한국산학기술학회논문지
Vol. 7, No. 6, pp. 1185-1193, 2006

인터넷에서 정보시스템의 생존성 관리 모델

김황래[1*], 박진섭[2]

A Study on Survivability Management Model for Information Systems Over Internet

Hwang-Rae Kim[1*] and Jin-Sub Park[2]

요 약 차세대 인터넷과 같은 무한 네트워크에서 정보시스템은 다양한 공격과 사고의 발생으로 손상을 입고 그 사용자들은 막대한 비용의 손실을 입는다. 본 논문에서는 보안 시스템의 비용-효과 측면에서 적정수준의 투자를 할 수 있는 효과적인 의사결정을 지원할 수 있도록 하는 정보시스템의 생존성 관리 모델을 제안하였다. 시뮬레이션을 통하여 서비스 가중치를 고려한 비용에 따라 생존성이 어떻게 변화하는지를 검사하였다. 방어 비용이 방어 수준에 따라 변화하기 때문에 비용/생존성과 서비스 가중치/생존성 그래프를 도출하여 관리자가 적정 수준의 보안을 유지하는 방어 비용을 결정할 있도록 하였다.

Abstract The next generation networked information system over unbounded internet is open to various network attacks and incidents, so many users suffer from damage and financial loss. In this paper we propose a survivability management model to evaluate the tradeoffs between the cost of defence mechanisms for information systems with weighted service and the resulting expected survivability after a network attack or occurrence of incidents.

By varying the level of defence in the simulation, we examine how survivability changes according to the defense level. We derive a cost/survivability and weighted service/survivability curve that managers can use to decide on the appropriate level of defense for the network system of their organizations.

Key words : Network security, Survivability, Internet

1. 서 론

오늘날 정보시스템은 웹과 통신 기술의 비약적인 발전으로 무한 네트워크에 서로 연결되어 있다. 개인과 기업이 컴퓨터 네트워크에 대한 의존도가 높아지고, 접근의 용이성으로 인하여 더 많은 잠재적인 공격자들의 접근을 허용하기 때문에 네트워크 시스템에 대한 보안 취약성이 훨씬 더 증가하게 되었다[1][3][9].

다양한 불법적인 공격이 무한 네트워크에서 불가피하게 발생할 것이며, 공격자들은 시스템에 치명적인 손상을 입히고 사용자에게 막대한 손실을 줄 것이다. 공격에 의한 피해와 비용은 해마다 증가하고 있으며, 또한 정보화 역기능의 증가로 인해 공공기관은 물론 산업분야에서도 정보보호대책이 날로 증가하고 있고, 인터넷 이용의 대중화로 개인에게도 기본적인 정보보호 능력을 갖추는 것이 필요하게 되었다. 그러므로 시스템 관리자와 연구자, 그리고 개인 사용자들에게 있어 정보시스템의 보안을 개선하는 일이 필요하다[2][4]-[6].

그러나 절대적 보안이란 없으므로 실제적인 문제는 임의의 공격에 대비해 어느 수준으로 방어 장치를 설치하는가이다. 보안성을 향상시킬 때 제한된 비용에서 얼마만큼의 효과로 향상시킬 수 있는 지를 결정하는 것이 중요하다. 즉, 시스템 관리자는 정보시스템에 대한 네트워크 보안을 어떻게 효율적으로 향상시킬 것인지를 결정해야 한다.

이와 같이 네트워크 보안 수준을 효율적으로 향상시키기 위해서는 비용/효과 분석을 하는 것이 필요하다. 비용은 공격에 대해 시스템과 사이트를 보호하기

[1]공주대학교 컴퓨터공학부
[2]대전대학교 컴퓨터공학부
*교신저자: 김황래(plusone@kongju.ac.kr)

위해 설치되는 다양한 방어 장치들에 대한 비용이고, 그 효과는 정보시스템의 생존성을 의미한다. 생존성은 공격, 장애, 사고 등이 발생하였을 경우에도 적절한 방식을 통하여 임무를 수행할 수 있는 시스템의 능력, 즉 시스템의 회복정도를 의미한다[1][9][13][16]. 그러므로 비용/효과 면에서 네트워크 정보시스템의 생존성을 평가하고 향상시키는 방법의 연구가 필요하다.

따라서 본 논문에서는 무한 네트워크에서 정보시스템의 다양한 생존성 척도를 유도하여 시스템 내의 보안에 대한 비용/효과 분석을 위한 방법론적인 기본구조를 구축하였으며, 서비스 가중치에 대한 상대적인 효과 분석 방법을 제공하고, 시스템 보안과 생존성 관리를 위한 의사결정 지원 시스템의 모델로 개발되기 위한 방안을 제시하였으며, 시뮬레이션을 통하여 비용/효과 면에서 생존성을 분석하고 평가하였다.

본 논문의 나머지 부분은 다음과 같이 구성되어 있다. 2장에서는 생존가능 시스템의 개념 및 관련 연구에 대하여 기술하고, 3장에서는 생존성 관리 모델을 제안하며, 4장에서는 시뮬레이션 및 분석에 대해 기술하고, 5장에서는 결론 및 향후 연구 방향에 대해 기술한다.

