An Economic Analysis of Security Investment in Information Systems with Security Threats: A Stochastic Approach

Won Seok Yang, Tae-Sung Kim, and Eun Saem Yang

***Abstract*—**We present an economic analysis of an information system with security threats. We categorize the types of threats and introduce a stochastic model to describe the occurrence of threats and their damage. The results of the stochastic analysis are used for analyzing the revenue and the average costs such as the loss cost, the repair cost, the recovery cost, and the holding cost. We present the NPV (Net Present Value) considering the security investment and the discount rate. In addition, we propose a parameter estimation method of the stochastic model and show a numerical example. The approach in this paper can be useful for a security investment decision-making to determine the optimal investment portfolio.

***Keywords*—**economic analysis, security investment, security threat, stochastic model.

I. Introduction

Since Gordon and Loeb in [1] considered the vulnerability of information to determine the optimal amount of security investment, many researchers have studied on the security investment decision-making [2]-[4]. Threats to information assets incur various types of damage including data loss, hardware replacement or repair, and performance deterioration of an information system. In order to make a reasonable decision regarding information security investment, it is required to consider the economic impact of each type of damage to the information system management.

We consider an information system with three types of threats. First, type-1 threats remove data that the system currently processes. It is assumed that the data become lost. Second, type-2 threats damage hardware and a portion of data stored in hardware. The system requires repairing or replacing the hardware and recovering the damaged data. Finally, type-3 threats deteriorate the system performance, that is, the service rate or the processing speed.

Won Seok Yang is with the Department of Business Administration, Hannam University, 133 Ojung-dong, Daeduk-gu, Daejeon 306-791, South Korea (e-mail: wonsyang@hnu.kr).

Tae-Sung Kim is with the Department of Management Information Systems, Chungbuk National University, 12 Gaeshin-dong, Heungduk-gu, Cheongju, Chungbuk 361-763, South Korea (corresponding author. phone: +82-43-261-3343; fax: +82-43-273-2355; e-mail: kimts@cbnu.ac.kr).

Eun Saem Yang is with the Department of Computer Engineering, Hallym University, Chuncheon, KangwonDo 200-702, South Korea (e-mail: yanges@hallym.ac.kr).

We present a stochastic model that describes the occurrence of threats and their damage to the system. We use the notion of negative customer to describe type-1 threat. Negative customers remove works in the system. Queues with negative customers have been studied extensively (See [5] and the references therein.) In addition, we apply the research of system deterioration to model type-3 threat. We use the stochastic model in [6] to describe the system deterioration by threats. It is necessary to manage the system performance for providing quality of service to customers. A preventive maintenance policy is considered. The system is monitored continuously and repaired whenever its performance is lower than a predetermined level. The maintenance is important in software services as the industry of information technology grows [7]. We model type-2 threat using a stochastic process. Next, we present an economic analysis which results in the NPV (Net Present Value), analyzing the costs and the revenue of the system. The system has the following cost and benefit structure. The system requires initial security investment. The costs consist of the loss cost for the removed data currently being processed, the repair cost for damaged hardware, the recovery cost of the damaged data in hardware, the repair cost for the system maintenance, and the holding cost of the system operation. The system earns revenue by processing data. The approach in this paper can be useful for a security investment decision-making to determine the optimal investment portfolio and be applicable to information service systems that have the structure of queueing systems, for example, mobile computing, smart grid, and m-learning services [8]-[10].

The rest of this paper is structured as follows. In section 2, we review previous research. In section 3, we describe a stochastic model with some notations. In section 4, we analyze the stochastic model. In section 5, we present the NPV. In section 6, we present a parameter estimation method. In section 7, we show a numerical example. Finally, we conclude this study in section 8.

II. Literature Review on Information Security Investment

Investment accompanies predictions of the effect of the investment and its objective assessment. The information security field is not an exception, as analysis of the effect of an investment and its objective assessment is required. As the

importance of human behavior in the information security field often exceeds that of any technological aspect through the passage of time, economic approaches such as adequate investment levels for information security, information sharing for information security, and the establishment of incentive systems to solve information security issues are freshly gaining the spotlight.

As to the need for socioeconomic study for information security, Soo Hoo analyzed the need for studying information security issues in the insurance industry and companies, suggesting the need for discussions of an efficient investment size as well as related analyses [11]. Not only social scientists such as Gordon et al. [12], Gal-Or and Ghose [13] or Shin [14] but also those who are considered to be traditional information security technology experts such as Anderson [15] have emphasized the need for socioeconomic investigations of information security as opposed to studies of flaws in mathematical codes for information security issues; they have suggested the need for discussion pertaining to the efficient investment size and its effect, among other issues.

