정보시스템의 생존성 관리 모델

김황래*, 박진섭**
*천안공업대학 컴퓨터과
**대전대학교 컴퓨터정보통신공학부

A Survivability Management Model for Information Systems

Hwang-Rae Kim* Jin-sub Park**
* Dept. of Computer Engineering, Cheonan National Technical College
E-mail : hrkim@cntc.ac.kr
**Div. of Computer and Communications Engineering, Daejeon Univ.
E-mail : jspark@dju.ac.kr

요 약

본 논문에서는 불법적인 공격이 다양하게 발생하는 무한 네트워크에서 정보시스템에 대한 네트워크 보안 장치를 효율적으로 모색할 수 있도록 지원하고, 비용-효과적인 측면에서 서비스 수준을 유지하도록 정보시스템의 생존성 관리 모델을 제안하였다. 시뮬레이션을 통하여 시스템 관리자들이 적절한 비용으로 공격에 대비한 방어장치의 수준을 결정할 수 있도록 지원하는 방안을 제시한다.

1. 서 론

1.1 연구의 배경 및 목적

오늘날 정보시스템은 무한한 네트워크에 서로 연결되고 있으며[Ellison 97, Fisher 99], 개인과 회사가 컴퓨터 네트워크에 상당히 의존적으로 되고, 더 많은 잠재적인 공격자들이 네트워크에 접근하여 다른 시스템에 접근하기 때문에, 네트워크 시스템의 취약성이 증가하고 있다.

불법적인 다양한 공격이 인터넷과 같은 무한 네트워크에서 불가피하게 발생할 것이며, 일부 공격자들이 시스템에 손상을 입히고 사용자에게 손실을 줄 것이다. 그러한 공격에 의한 피해와 비용은 해마다 상당한 수준으로 증가하고 있다[CSI 98]. 그러므로 시스템 관리자들은 정보시스템의 보안 개선 방법을 찾는 일이 필수로 되었다.

그러나, 절대적인 보안이란 없으며, 임의의 공격에 대비해 어느 수준으로 방어장치를 설치하는가가 실제적인 문제이다. 즉, 보안을 향상시킬 필요는 있지만, 주어진 비용에서 얼마만큼의 비용으로 향상시킬 수 있을 것인지를 결정할 필요가 있다. 다시 말해, 정보시스템에 대한 네트워크 보안을 어떻게 효율적으로 향상시킬 것인지를 결정해야 한다.

네트워크 공격 위험과 비용에 대한 보안 수준을 효율적으로 향상시키기 위해서는 비용/효과 분석을 해야한다. 비용은 공격에 대해 시스템과 사이트를 보호하기 위해 설치되는 다양한 방어장치들에 대한 비용이고, 그 효과는 시스템과 사이트의 향상된 생존성이다. 생존성은 시스템이 공격으로부터 회복하는 능력 특히, 그 회복 정도를 의미한다[Ellison 97]. 그러므로 비용/효과 면에서 네트워크 정보 시스템의 생존성을 향상시키는 방법의 연구가 필요하다.

한가지 접근 방법은 공격의 발생, 시스템 반응, 공

격에 따른 영향을 시뮬레이션하고, 서로 다른 매개 변수들이 어떻게 시스템 생존성에 영향을 주는지 조사하기 위해 여러 상황을 시뮬레이션 하는 것이다. 본 논문에서는 무한 네트워크에서 정보시스템의 생존성 관리 모델들을 제안하고, 여러 조건하에서 네트워크 생존성 분석을 위해 모델을 시뮬레이션 하였다.

이를 통하여 정보 시스템의 생존성 척도를 유도하고, 시스템에서 보안의 비용/효과 분석에 대한 방법론에 관한 기본구조를 제안하며, 시스템 보안과 생존성 관리를 위한 의사결정 지원 시스템을 지원한다.

1.2 관련 연구

통신 분야에서도 생존성에 관한 많은 연구들이 행해져 왔으나, 단지 위상적 고려에 기초를 두고 있으며, 링크 또는 노드 고장 등이 연구의 대상이었다 [Moitra 97, Howard 95, Fisher 99, Ellison 97, Linger 98]. 이들 연구는 네트워크의 위상이 생존성에 미치는 영향, 또는 노드의 단순한 고장이 생존성에 미치는 효과 등에 초점이 맞추어져 있다. 이들 연구에서 정의한 컴퓨터 보안사고에 대한 공통언어를 본 논문에서 사용하고자 한다[Howard 98].