2. 생존 가능 시스템

2.1 시스템 생존성의 개념

생존성은 공격, 장애, 사고 등이 발생하였을 경우에도, 적절한 방식을 통해 임무를 수행할 수 있는 시스템의 능력으로서 정의된다. 네트워크에서의 정보시스템 생존성은 중앙 제어 및 관리를 요구하는 전통적인 보안 대책과는 달리, 중앙 집중적이지 않고, 통일된 보안 정책을 갖고 있지 않은 고도로 분산되고 분리된 새로운 환경에서 다루어진다. 생존성은 시스템이 침입당하거나 손상된 경우에도 필수적인 서비스를 전달하고, 필수적인 자산을 보존하는 것에 초점을 둔다[1]. 생존성은 새롭게 부상하는 분야로서, 기존의 보안, 고장 허용성, 신뢰성, 재사용 등의 개념을 포함하는 개념이라 할 수 있다.

2.2 생존 가능 시스템의 요구사항

생존성 요구사항에 대한 정의와 분석은 시스템 생존성을 성취하기 위한 첫 번째 단계이다[15,16]. 이와 같은 요구사항에 대한 정의가 그림 1에서 보여주고 있다. 생존성은 소프트웨어 기능을 위한 요구사항 뿐만 아니라 소프트웨어 이용, 개발, 운용, 개선을 위한 요구사항이 제시되어야만 한다. 그러므로 5가지의 요구사항에 대한 정의가 되어 있는 이 모델이 생존 가능 시스템과 관련된다.

2.3 관련 연구

컴퓨터시스템에서의 공격의 본성에 대한 광범위한 분석과 컴퓨터 보안 위반에 대한 데이터의 분석을 기술하는 연구와, 네트워크 시스템 환경에서의 생존성의

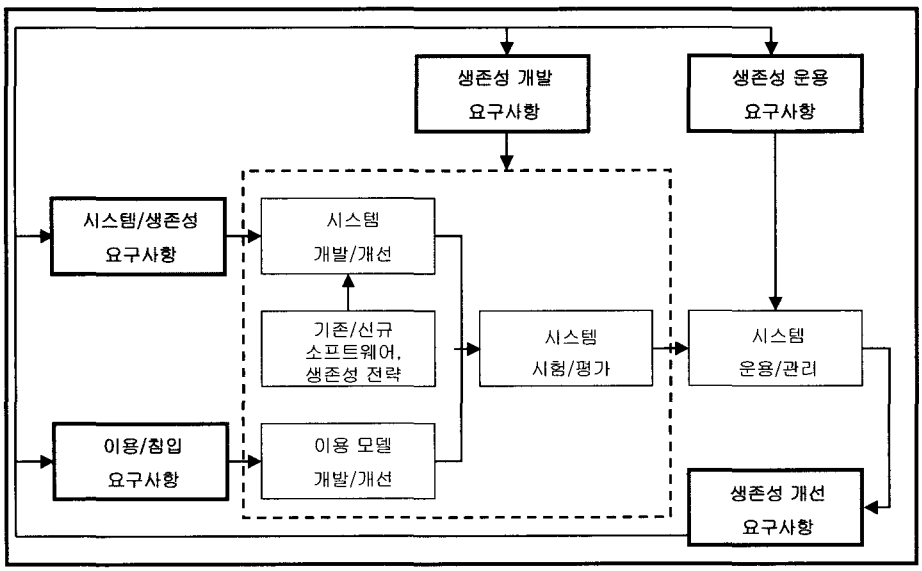


그림 1. 생존 가능 시스템에 대한 요구사항

문제를 논의하고, 향후 연구에 필요한 일련의 요소들을 제안한 연구가 있다. 또한 네트워크 시스템의 생존성 분석을 중요한 문제로 확장시키고 시스템 생존성을 위한 요구사항을 정립한 연구 및 분산시스템 환경하에서의 생존성 향상을 위한 방법을 제시한 연구 등이 있다. 이와 같은 연구들은 개념적인 면에서 생존성을 접근하였다[1][9][10][12].

또한 네트워크의 위상만을 고려한 연구가 있는데, 이는 링크 또는 노드 고장 등이 연구의 대상이었다. 이들 연구는 네트워크 위상이 생존성에 미치는 영향, 또는 노드의 단순한 고장이 생존성에 미치는 효과 등에 초점이 맞추어져 있다[9][13].

시스템 생존성은 사고에 대해 시스템이 어떻게 반응하는 지에 달려 있으며, 방어 장치인 보안 시스템의 구성에 따라 달라진다. 이 반응을 사고 유형과 방어 장치의 작용으로 평가하며, 사고 발생 과정은 사고 발생 후 시스템이 도달하게 될 가능한 상태에 대한 확률로 표현되며, 이 확률은 사고 유형 및 보안 시스템 구성에 따라 달라진다[7][8].

이러한 연구들은 시스템의 생존성을 향상시키는 기반 기술들에 관한 것이며, 정책적이며 관리적으로 생존성을 향상시키는 방안에 관한 연구는 미흡한 상태이다.