Gordon and Loeb [1] utilized the net present value (NPV) model to analyze effects of information security investment, and through game theory, Cavusoglu et al. [16] determined the optimal investment in security controls. Carnegie Mellon University and the University of Idaho presented a method to produce a return on security investment (ROSI) using diverse variables of information security investment [17].

However, these studies were limited in terms of actual applications due to the convenience issues pertaining to data collection, quantification of information security usefulness and the absence of concrete calculation methods associated with the cost of information security. To overcome these limitations, Kim and Park [17] as well as Lee and Lee [18] presented an improved ROSI method based on the total cost of ownership (TCO). Al-Humaigani and Dunn [19], Tsiakis and Stephanides [20], Hausken [21], and Davis [22] also defined economic assessments of information security investment with ROSI and other methods; they approached the correlation between the investment cost and effect of information security with mathematical modeling. Blatchford [23], Lee [24], and Cavusoglu et al. [16, 25] categorized various factors that need to be considered during information security investment. Bodin et al. [26] and Scott [27] also suggested investment criteria for information security and mentioned that as information security investment in general has the characteristic of a long-term guarantee while reducing long-term risk, in many instances it does not provide a quantitative investment effect in the short term. Blakely [28], Witty et al. [29], Harris [30], Roper [31], and Sun [32] also categorized the cost factors of information security investment. Hong [33] quantified the level of information security management and analyzed how efforts towards information security affect organizations. Nam [34] analyzed the effects of information security investment through how the security incidents of a company affect its stock prices. Gwon and Kim [35] utilized changes in a company's market value while quantitatively measuring information security investment what is known as the event study methodology, a type of social scientific methodology.

Assessing and analyzing an investment should systematically quantify the activities and assets of an organization, enable strategic planning, and multi-dimensionally assess even the long-term and intangible effects of an organization. In particular, the following facts must be considered when analyzing information security investment [34]. The first of these involves the time constraint characteristic of the measuring of the information security investment effect: information security investment should not be restricted to the preservation of current asset value but should be considered in terms of preserving future value. Second is the intangible aspect of the effect of information security investment: as information security has numerous intangible elements in terms of costs and benefits, they are difficult to identify. Even when they are, transformation into monetary value is difficult. The third fact is the multi-faceted aspect of the effect of information security investment: this implies that information security investment is difficult to measure as it contains both qualitative and quantitative aspects. Fourth is the ambiguity of effect of information security investment: the scope of performance measurement for information security investment is extensive and difficult to assess in connection with goals already set within the organization. Therefore, an analytic system should be developed to test the validity of information security investment through the structure of feedback if possible within the business activities of organizations and companies.

III. Model Description

There are M security investment portfolios, which consists of multiple information security systems. Let PF_m denote the mth portfolio. PF_0 represents the current security level. The security level becomes higher as m increases.

The data that an information system handles, for example, banking and shopping, arrive according to a Poisson process with rate λ. The server has finite states $0,1,\cdots,\beta$, which represent the processing conditions of the system. The processing times are independent exponential random variables with rate μ_k, where k represents the system state. The states are ordered according to the relative degree of deterioration of the system. That is, $\mu_i < \mu_j$ for $i > j$. The system processes the data and stores them in hardware. It is assumed that there is no data at the initiation of the system operation.

Threats are classified into three types according to the damage: First, data that the system processes, including waiting data, are lost by type-1 threats. Let d_k denote the loss probability of the number of data that are lost. It is assumed that the loss probability follows a geometric distribution, such as $d_k = d(1-d)^{k-1}$, $k = 1,2,\cdots$. Second, type-2 threats break down hardware and damage the data that are stored in hardware. The ratio of damaged data is f among the total data. It is

assumed that hardware is repaired and data are recovered instantaneously. Third, type-3 threats deteriorate the system, that is, increases the system state by k with probability g_k. Type-i threats occur according to a Poisson process with rate ω_m^i in PF_m. Note that $\omega_k^i < \omega_l^i$ for $k > l$.

We consider a preventive maintenance policy in order to operate the system stable. The system is repaired at or above state α, which we call maintenance level. The repair time is exponentially distributed with rate $1/\delta$. It is assumed that threats do not occur in the system during a repair.