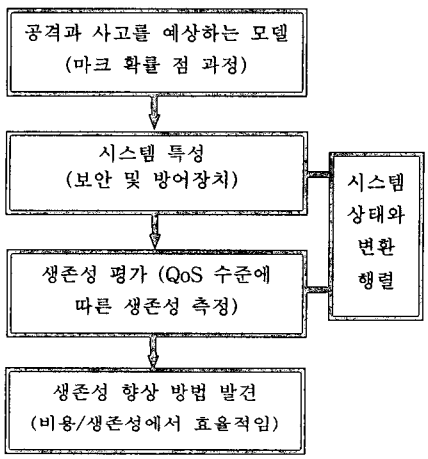
*공격*은 승인되지 않은 결과를 얻기 위해 공격자에 의해 취해진 일련의 의도적인 과정으로 정의한다. *사고*는 공격자, 공격, 목적, 사이트, 그리고 시간 등이 달라 다른 공격과는 구별이 되는 관련된 공격들이라고 정의한다.

그리고 공격의 전체 과정과 사고에 대한 시스템 반응을 뜻하는 에피소드(episode)를 [사건+반응]의 조합으로 정의한다. 또한 사이트에 관련된 컴퓨터와 네트워크 구성요소 집합체를 시스템으로 하며, 시스템 구성을 설계와 그 방어장치의 결합으로 정의한다.

1.3 접근 방법

본 논문의 접근 방식은 [그림 1]에서와 같이 시간에 따라 일련의 사고를 겪었을 때 정보시스템의 생존성을 측정하는 것이다. 우선 오랜 시간동안 사고 과정을 경험한 시스템이나 사이트의 사고 발생 과정을 모델화 한다. 이 과정은 시간 내에 사고가 임의의 시점에서 발생하는 확률 점 과정과 동일하다. 본 모델은 사고 발생 후 시스템이 도달하게 될 가능한 상태에 대한 확률을 제공하는 변환 행렬(transition matrix)로 표현되며, 이 확률은 사고 유형 및 시스템 구성에 따라 달라진다.

다음은 시스템이 생존하는 정도를 측정한다. 생존 정도는 사고 후에 시스템이 도달하는 상태와 발생한 손상 정도에 대한 함수가 된다. 이를 위해, 다른 차원에서의 생존성, 즉 손상될 수 있는 여러 기능 및 서비스의 생존성을 고려하는 몇 가지 새로운 생존성 척도를 제안한다.



[그림 1] 시뮬레이션 모델의 틀

시뮬레이션을 통하여 다양한 방어장치의 비용과 효과를 분석할 수 있다. 이런 분석을 기초로 시스템 관리자들은 그들의 요구에 가장 적합한 시스템 구성을 결정할 수 있다.

본 논문의 나머지 부분은 다음과 같이 구성되어 잇다. 2장에서는 우리가 사용할 모델을 제안하고, 3장에서는 시뮬레이션 절차와 가정을 설명한다. 4장에서는 분석결과를 기술하며, 5장에서는 분석 결과와 향후 연구분야에 대해 기술한다.

2. 모델의 정의

2.1 기호의 정의

i) i,j = 사고 유형 공간 {M}의 인덱스
ii) P(m) = 어떤 사고가 유형 m일 확률
iii) τ (i,j) = 사고 i와 j사이의 시간 간격
iv) a = 사고 도착률 = $1/\tau$
v) r,s = 시스템 상태에 대한 인덱스, {S} 안의 r,s
vi) d = 시스템 설계 공간 {D}의 d

vii) b = 방어장치 공간 {B}의 b

viii) c = 구성 공간 {D x B}에서의 한 구성 c, 설계 x 장치

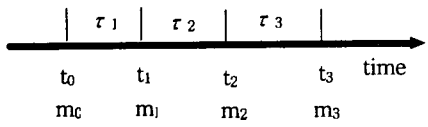
ix) T = {p(r,s)} 원소를 갖는 변환 행렬, {p(r,s)}는 i,j,d,b 의 함수임

x) l - 사이트 공간 {L} 안의 l

xi) h(l) = 개별 사이트 l의 사고에 대한 인덱스: h(l) = 1,2,3, ...

