost reduction in Model 1 (Model 2) was found in each parameter setting. On the other hand, when Model 1 is compared with Model 2, Model 1 could reduce the 75%∼85% average cost more than Model 2. This is a natural conclusion because the vulnerable states are always detectable in Model 1 but not in Model 2. For instance, if the vendors or the CERT/CC could detect the vulnerabilities more quickly than the malicious attackers, they will be able to reduce the operation cost effectively.

References

1. Y. Deswarte, L. Blain and J. C. Fabre: Intrusion tolerance in distributed computing systems. Proceedings of 1991 IEEE Symposium on Research in Security and Privacy, pp. 110–121. IEEE Press (1991).
2. L. Garber: Denial-of-service attacks rip the Internet. IEEE Computer, 33 (4), pp. 12–17 (2000).
3. V. Guputa, V. Lam, H. V. Ramasamy, W. H. Sanders and S. Singh: Dependability and performance evaluation of intrusion-tolerant server architectures. LADC 2003, LNCS 2847, pp. 81–101, Springer-Verlag (2003).
4. M. Imaizumi, M. Kimura and K. Yasui: Reliability analysis of a network server system with illegal access. Advanced Reliability Modeling II (W. Y. Yun and T. Dohi, eds.), pp. 40–47, World Scientific (2006).
5. E. Jonsson and T. Olovsson: A quantitative model of the security intrusion process based on attacker behavior. IEEE Transactions on Software Engineering, 23 (4), pp. 235–245 (1997).
6. B. Littlewood, S. Brocklehurst, N. Fenton, P. Mellor, S. Page, D. Wright, J. Doboson, J. McDermid and D. Gollmann: Towards operational measures of computer security. Journal of Computer Security, 2 (2/3), pp. 211–229 (1993).
7. B. B. Madan, K. Goseva-Popstojanova, K. Vaidyanathan, and K. S. Trivedi: Modeling and quantification of security attributes of software systems. Proceedings of International Conference on Dependable Systems and Networks (DSN 2002), pp. 505–514, IEEE CS Press (2002).
8. B. B. Madan, K. Goseva-Popstojanova, K. Vaidyanathan, and K. S. Trivedi: A method for modeling and quantifying the security attributes of intrusion tolerant systems. Performance Evaluation, 56 (1/4), pp. 167–186 (2004).
9. R. Ortalo, Y. Deswarte and M. Kaaniche: Experimenting with quantitative evaluation tools for monitoring operational security. IEEE Transactions on Software Engineering, 25 (5), pp. 633–650 (1999).
10. H. Pant, A. R. McGee, U. Chandrashekhar and S. H. Richman: Optimal availability and security for IMS-based VoIP networks. Bell Labs Technical Journal, 11 (3), pp. 211–223 (2006).
11. S. Singh, M. Cukier and W. H. Sanders: Probabilistic validation of an intrusion tolerant replication system. Proceedings of International Conference on Dependable Systems and Networks (DSN 2003), pp. 615–624, IEEE CS Press (2003).
12. F. Stevens, T. Courtney, S. Singh, A. Agbaria, J. F. Meyer, W. H. Sanders and P. Pal: Model-based validation of an intrusion-tolerant information system. Proceedings of 23rd IEEE Reliablr Distributed Systems Symposium (SRDS 2004), pp. 184–194, IEEE CS Press (2004).
13. R. Stroud: A qualitative analysis of the intrusion-tolerant capabilities of the MAFTIA architecture. Proceedings of International Conference on Dependable Systems and Networks (DSN 2004), pp. 453–461, IEEE CS Press (2004).
14. P. E. Verissimo, N. F. Neves and M. Correia: Intrusion-tolerant architectures: concepts and design. Architecting Dependable Systems (R. Lemos, C. Gacek and A. Romanovsky, eds.), LNCS 2677, pp. 3–36, Springer-Verlag (2003).
15. P. E. Verissimo, N. F. Neves, C. Cachin, J. Poritz, D. Powell, Y. Deswarte, R. Stroud and I. Welch: Intrusion-tolerant middleware. IEEE Security and Privacy, 4 (4), pp. 54–62 (2006).
16. H. Wang and P. Liu: Modeling and evaluationg the survivability of an intrusion tolerant database system. ESORICS 2006 (D. Gollmann, J. Meier and A. Sabelfeld, eds.), LNCS 4189, pp. 207–224, Springer-Verlag (2006).