The system earns revenue p per data. The system costs consist of as follows: The loss cost c_L per data, the repair cost of damaged hardware c_W per repair, the recovery cost of damaged data c_D per data, and the holding cost c_H per unit time and data. The system repair cost is c_R^i per repair with the maintenance level i. The security investment cost is c_P^m in x_{ij}. It is assumed that $c_P^i > c_P^j$ for the portfolio $i > j$. The investment occurs at time 0. Finally, we denote the length of a fiscal period and the discount rate of a fiscal year as τ and θ, respectively.

IV. Stochastic Analysis

First, we analyze the number of data that the system processes by using the Markov Chain. Let (i, j) denote the state of a Markov chain. The notation i represents the number of data in the system and j stands for the system state, for $i = 0,1,\cdots$ and $j = 0,1,\cdots,\beta$. Arranging the states in a lexicographic order gives the following matrix structure:

$$Q = \begin{pmatrix} B_0 & A_0 & & \\ B_1 & A_1 & A_0 & \\ B_2 & A_2 & A_1 & \ddots \\ B_3 & A_3 & A_2 & \ddots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}. \quad (1)$$

The matrices A_k and B_k in (1) are the square matrices of the size $(\beta+1)$. The elements of the matrices in (1) are shown in Appendix.

Let x_{ij} be the steady-state probability that the Markov chain is in state (i, j). Let π_j be the steady-state probability that the system is in state j.

Let us define

$$\boldsymbol{\pi} = (\pi_0, \cdots, \pi_\beta),$$
$$\mathbf{x}_i = (x_{i0}, \cdots, x_{i\beta}), \text{ for } i = 0,1,\cdots,$$
$$\boldsymbol{\mu} = (\mu_0, \cdots, \mu_\beta).$$

Applying the matrix geometric method in [36] to (1) results in

$$\mathbf{x}_k = \boldsymbol{\pi}(I - R)R^k, \ k = 1,2,\cdots, \quad (2)$$

where $\boldsymbol{\pi}$ is the steady-state probability of the Markov chain with the transition rate matrix A. The definition of matrix A and the numerical method of solving $\boldsymbol{\pi}$ and R in (2) are given in Appendix.

Let N_m denote the average number of data that the system processes in PF_m. Using (2) gives

$$N_m = \sum_{k=1}^{\infty} k\mathbf{x}_k\mathbf{e} = \boldsymbol{\pi}R(I - R)^{-1}\mathbf{e}. \quad (3)$$

Let us define the throughput and the loss rate as the number of data processed successfully and lost by the type-1 threat, respectively, per unit time. Let Ψ_m and Ω_m denote the throughput and the loss rate in PF_m. Then, we have

$$\Psi_m = \boldsymbol{\pi}\boldsymbol{\mu} = \sum_{j=0}^{\beta} \pi_j \mu_j, \quad (4)$$

$$\Omega_m = \frac{\omega_m^1}{d}\boldsymbol{\pi}V\mathbf{e} = \left(\omega_m^1 \sum_{j=0}^{\alpha-1} \pi_j\right)\left(\frac{1}{d}\right). \quad (5)$$

Suppose that the system does not transit to different states when the system is at, or above, state α. In this case, the system behaves stochastically governed by the absorbing Markov chain with the following transition rate matrix $\tilde{A}$.

$$\tilde{A} = \begin{bmatrix} G & \overline{G} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}. \quad (6)$$

The elements of G is given by

$$G = \begin{bmatrix} -\omega_m^3 & \omega_m^3 g_1 & \omega_m^3 g_2 & \cdots & \omega_m^3 g_{\alpha-1} \\ & -\omega_m^3 & \omega_m^3 g_1 & \cdots & \omega_m^3 g_{\alpha-2} \\ & & \ddots & \ddots & \vdots \\ & & & -\omega_m^3 & \omega_m^3 g_1 \\ & & & & -\omega_m^3 \end{bmatrix}.$$

Let Γ_m^1 be the time interval from the point when the system state is 0 to the point when the system repair begins in PF_m. Let Γ_m^2 be the time interval form the initiation to the end of the system repair. Let $\Gamma_m = \Gamma_m^1 + \Gamma_m^2$. Γ_m^1 is equivalent to the absorption time of the Markov chain with the transition rate matrix of (6). Then, we have $E[\Gamma_m^1] = -\mathbf{q}_0 G^{-1}\mathbf{e}$. The average

repair time is $E[\Gamma_m^2]=1/\delta$. This gives

$$E[\Gamma_m]=-\mathbf{q}_0 G^{-1}\mathbf{e}+1/\delta. \quad (7)$$

where $\mathbf{q}_0$ is the column vector of size α and $\mathbf{q}_0=(1,0,\cdots,0)$.