3. 정보시스템의 생존성 관리 모델의 제안

3.1 생존성 관리 모델

본 논문에서 제안한 정보시스템의 생존성 관리 모델은 그림 2와 같다. 시간에 따라 일련의 사고를 겪었을 때 사고 발생에 따른 시스템의 상태 정보를 나타내는 변환행렬을 이용하여 정보시스템의 생존성을 측정하는 것이다. 우선 오랜 시간에 걸쳐 사고 과정을 경험한 시스템이나 사이트로부터 사고 발생 과정을 예상한다. 이 과정은 시간 내에 사고가 임의의 시점에서 발생하는 확률 점 과정과 동일하다.

제안된 모델을 통하여 여러 가지 시나리오에서 다양한 방어 장치의 비용과 효과를 분석할 수 있다. 이런 분석을 기초로 시스템 관리자들은 그들의 요구에 가장 적합한 보안 시스템 구성을 결정할 수 있다.

제안한 모델은 미래의 공격과 그 영향에 대한 불확실성이 높은 상황에서 본 모델을 통하여 생존성을 평가하고 관리하기 위한 실질적인 접근 방안을 제시한다.

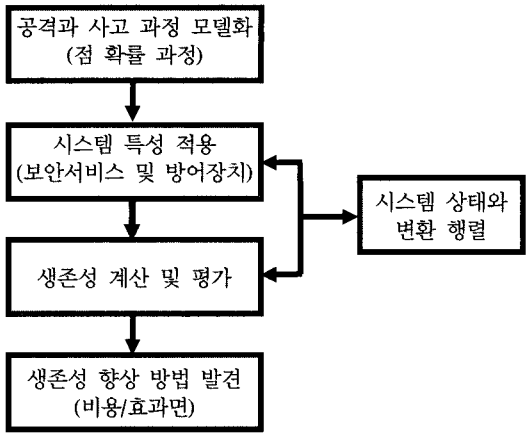


그림 2. 정보시스템 생존성 관리 모델

3.2 기호의 정의

본 논문에서 제안된 모델에 사용되는 기호는 다음과 같다.

① i,j = 사고 유형 공간 {M}의 인덱스
② P(m) = 어떤 사고가 유형 m일 확률
③ τ (i,j) = 사고 i와 j사이의 시간 간격
④ a = 사고 도착률 = $1/\tau$
⑤ r,s = 시스템 상태에 대한 인덱스, {S} 안의 r,s
⑥ d = 시스템 설계 공간 {D}의 d
⑦ b = 방어장치 공간 {B}의 b
⑧ c = 구성 공간 {D x B}에서의 한 구성 c, 설계 x 장치
⑨ T = {p(r,s)} 원소를 갖는 변환 확률 행렬, {p(r,s)}는 i,j,d,b 의 함수임
⑩ l - 사이트 공간 {L} 안의 l
⑪ h(l) = 개별 사이트 l의 사고에 대한 인덱스: h(l) = 1,2,3, ...
⑫ H(l) = 사이트 l에서의 사고의 총 횟수
⑬ t(h(l),l) = 사이트 l에서 h번의 사고 시간

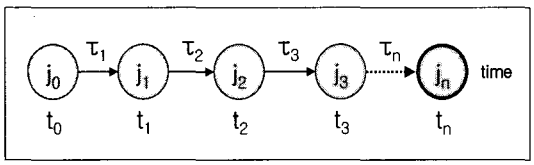
$$= \sum_{k=1}^{k=h} \tau(k),\ \tau(k) = t(k) - t(k-1)$$

⑭ n = 동시 공격 사이트의 수

3.3 사고 과정의 모델화

사고는 주어진 시간 내에 임의의 시점에서 발생하는 사건이고, 사고유형은 사고와 관련된 마크로 표시하고, 점-확률 과정으로 모델화 한다[7, 8]. 마크는 사고가 일어나는 시점과 관련된 임의량을 확인하기 위해 사용된다. 이 모델의 마크 혹은 사고유형에서는 유형의 종류와 동시 공격의 가능성 그리고 사고의 심각성 정도를 고려해야 한다. 왜냐하면 분산 개방형 네트

워크 환경에서 발생되는 과정으로 모델링하기 때문이다[11]. 그러므로 기호 공간은 2차원적이며, 사고의 심각성과 공격자수에 의해 특성이 구별될 것이다. 비록 2차원적 마크 확률 과정으로 모델이 만들어졌다 하더라도 사고마다 공격자수 분포에 대한 데이터는 얻을 수 없다. 그래서 사고유형의 심각성에 따른 1차원적 마크 공간만이 시뮬레이션에서 사용되었다. 그림 3과 같이, 시간적 점-과정에서 k번째 사고의 발생시간 tk는 연관된 마크 jk를 가지며, jk는 지정된 공간에서의 값을 갖게 된다.