Let $\Lambda(t)$ denote the average number of data that have been stored in hardware by time t. The data is stored at the rate of Ψ_m in (4). Then, the average number of data in hardware by the j th fiscal period is

$$\Lambda((j-1)\tau)=\Psi_m(j-1)\tau. \quad (8)$$

Let Z_k be the point that the k th type-2 threat occurs during $(0,\tau)$. Let Y_k be the interval from the $(k-1)$ th to the k th occurrence point of the type-2 threat. Note that $Z_k=Y_1+\cdots+Y_k$ and $E[Y_k]=1/\omega_m^2$. Then, the average number of data stored by Z_k is given by

$$\Lambda(Z_k)=\Psi_m E(Y_1+\cdots+Y_k)=\frac{\Psi_m}{\omega_m^2}k. \quad (9)$$

Let $H_k^{(j)}$ be the average number of data that are damaged by the k th type-2 threat and also recovered during the j th fiscal period $[(j-1)\tau, j\tau]$. The portion of f is damaged among the data in hardware. Then, we have

$$H_k^{(j)}=f\Psi_m\left\{(j-1)\tau+\frac{k}{\omega_m^2}\right\}. \quad (10)$$

Let a_k be the probability that k type-2 threats occur during $[(j-1)\tau, j\tau]$. Type-2 threats occur according to a Poisson process. Thus, we have

$$a_k=\frac{e^{-\omega_m^2\tau}(\omega_m^2\tau)^k}{k!}.$$

Let F_m^j be the average number of data recovered during $[(j-1)\tau, j\tau]$ in PF_m. Using (10) gives

$$\begin{aligned}F_m^j&=\sum_{k=1}^{\infty}\left\{H_1^{(j)}+\cdots H_k^{(j)}\right\}a_k\\&=f\Psi_m\left\{(j-1)\tau(1-a_0)+\frac{1}{\omega_m^2}\sum_{k=1}^{\infty}(1+\cdots+k)a_k\right\}.\end{aligned} \quad (11)$$

where $a_0=e^{-\omega_m^2\tau}$.

V. Economic Analysis

We analyze the cumulative NPV at the end of the fiscal period y. Let us consider the average cost incurred in the j th fiscal period for $j=1,\cdots,y$ and in m th investment portfolio PF_m. From (5), the average loss cost during τ results in $c_L(\Omega_m\tau)$. The type-2 threat occurs $\omega_m^2\tau$ during τ. Therefore, the average repair cost of a hardware during τ is $c_W(\omega_m^2\tau)$. From (11), the average recovery cost of damaged data during the j th fiscal period in PF_m gives $c_D F_m^j$. The system is repaired once during $E[\Gamma_m]$ in (7). Thus the average repair cost of the system during τ is $c_R^{\alpha}(\tau/E[\Gamma_m])$. Since the holding cost is proportional to the number of data that are served, the average holding cost during τ is $c_H N_m\tau$. Adding the abovementioned costs gives the average cost of the j th fiscal period as follows.

$$AC(j)=\left\{c_L\Omega_m+c_W\omega_m^2+\frac{c_R^{\alpha}}{E[\Gamma_m]}+c_H N_m\right\}\tau+F_m^j c_D. \quad (12)$$

Let $P(m,\alpha,y)$ be the cumulative NPV at the end of the fiscal period y with a maintenance level α in PF_m. Let θ denote the discount rate of a fiscal year. The average revenue during τ is $p(\Psi_m\tau)$. The initial security investment cost is c_P^m. Applying the discount rate to the revenue and cost in each fiscal period results in

$$P(m,\alpha,y)=-c_P^m+\sum_{j=1}^{y}\frac{p\Psi_m\tau-AC(j)}{(1+\theta)^j}. \quad (13)$$

VI. Parameter Estimation

The operational data for parameter estimation can be gathered in information systems. In this paper, $\hat{a}$ represents the estimator of the parameter a. Let $\xi(t)$ denote the number of data that have occurred in the system by time t. For a long time t, $\hat{\lambda}$ is given by [37].

$$\hat{\lambda}\approx\xi(t)/t. \quad (14)$$

Let $\Phi_i(t)$ denote the number of type-i threats that have occurred by time t. Similar to (14), for a long time t, we have

$$\hat{\omega}_0^i\approx\Phi_i(t)/t,\ i=1,2,3. \quad (15)$$

Note that benchmarking requires to set $\hat{\omega}_m^i$ in PF_m.

The number of the system state depends on the threats and the scale of their damage to the system. However, if its number is too big or small, it's difficult to design a proper maintenance

policy. Assume that the system has $0,1,\cdots,\beta$ states. Let τ_k and $U_k(t)$ denote the time duration when the system operates at state k, and the number of data processed during τ_k by time t, respectively. Then, we have

$$\hat{\mu}_k = U_k(t)/\tau_k \ , \ k = 0,1,\cdots,\beta \ . \tag{16}$$

Let θ_j and θ_j^f denote the number of data that were stored and damaged, respectively, at the occurrence point of the j th type-2 threat. Then, we have

$$\hat{f} = \frac{\sum_{j=1}^{n} \theta_j^f / \theta_j}{n} . \tag{17}$$

Let Δ_j be the amount of the deterioration at the j th type-3 threat. That is, the system state jumps by an amount of Δ_j. Then, the estimator of $\hat{g}_k$ is given by

$$\hat{g}_k = \frac{\sum_{j=1}^{n} I_k(\Delta_j)}{n} . \tag{18}$$

where $I_k(\Delta_j) = 1$ for $k = j$. Let κ_j be the duration of j th system repair. Applying the method of moments in [38] gives

$$\frac{1}{\hat{\delta}} = \frac{\sum_{j=1}^{n} \kappa_j}{n} . \tag{19}$$

Let l_j be the number of data lost by a j th type-1 threat. Applying the method of moments [38] gives

$$\frac{1}{\hat{d}} = \frac{\sum_{j=1}^{n} l_j}{n} , \tag{20}$$

where n is the number of observations.

VII. NUMERICAL EXAMPLE

We show a numerical example assuming that the parameters of the model in section 2 have arbitrary values.

We assume 4 security investment portfolios. In each portfolio, the security investment costs are $c_P^0 = 0$, $c_P^1 = 10$, $c_P^2 = 20$, $c_P^3 = 40$, and $c_P^4 = 80$. The unit is 100 million. It is assumed that the length of a fiscal period is 1 year and the discount rate is 10%. Then, $\tau = 8{,}760$ hours and $\theta = 10\%$.

It is assumed that the system has 5 states, that is, $\beta = 4$. The parameters of the system are shown in Table 1 and 2. Table 1 shows the arrival rates of data and the service rates. The values in Table 1 represent the number of data per hour.

Table 1. The arrival rates of data and the service rates

parameter	value
λ	1,000
μ_0	1,300
μ_1	1,200
μ_2	1,100
μ_3	1,000
μ_4	900

The arrival rates of the threats in each portfolio are shown in Table 2. The values in Table 2 represent the number of threats per hour. The values in Table 2 represent business goals in each security investment portfolio.

Table 2. The arrival rates of threats

parameter	value
$\omega_0^1, \cdots, \omega_4^1$	0.0342, 0.0171, 0.0086, 0.0043, 0.0021
$\omega_0^2, \cdots, \omega_4^2$	0.0057, 0.0029, 0.0014, 0.0007, 0.0004
$\omega_0^3, \cdots, \omega_4^3$	0.0571, 0.0285, 0.0143, 0.0071, 0.0036

For convenient, it is assumed that the system deteriorates by one state. The repair time of the system is 24 hours. The parameters of the loss probability and the system deterioration are assumed that $d = 0.01$ and $g_1 = 0.5$. The ratio of damaged data is assumed that $f = 0.001$.

The unit price and costs are shown in Table 3.

Table 3. The unit price and costs

parameters	value
p	1,000
c_L	200
c_W	10,000,000
c_D	20
c_H	0.01
c_R^i	5,000,000

Table 4 shows the cumulative NPV in the portfolio 1 for 10 years. From the year 1 to 5, the NPV is maximized when the maintenance level is 1. However, after the year 5, the NPV is maximized when the maintenance level is 2. The maintenance levels 3 and 4 have never been economical, compared to the levels 1 and 2.