$\tau_{i\ (i=1,2,\ldots,n)}$: 사고 발생 간격

$t_{i\ (i=1,2,\ldots,n)}$: 사고 발생 시간

$j_{i\ (i=1,2,\ldots,n)}$: 각 사고(사고유형)와 관련된 마크

그림 3. 점-확률 과정

점-확률 과정은 일반적으로 $\{x(t) : t \in T\}$로 표현될 수 있다. 여기서 $\{x(t) : t \in T\}$는 파라미터 t로 인덱스 되는 확률변수의 집합이며, 파라미터 t는 확률과정의 인덱스 집합인 파라미터 집합 T에 속한 값이다. 이 모델에서 t는 시간을 나타내는데, T는 실제 시간 공간 R의 부분집합이기 때문에 연속적인 파라미터의 과정이다. 점-확률 과정 $\{x(t) : t \in T\}$는 완전히 통계적으로 다음과 같은 결합(joint) 분포함수의 특징을 갖는다.

$$P_{x(t_1),x(t_2),\ldots,x(t_k)}(X_1, X_2, \cdots, X_k) = \Pr(x(t_1) \le X_1, x(t_2) \le X_2, \cdots, x(t_k) \le X_k)$$

확률변수 x(t1), x(t2), ..., x(tk)에 대해 결합 분포함수는 다음과 같다.

Px(t1), x(t2), ... x(tk)(X1, X2, .., Xk)
= Pr(x(t1)≤X1, x(t2)≤X2, .., x(tk)≤Xk)

사고간격(τ)의 확률밀도함수 f(t)는 다음과 같다.

f(t)=Pr{t≤τ ≤t+dt}

이 과정이 포아송(Poisson) 분포일 때, 밀도함수 f(t)는 다음 식으로 주어지며,

$$f(t) = a^* e^{-at}$$

여기서 a는 사고발생률이며, 확률분포함수 F(t)는 다음과 같다.

$$F(t) = 1 - e^{-at}$$

3.4 정보시스템 상태 변환 모형

시스템이 공격에 의하여 상태가 변하기 때문에 시스템 설계와 시스템에서 사용하는 방어장치에 대한 규정이 필요하다. 시스템의 설계 공간 {D}와 방어장치 공간 {B}의 조합이 구성 공간 {D x B}이 된다. 모든 가능한 구성공간을 고려할 수 없으므로 본 논문에서는 한가지 설계만 고려하였다.

반응 예측 모델에서 하나의 공격/사고가 발생한 후 시스템은 새로운 상태로 전이되며, 이 전이는 사고유형과 구성에 대한 함수 또는 조건부 확률 p(r,s)=p(r,s|m,d,b)이 될 것이다. 그러므로, 사고유형 m과 초기시스템 상태 r이 주어지면 다음 상태 s는 정상, 가벼운 손상, 중대한 손상, 매우 심각한 손상, 고장 등 시스템의 가능한 상태 집합 {S}의 한 요소가 된다. 실제 상태는 물론 구성에 따라 다를 것이다. 전이행렬 T는 m,d,b가 주어지면 확률적으로 r을 s로 매핑한다. 즉, T의 각 요소는 사고유형 m을 겪을 때, 설계 d와 방어장치 b를 가지는 시스템이 다른 상태로 전이하는 확률이다.

본 모델에서는 T의 구조를 다음과 같이 가정한다. 일반성을 유지하면서 그 상태가 손상정도에 의해 순서화 된 것이라고 가정한다. 즉, 손상정도는 s=1=정상(완전기능)에서 s=0=(완전)고장까지이다. 사고가 발생하면 시스템은 결코 나은 상태로 가지 않는다. 그러므로 행렬 T의 대각선 축 아래 삼각형 모양에서 보이듯이 구조상 0을 갖는다.

$$T = \begin{bmatrix} p11 & p12 & p13 & p14 & p15 \\ 0 & p22 & p23 & p24 & p25 \\ 0 & 0 & p33 & p34 & p35 \\ 0 & 0 & 0 & p44 & p45 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

각 상태에서 변환확률이 구해지면, 데이터를 직접 모델에 입력할 수 있다. 그렇지 않으면, 변환확률 행렬 T의 요소 {p(r,s)}를 생성시키는 모델을 전개하거나 시스템이 경험하게 되는 공격-반응 에피소드 동안 중간상태를 고려하여 확률을 계산할 수 있다.

본 모델에서의 시스템 상태 변환 모형은 그림 4와 같다.

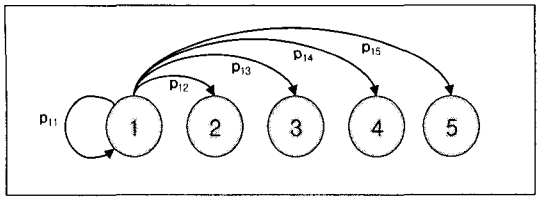


그림 4. 시스템 상태 변환 모형

시스템은 초기 상태와 마찬가지로 항상 정상 상태에서 사고가 발생하기 때문에 상태 변환 확률, 정상상태에서 상태 s로 변환할 상태전이확률 $p(1,s)$를 생성하는 식을 다음과 같이 제안한다.

p(1,s)=p(s,m,cost(b); π 0,μ 0,π ₁ ,π ₂ ,μ ₁ ,μ ₂)
여기서 s=1과 s 〉 1인 2 가지 경우로 나누었다.

정상상태에서 정상상태로 전이할 확률 p(1,1)은

$p(1,1) = \pi_2 * (1 - e^{-\pi_1(\cos t(b) - \pi_0)})$ 이고,

정상상태에서 손상상태로 전이할 확률 p(1,s)는

$p(1,s) = \mu_2 * (1 - e^{-\mu_1(\cos t(b) - \mu_0)})$ 이다.