Table 4. The cumulative NPV in the portfolio 1

year	maintenance level			
	1	2	3	4
0	-10.0	-10.0	-10.0	-10.0
1	72.3	72.0	71.2	70.2
2	139.4	138.9	137.4	135.7
3	193.2	192.7	190.8	188.6
4	235.7	235.3	233.1	230.5
5	268.4	268.3	265.9	263.0
6	292.9	293.0	290.6	287.6
7	310.2	310.7	308.4	305.3
8	321.6	322.5	320.3	317.2
9	327.9	329.2	327.2	324.2
10	330.0	331.8	330.1	327.2

Summarizing the most profitable cases in each portfolio, we obtain Table 5. The portfolio 0 implies there is no security investment. The optimal portfolio that maximizes the NPV changes over the year. In the year 1, the optimal portfolio is 0. From the year 1 to 6, it changes to 2. After the year 7, the optimal portfolio becomes 3. The result in Table 3 implies that the optimal investment decision depends on the investment strategy such as short-term, mid-term, or long-term investment.

Table 5. The optimal NPV of each portfolio

year	portfolio				
	0	1	2	3	4
0	0.0	-10.0	-20.0	-40.0	-80.0
1	74.3	72.3	68.7	53.1	15.8
2	134.1	139.4	141.4	129.7	94.8
3	181.7	193.2	200.2	191.9	159.1
4	218.6	235.7	247.0	241.8	210.9
5	246.4	268.4	283.7	281.1	251.8
6	266.5	293.0	311.5	311.3	283.4
7	280.0	310.7	331.8	333.7	307.1
8	288.0	322.5	345.8	349.5	324.0
9	291.3	329.2	354.5	359.7	335.2
10	290.8	331.8	359.0	365.2	341.5

VIII. Conclusion

We evaluated information security portfolios considering types of damages: threats which remove data; threats which damage hardware and a portion of data in hardware; and threats which deteriorate systems performance. We presented a stochastic model to describe the damage of the threats in information systems. We derived the average costs of the system using the results of the stochastic analysis and presented the NPV. In addition, we showed a parameter estimation method of the stochastic model and a numerical example.

From the limited availability of data in this paper, empirical verification has not performed. Only if we obtain data, we can estimate all the parameters to evaluate information security investment portfolios in order to protect information systems from possible security threats. The model presented in this article can be widely used for evaluating information security investment decisions.

Appendix

For PF_m and $k = 0,1,\cdots$, we have

$$A_0 = \lambda I,\ A_2 = U + \omega_m^1 d_1 V = U + \omega_m^1 dV,$$
$$A_k = \omega_m^1 d_{k-1} V = \omega_m^1 d(1-d)^{k-2} V,\ k = 3,4,\cdots.$$

where I is the identity matrix of size $(\beta+1)$. U and V are the square matrices of size $(\beta+1)$ and their elements are given by

$$U = \begin{pmatrix} \mu_0 & & & & \\ & \mu_1 & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & \mu_\beta \end{pmatrix},$$

$$V = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & 0 & \\ & & & & \ddots \end{pmatrix}.$$

The matrix A_1 is given by

$$A_1 = \begin{pmatrix} -(\lambda+\mu_0+\omega_m^1+\omega_m^3) & \omega_m^3 g_1 & \cdots & \omega_m^3 g_\alpha & \cdots & \omega_m^3 \bar{g}_\beta \\ 0 & \ddots & \omega_m^3 g_1 & \cdots & \cdots & \omega_m^3 \bar{g}_{\beta-1} \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \delta & \vdots & \ddots & -(\lambda+\mu_\alpha+\delta) & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ \delta & 0 & \vdots & 0 & \ddots & -(\lambda+\mu_\beta+\delta) \end{pmatrix}.$$

where $\bar{g}_j = \sum_{l=j}^{\infty} g_l$. For $k = 1,2,\cdots$, let us define $\bar{d}_k$ as follows:

$$\bar{d}_k = \sum_{j=k}^{\infty} d_j = (1-d)^{k-1}.$$

Then, the matrices B_k, for $k = 1,2,\cdots$, are as follows:

$$B_0 = A_1 + B_1 = A_1 + A_2 + \cdots,$$
$$B_1 = U + \omega_m^1 \bar{d}_1 V = U + \omega_m^1 V,$$
$$B_k = \omega_m^1 \bar{d}_k V = \omega_m^1 (1-d)^{k-1} V,\ k = 2,\cdots.$$

The matrix A is defined as follows:

$$A = \sum_{k=0}^{\infty} A_k = \lambda I + A_1 + U + \omega_m^1 V.$$

The matrix A implies the transition rate matrix for the system state. Therefore, we obtain the probability vector $\boldsymbol{\pi}$ in (2) by solving the following linear equations:

$$\boldsymbol{\pi}A = 0,$$
$$\boldsymbol{\pi}\mathbf{e} = 1,$$

where $\mathbf{e}$ is a column vector of size $(\beta+1)$ and the elements are all 1.