이들 함수식은 비용에 따라 감소하는 결과를 나타내며, π ₁ 과 μ ₁ 은 방어장치 비용인 cost(b)에 따른 변환확률을 결정하는 중요 계수이다. 이는 또한 생존성이 비용에 따라 어떻게 변화하는지를 결정한다.

π_2는 선형 함수로 $\pi_2 = \pi_3 * j$ 이다. 그리고

$\mu_2 = \mu_2(m,s) = \mu_3 * ((6-s) - (.4*m))$ 이며, s와 m의 선형함수이다.

상수뿐만 아니라 계수 π_3 와 μ_3는 위에서 주어진 모든 제한 조건에 따르는 전이확률의 적절한 값을 구하기 위함이며, 위치 계수 π_0 와 μ_0는 0으로 설정되고, π_1, μ_1, π_3, μ_3 등은 시뮬레이션 동안 변화한다.

3.5 생존성의 계산

생존성은 공격들에 견딜 수 있는 정도와 공격 후의 새로운 상태에서 어느 정도의 서비스를 제공하는가의 능력을 말한다. 새로운 상태 s는 일반적으로 손상상태가 될 것이며, 시스템이 완전히 회복하기 전의 상태 또는 정상상태로 복구하기 위해 수리되는 상태를 뜻한다. 개념적 수준에서 생존성을 다음과 같이 정의한다.

$$SV = \frac{\text{새로운 상태에서의 성능 수준 } s}{\text{정상 성능 수준}}$$

성능 수준의 측정은 공격 후 새로운 시스템 상태에서 각 기능이 어느 정도 제공되는가의 척도이다. 정해진 기능이 본래대로 회복한다면, 그 값은 1이 되고, 시스템이 그 서비스를 완전히 제공하지 못하면 0의 값이 된다. 중간상태는 0과 1사이의 값을 갖게 된다.

φ (s,u)를 손상된 서비스 u가 상태s에서 생존하는 정도라고 가정하고, ω (u)를 서비스의 중요도라고 가정하면 생존성에 관한 한가지 측정 방법은 다음과 같이 가중치 합계의 형태가 될 수 있다.

$$SV(s) = \sum_u \omega(u) * \phi(s,u)$$

여기서 시스템의 완전 상태집합 {S}가 정의되고, 시스템 분석가나 정보시스템 관리자가 각각의 u와 s에 대한 φ (s,u)을 측정할 수 있다고 가정한다. φ (s,u)는 각 s 상태에서 서비스 u가 생존하는 평균 수준이 된다. 정보시스템이 높이 평가하는 특별한 서비스가 있다면 이의 가중치는 매우 높을 것이며, 이 서비스에 대한 생존성은 가벼운 손상을 입을 지라도 낮게 될 것이다. 그러면 이 기능을 보호하는 방어장치는 높은 비용을 부여하여 높은 효과가 될 것이며, 반면에 이 기능을 보호하지 못한 방어 장치는 낮은 값을 부여하여 낮은 효과를 얻을 것이다.

서비스의 가중치 ω (u)는 $0 \le \omega(u) \le 1$ 이며, 가중치의 합은 1이다.

$$\sum_u [\omega(u)] = 1$$

.

φ (s,u) 값들은 $0 \le \varphi(s,u) \le 1$로 정규화된 수치이다. 그러면 SV(s)는 0과 1사이가 되며, 여기서 0은 완전고장, 1은 완전한 정상을 의미한다.

또 다른 척도는 상대적 생존성 척도이다. 이것은 정상상태에서 u의 최대 서비스 수준 Y(u)를 고려하며, 요구되는 기능 수준 y(u)는 $0 \le y(u) \le Y(u)$가 된다. 상태 s에서 서비스 u가 생존할 정도를 y'(u,s)라고 하면, 요구사항에 대한 상대적 생존성을 다음과 같이 정의할 수 있다.

$$\phi'(u,s) = \frac{y'(u,s)}{y(u)} \quad y' < y \text{인 경우,}$$
$$\phi'(u,s) = 1 \quad y' > y \text{인 경우.}$$

y' 〈 y 이면 상대적인 생존성은 정상 상태에 대한

생존의 정도로 정의될 수 있고, y' 〉 y 이면 생존수준이 요구되는 것보다 더 높기 때문에 φ '(u,s) = 1이다.

여러 실제 상황에서 시스템 취약성에 대한 모든 가능성을 항상 인식 할 수는 없다. 그러나 취약성이 주어지면, 발생할 수 있는 모든 손상들의 집합을 열거할 수는 있다. 그런 경우에 다음과 같이 처리할 수 있다.

서비스 u가 사고유형 m에 의해 y 정도로 손상될 확률이 $p_{mj}(y)$로 주어진다면, 모든 u에 대한 전체적인 손상을 시뮬레이션 할 수 있고, 각 사고 후의 생존성을 계산할 수 있다. 그리고 m에 대해 예상되는 손상기대치 E[y(u,m)]를 계산할 수 있다.

여기서 $0 \le y \le 1$로 가정할 때,

$$E[y(u,m)] = \int_0^1 y^* p_{um}(y)dy$$

이고, 각 사고 후의 생존성을 다음과 같이 계산할 수 있다.

$$SV \mid m = \sum_u \omega(u)^*(1 - E[y(u,m)]$$

차세대 인터넷에서는 서비스 집합 {U}를 {U_0, U_1, U_2, U_3}로 나눌 수 있다. 여기서 U_0는 중요하지 않은 일반 서비스의 집합을, U_1은 매우 자주 사용되나 중요하지 않은 고용량 고품질 서비스의 집합, U_2는 대화형 작업, U_3은 필수적인 임계 서비스들의 집합이다. 이 경우의 생존성은 다음과 같이 계산된다.

$$SV(s) = [\prod_u \phi(s,u')^{\omega(u')}]^*[\sum_u \omega(u)^*\phi(s,u)]$$

곱의 형식은 필수적인 서비스가 고장나면 생존성이 0이 됨을 나타낸다.

4. 시뮬레이션 결과와 분석

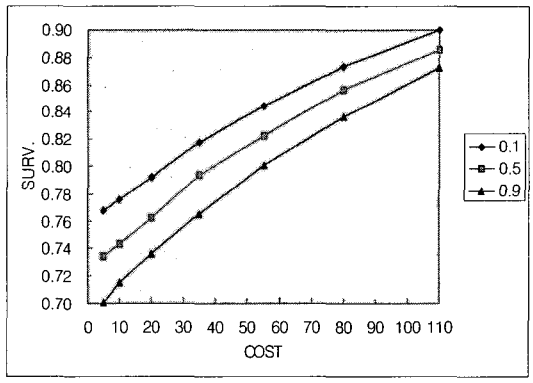
생존성의 영향은 분명히 시스템에 설치된 방어장치의 수준과 공격의 수준 모두에 달려있다. 강력한 방어장치를 가진 시스템일수록 정상상태에서 공격에 잘 견뎌내고 시스템의 손상 정도는 작아진다. 다시 말해서 시스템에서의 변환 확률은 방어장치에 대한 함수이고, 이 함수를 통하여 어떠한 공격 시나리오에 있어서든 시스템의 생존기대값을 계산한다. 그러므로 시뮬레이션은 사고유형, 방어장치의 비용 변화, 그리고 시스템 상태 변환 확률을 가지고 수행되었다.

아래 분석 결과들은 본 모델의 시뮬레이션 수행 결과 할 수 있는 모든 분석에 대한 일부분으로서 접근방법의 잠재력을 보여준다. 어떠한 사고 과정도 만들 수 있고, 어떠한 시스템 반응도 변환 행렬을 통해 모델에 적용할 수 있다. 그러므로 이 모델을 사용하여 어떤 시나리오에서든 어떤 방어장치 설정에서든 발생되는 손상과 생존성을 조사할 수 있다. 방어 장치 비용이 주어지면 아래에서 보여주듯이 생존성/비용 곡선을 유도할 수 있고 방어비용에 대한 효과적인 보안수준을 얻을 수 있다.

시스템 관리자는 생존성/비용 곡선으로부터 비용과 생존성 사이의 상관 관계를 분석하여 정보시스템의 생존성 및 서비스의 중요성 여부에 따라 최선의 선택을 할 수 있다.

4.1 사고발생률에 따른 생존성 분석

사고발생률의 변화에 따라 생존기대값의 변화 추세를 조사하였으며, 사고발생률에 따라 사고유형이 결정되게 되고 사고발생률의 증가는 심각한 사고의 발생이 많아짐을 의미한다. 그림 5는 사고 발생률과 생존성과의 관계를 나타낸다.



a=1.5, π 1=0.15, μ 1=0.008, π 3=0.25, μ 3=0.075

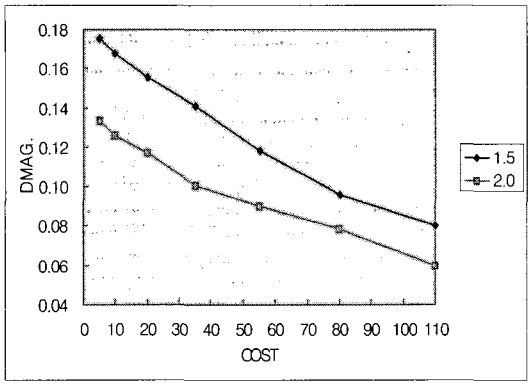
그림 5. 사고발생률과 생존성

변환 확률과 비용에 대한 관계로부터 추정되듯이 생존성은 방어장치 비용에 따라 증가하며, 사고발생률이 증가함에 따라 감소한다. 심각한 사고발생률이 높을수록 생존성은 낮아지고 비용 증가에 따라 생존성의 상대적인 민감도도 낮아진다.

4.2 평균 사고도착시간에 따른 평균피해 분석

평균 사고도착 시간의 변화에 따라 상대적인 생존성과 평균피해는 손상기대값의 합을 시뮬레이션동안 경과된 총시간으로 나누어 계산하며, 그림 6은 평균

사고도착시간에 따른 평균피해를 나타낸다.