The matrix R in (2) is the square matrix of size $(\beta+1)$ and satisfies the following equation

$$\lambda I + RA_1 + R^2U + \omega_m^1 d\left[I - (1-d)R\right]^{-1}R^2V = 0.$$

Solving the above equations iteratively, we can obtain R in (2) as follows.

$$R_0 = -\lambda A_1^{-1},$$
$$R_k = -\left[\lambda I + R_{k-1}^2U + \omega_m^1 d\left[I - (1-d)R_{k-1}\right]^{-1}R_{k-1}^2V\right]A_1^{-1},$$

where $k = 1,2,\cdots$.

ACKNOWLEDGMENT

This paper was supported by the 2013 Hannam University Research Fund. This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2011-0025512).

REFERENCES

[1] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Transactions on Information and System Security*, vol. 5, pp. 438-457, 2002.

[2] C. D. Huang and J. H. Goo, "Investment decision on information system security: A scenario approach," *Americas Conference on Information Systems 2009*, August 2009.

[3] K. Tatsumi and M. Goto, "Optimal timing of information security investment: A real options approach," *Workshop on the Economics of Information Security 2009*, June 2009.

[4] H. H. Kong, T. S. Kim, and J. D. Kim, "Evaluation of information security investments: A BSC perspective," *Journal of Intelligent Manufacturing*, vol. 23, no. 4, pp. 941-953, 2012.

[5] H. M. Park, W. S. Yang, and K. C. Chae, "Analysis of the GI/Geo/1 Queue with Disasters," *Stochastic Analysis and Applications*, vol. 28, pp. 44-53, 2010.

[6] W. S. Yang, D. E. Lim, and K. C. Chae, "Maintenance of deteriorating single server queues with random shocks," *Computers and Industrial Engineering*, vol. 57, pp. 1404-1406, 2009.

[7] A. B. AL-Badareen, M. H. Selamat, M. A. Jabar, J. Din, and S. Turaev, "The impact of software quality on maintenance process," *International Journal of Computers*, vol. 5, no. 2, pp. 183-190, 2011.

[8] T. Mantoro, M. A. Ayu, G. Brotosaputro, N. F. Ain, and N. Ghazali, "NFC secured online transaction in mobile computing business," *International Journal of Computers and Communications*, vol. 6, no. 4, pp. 265-273, 2012.

[9] T.-H. Kim, "Securing communication of SCADA components in smart grid environment," *International Journal of Systems Applications, Engineering & Development*, vol. 5, no. 2, pp. 135-142, 2011.

[10] C. Boja, P. Pocatilu, and A. Zamfiroiu, "Data security in m-Learning messaging services," *International Journal of Computers and Communications*, vol. 5, no. 3, pp. 198-205, 2011.

[11] K. J. Soo Hoo, *How Much is Enough? A Risk-Management Approach to Computer Security*, Stanford University, Palo Alto, CA, 2000.

[12] L. A. Gordon, M. P. Loeb, and W. Lucyshyn, "An economics perspective on the sharing of information related to security breaches," In *Proceedings of Workshop on the Economics of Information Security*, 2002.

[13] E. Gal-Or and A. Ghose, "The economic incentives for sharing security information," Working Paper, University of Pittsburgh and Carnegie Mellon University, 2004.

[14] I.S. Shin, "Review the economics means to information security," *Information Security Review*, vol. 1, no. 1, pp. 27-40, 2004 (in Korean).

[15] R. Anderson, "Why information security is hard-an economic perspective," *Proceedings of Computer Security Application Conference*, pp. 358=365, 2001.

[16] H. Cavusoglu, B. K. Mishra, and S. Raghunathan, Optimal Design of IT Security Architecture, Working Paper, University of Texas at Dallas, 2002.

[17] J. D. Kim and J. E. Park, "A study on TCO-based return on security investment (ROSI)," *Proceedings of the Korea Digital Policy Conference*, vol. 1, pp. 251-261, 2003 (in Korean).

[18] J. S. Lee and H. J. Lee, "Evaluating information security investment using TCO-based security ROI," *Proceedings of the Korea Information Processing Society Conference*, pp. 1125-1128, 2007 (in Korean).

[19] M. Al-Humaigani and D. B. Dunn, "A model of return on investment for information systems security," *Circuits and Systems*, vol. 1, pp. 483-385, 2003.

[20] T. Tsiakis and G. Stephanides, "The economic approach of information security," *Computers and Security*, vol. 24, no. 2, pp. 105-108, 2005.