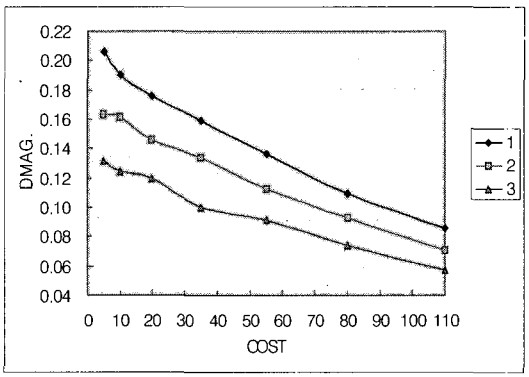
P(1)=0.5, π 1=0.15, μ 1=0.008, π 3=0.25, μ 3=0.075

그림 6. 평균 사고 도착시간과 평균피해

그림 6에서 보는 바와 같이 생존성의 상대적 변화는 없으며, 평균피해는 평균 사고도착시간에 비례함을 알 수 있다. 이것은 생존성은 사고 단위로 계산되기 때문에 평균 사고도착시간과는 전혀 무관하고, 평균피해는 시간에 의해 계산되기 때문에 평균 사고도착시간과 밀접한 관련이 있음을 의미한다.

4.3 사고유형과 평균피해 분석

다음은 사고발생률에 따른 사고유형과 평균피해의 상호관계에 대한 영향을 고려하여 시뮬레이션 하였다. 사고유형의 발생확률이 동일한 조건이라면 심각한 유형일 경우의 피해가 클 것으로 예상된다.



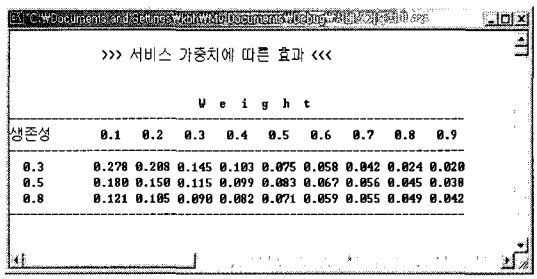
P(1)=0.5, a=1.5, π 1=0.15, μ 1=0.008, π 3=0.25, μ 3=0.075

그림 7. 사고유형에 따른 평균피해

그림 7에서 보는 바와 같이 심각한 사고유형의 시간당 평균피해가 큰 것을 확인할 수 있다. 이 결과는 j=1이 가장 심각한 사고, j=3이 가장 가벼운 사고임을 의미한다.

4.4 서비스 가중치와 생존성 분석

그림 8은 생존성의 변화에 따른 서비스의 가중치를 고려한 생존성의 상대적인 효과를 나타낸다. 그림 9의 그래프에서 보는 바와 같이 생존성의 변화와 무관하게 서비스 가중치 0.4~0.6 범위 내에서 수렴되는 지수분포를 이룬다. 이것은 시스템에서 서비스들의 중요도가 비교적 동일하다면 생존성에 전혀 민감하지 않음을 의미한다.


>>> 서비스 가중치에 따른 효과 <<<

W e i g h t

생존성	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
0.3	0.278	0.208	0.145	0.103	0.075	0.058	0.042	0.024	0.020
0.5	0.180	0.150	0.115	0.099	0.083	0.067	0.056	0.045	0.038
0.8	0.121	0.105	0.090	0.082	0.071	0.059	0.055	0.049	0.042

그림 8. 서비스 가중치에 따른 효과

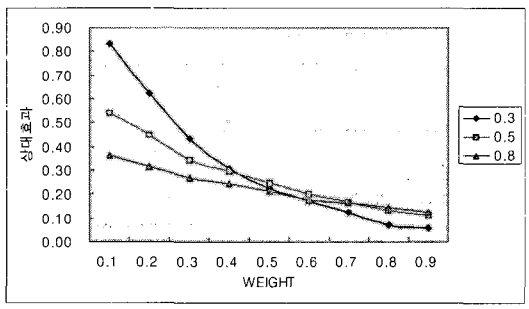


그림 9. 서비스 가중치에 따른 상대 효과

생존성이 높을수록 완만한 형태의 곡선을 이룬다. 이것은 생존성이 높은 경우보다 낮은 경우에 생존성의 상대적인 민감도가 크다는 것을 의미한다. 그러므로 특정 서비스의 중요성과 가용성이 요구되는 정보시스템일수록 일정 수준의 생존성이 보장되어야 시스템의 상태가 안정될 확률이 높아짐을 의미한다. 즉 시스템의 생존성이 향상됨을 의미하는 것이다. 그러므로 방어비용 투자 원칙에 따라 관리자들에게 자신의 조직에 가장 적합한 방어수준에 관한 결정을 할 수 있는 기준을 제공한다.

5. 결 론

본 논문에서는 분산 개방형 인터넷 정보시스템에 대한 공격과 시스템 반응을 통하여 시스템의 생존성을 추정하는 모델을 제안하였다. 제안된 모델은 평균 사고 도착시간, 사고발생률, 사고유형 사이의 상호관계, 서비스의 가중치 등 다양한 상황에 대한 분석이 가능하고, 시뮬레이션을 통하여 방어비용에 따른 시스템 생존 기대값에 대한 상관관계를 제시하였다.