[21] K. Hausken, "Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability," *Information Systems Frontiers*, vol. 8, no. 5, pp. 338-349, 2006.

[22] A. Davis, "Return on security investment-proving it's worth it," *Network Security*, vol. 2, pp. 8-10, 2005.

[23] C. Blatchford, "Information security controls are they cost-effective," *Computer Audit Journal*, vol. 3, pp. 11-19, 1995.

[24] V. C. S. Lee, "A fuzzy multi-criteria decision model for information system security investment," *Lecture Notes in Computer Science*, vol. 2690, pp. 436-441, 2003.

[25] H. Cavusoglu, H. Cavusoglu, and S. Raghunathan, "Economics of IT security management: Four improvements to current security practices," *Communications of the Association for Information System*," vol. 14, pp. 65-75, 2004.

[26] L. D. Bodin, L. A. Gordon, and M. P. Loeb, "Evaluating information security investments using the analytic hierarchy process," *Communications of the ACM*, vol. 48, pp. 79-83, 2005.

[27] D. Scott, *Security Investment Justification and Success Factors*, Gartner, Stamford, 1998.

[28] B. Blakely, "Returns on security investment: An imprecise but necessary calculation," *Secure Business Quarterly*, vol. 1, no. 2, pp. 27, 2001.

[29] R. J. Witty, J. Girard, J. W. Graff, A. Hallawell, B. Hildreth, N. MacDonald, W. J. Malik, J. Pescatore, M Reynolds, K. Russell, V. Wheatman, J. P. Dubiel, and A. Weintraub, *The Price of Information Security*, Gartner, Stamford, 2001.

[30] S. Harris, *CISSP All-in-One Exam Guide*, McGraw-Hill, New York, 2001.

[31] C. A. Roper, *Risk Management for Security Professionals*, Butterworth-Heinemann, London, 1999.

[32] H. G. Sun, "A study on the effect of information security policy and organiation on the performance of information security," *Proceedings of the Korea Management Information Systems International Conference*, pp. 1087-1095, 2005.

[33] K. H. Hong, *A Study on the Effect of Information Security Controls and Processes on the Performance of Information Security*, Kook-Min University, Seoul, South Korea, 2003 (in Korean).

[34] S. H. Nam, *An Empirical Study on the Impact of Security Events to the Stock Price in the Analysis method of Enterprise Security Investment Effect*, Korea University, Seoul, South Korea, 2006 (in Korean).

[35] Y. O. Gwon and B. D. Kim, "The effect of information security breach and security investment announcement on the market value of Korean firms," *Information Systems Review*, vol. 9, no. 1, pp. 105-120, 2007 (in Korean).
[36] M. F. Neuts, *Matrix-Geometric Solutions in Stochastic Models: An Algorithmic Approach*, The Johns Hopkins University Press, Baltimore, 1981.
[37] H. W. Lilliefors, "Some confidence intervals for queues," *Operations Research*, vol. 14, pp. 723-727, 1966.
[38] W. Mendenhall,, R. Scheaffer, and D. D. Wackerly, *Mathematical Statistics with Applications*, 3rd edition, Duxbury Press, Boston, 1986.

Won Seok Yang received his master's degree and Ph.D. from KAIST (Korea Advanced Institute of Science and Technology), Daejeon, Korea. Currently, he is a professor of Department of Business Administration at Hannam University. His research interests include stochastic modeling, queueing theory, production management, telecommunication networks and policy, information security.

Tae-Sung Kim is a professor at the Department of Management Information Systems at Chungbuk National University. He received his bachelor, master, and doctoral degrees in Management Science from Korea Advanced Institute of Science and Technology (KAIST). He worked for Electronics and Telecommunications Research Institute (ETRI) as a Senior Researcher for more than three years. Also, he worked as a visiting professor at the Department of Business Information System and Operation Management, the University of North Carolina at Charlotte and a visiting research scholar at the School of Computing, Informatics and Decision Systems Engineering, Arizona State University. His research areas include management and policy issues in telecommunications and information security. His recent research papers have appeared in international journals, such as European Journal of Operational Research, ETRI Journal, Journal of the Operations Research Society, Journal of Intelligent Manufacturing, Operations Research Letters, and Stochastic Analysis and Applications.

Eun Saem Yang received her master's degree and Ph.D. from Kangwon National University, Chuncheon, Korea. She is currently working as a professor of Department of Computer Engineering at Hallym University. Her research interests include mobile and wireless systems, interworking of heterogeneous wired and wireless networks and mobility management.