사고유형과 방어 장치의 함수로 상태 변환 행렬을 확률적으로 모델화 하였다. 제안한 모델은 다양한 형태의 도착률 분포나 사고유형의 수, 방어비용의 변화 등의 조건하에서도 쉽게 적용될 수 있다. 또한 본 모델에서의 생존성 척도는 향후 시스템이 수행해야 될 기능들과 함께 하나의 서비스로 포함되어 시스템 관리자나 책임자들이 그들의 시스템 관리에 있어서 비용/효과 분석을 할 때 유용하게 사용될 수 있다. 나아가 이와 같은 발견적 방법을 활용함으로써 생존성 향상에 효율을 기대할 수 있다.

분석 결과 (1) 사고발생률이 높을수록 생존성은 낮아지고 방어비용 증가에 따라 상대적인 민감도는 작으며, (2) 서비스의 가용성과 중요성에 따라 가중치를 부여한 생존성의 효과를 분석하여 가중치의 정도에 따라 일정 수준의 생존성이 유지되어야만 하는 것을 검증하였다.

제안된 모델은 사고에 대한 네트워크 시스템의 보안을 향상시키는데 시스템 관리자들이 올바른 결정을 할 수 있도록 도와준다. 실제적으로 모델에서 요구하는 신뢰성 있는 데이터만 있으면, 관리자들은 언제든 손쉽게 자신의 시스템에 대한 생존성 평가를 통하여 (생존성/비용 곡선을 통하여) 최선에 가까운 결론을 얻을 수 있다.

본 논문에서는 몇몇 중요한 가정들을 전제로 하여 분석하였으나, 이러한 가정을 최소화 할 수 있는 방향으로의 향후 연구가 필요하다.

참고문헌

[1] Ellison, R.J.; Fisher, D.A.; Lipson, H.F.; Longstaff, T. & Mead, N.R. "Survivable Network Systems: An Emerging Discipline"(CMU/SEI- 97-TR-013 ADA 341963) Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1997.

[2] Baker, R.H., "Network Security: How to Plan for it and Achive it", New York, NY:McGraw-Hill, 1995.

[4] Boni, W.C. & Kovacich, G.L., "I-Way Robbery: Crime on the Internet", Londonm England: Butterworth-Heinemann, 1999.

[5] Cohen, F., "Simulating Cyber Attacks, Defenses, and Consequences", Fred Cohen & Associates 1999.

[6] Computer Security Institute, "Computer Security Issues and Trends", 4, 1(Winter 1988).

[7] Basawa, I.V. & Prakasa, B.L.S, "Statistical Inference for Stochastic Processes". New York, NY: Academic Press, 1980.

[8] Daley, D.J. & Vere-Jones, D. "An Introduction to the Theory of Point Processes". New York, NY: Springer-Verlag, 1988.

[9] Fisher, D.A. "Emergent Algorithms-A New Method for Enhancing Survivability in Unbounded Systems", IEEE Proceedings of the Hawaii International Conference on Systems Sciences. Wailea, HI, Jan. 5-7, 1999.

[10] Howard, J. "An Analysis of Security Incidents on the Internet(1989-1995)". Ph.D. Dissertation, Carnegie-Mellon University, Pittsburgh, PA, 1995.

[11] Law, A.M. & Kelton, W.D. "Simulation Modeling and Analysis". New York, NY: McGraw-Hill, 1982.

[12] Linger, R.C.; Mead, N.R.; & Lipson, H.F. "Requirements Definition for Survivable Network Systems". 1988 by IEEE. Proceedings of the International Conference on Requirements Engineering, Colorado Springs, CO: April 6-10, 1988. New York, IEEE Computer Society Press.

[13] Moitra, S.D.; Oki, E.; & Yamanaka, N. "Some New Survivability Measure for Network Analysis and Design". IEICE Transactions on Communications. E80-B, 4, April 1997.

[14] Snyder, D.S. & Miller, M.I. "Random Point Processes in time and Space". New York, NY: Springer-Verlag, 1991.

[15] 김봉회, 김 강, 성장렬, 박진섭, "무결성 보호 보안정책 모델 분석", 한국통신정보보호학회 충청지부 학술발표논문집 제2권 제1호, 1998. 11.

[16] 박진섭, 김봉회, "베이스라인 보안정책을 위한 위험분석 체크 리스트", 대전대학교 산업기술연구소 논문집 제8권 제2호, 1997.12.

김 황 래(Hwang-Rae Kim) [정회원]

- 1982년 9월 : 중앙대학교 전자계산학과 (이학사)
- 1991년 2월 : 중앙대학교 컴퓨터공학과 (공학석사)
- 2005년 2월 : 대전대학교 컴퓨터공학과 (박사수료)
- 1983년 3월 ~ 1994년 2월 : 한국전자통신연구원 선임연구원
- 1994년 3월 ~ 현재 : 공주대학교 컴퓨터공학부 교수

<관심분야>
컴퓨터네트워크, 네트워크보안, 무선인터넷, 네트워크 생존성 관리

박 진 섭(Jin-Sub Park) [정회원]

- 1981년 2월 : 중앙대학교 컴퓨터공학과 (이학사)
- 1983년 2월 : 중앙대학교 컴퓨터공학과 (공학석사)
- 1990년 2월 : 중앙대학교 컴퓨터공학과 (공학박사)
- 1988년 3월 ~ 현재 : 대전대학교 컴퓨터공학과 정교수

<관심분야>
컴퓨터구조, 정보통신, 네트워크 보안, 관리