2.2 사고 과정 모델

사고는 시간내에 임의의 시점에서 발생하는 사건이고, 사건 유형은 사고와 관련된 마크로 표시하고, 마크 확률 점 과정으로 모델화 한다[Snyder 91]. 마크는 사고가 일어나는 시점과 연관된 임의량을 확인하기 위해 사용된다. [그림 2]와 같이, 시간적 점-과정에서 k번째 사고의 발생시간 t_k는 연관된 마크 j_k를 가지며, j_k는 지정된 공간에서의 값을 갖게 된다. 이 모델의 마크 혹은 사건 유형에서는 단일 혹은 다수 복합적이고 동시적인 공격 가능성과 사고의 심각성 정도를 고려해야 한다[Ellison 97]. 그러므로 마크 공간은 2차원이며, 유형(심각성)과 공격자 수에 의해 특성이 구별될 것이다. 즉, 마크공간은 {J x N}이 될 것이다. 비록 2차원 마크 확률과정으로 모델이 만들어졌다 하더라도 사고마다 공격자수 분포에 대한 데이터를 얻을 수 없다. 그래서 오직 심각성에 따른 1차원 마크 공간만이 시뮬레이션에서 사용되었다.



τ : 사고 간격 시간
t : 사고 발생 시간
m : 각 사고(사고 유형)와 연관된 마크

[그림 2] 마크 확률 점 과정

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

확률변수 $x(t_1)$, $x(t_2)$, ..., $x(t_k)$에 대해 결합 분포함수는 다음과 같다.

$P_{x(t1),\ x(t2),\ \ldots\ x(tk)}(X_1, X_2, .., X_k) =$

$Pr(x(t_1) \le X_1,\ x(t_2) \le X_2,\ ...,\ x(t_k) \le X_k)$ … (식1)

사고간격(τ)의 확률밀도함수 f(t)는 다음과 같다.

$f(t) = Pr\{t \le \tau \le t+dt\}$ … (식2)

이 과정이 포아송(Poisson) 분포일 때, 밀도함수 f(t)는

$$f(t) = a * e^{-at} \quad \cdots \text{(식3)}$$

로 주어지고, 여기서 a는 사고발생률이며, 확률분포함수 F(t)는 다음과 같다.

$$F(t) = 1 - e^{-at} \quad \cdots \text{(식4)}$$

2.3 시스템 상태 모델

하나의 공격/사고가 발생한 후 시스템은 새로운 상태로 변환되며, 이 변환은 사고유형과 구성에 대한 함수 또는 조건부 확률 p(r,s)=p(r,s|m,d,b)가 된다. 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. 변환행렬 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 변환하는 확률이다.

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

상태 변환확률 p(1,s)를 생성하는 식을 다음과 같이 제안하였다.

$p(1,s) = p(s,m,cost(b);\ \pi_0, \mu_0, \pi_1, \pi_2, \mu_1, \mu_2)$ …(식5)

여기서 s=1과 s > 1인 2 가지 경우로 나누었다. s = 1 일 때

$$p(1,1) = \pi_2 * (1 - e^{-\pi_1(\cos(b) - \pi_0)}) \quad \cdots \text{(식6)}$$

이고, s > 1 일때

$$p(1,s) = \mu_2 * (1 - e^{-\mu_1(\cos(b) - \mu_0)}) \quad \cdots \text{(식7)}$$

이다.

이들 함수는 비용에 따라 감소하며, 0과 1 사이의 값을 가지며, π_1 과 μ_1 은 방어장치 비용인 cost(b)에 따른 변환확률을 결정하는 계수이다. 이는 또한 생존성이 비용에 따라 어떻게 변화하는지를 결정한다.

$\pi_2 = \pi_3 * j$ 이며, 선형 함수이고,

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

상수뿐만 아니라 계수 π_3 와 μ_3는 주어진 제한 조건에 따르는 변환확률의 적절한 값을 구하기 위한 것이며, 위치 계수 π_0 와 μ_0는 0이고, π_1, μ_1, π_3, μ_3 등은 시뮬레이션 동안 변화하는 값이다.

2.4 생존성 모델링

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. 개념적으로 생존성을 다음과 같이 정의한다.

$$SV = \frac{\text{새로운 상태에서의 성능 수준 } s}{\text{정상 성능 수준}} \quad \cdots \text{(식8)}$$

성능 수준은 공격 후 새로운 시스템 상태에서 각 서비스가 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 형태로 정의할 수 있다.

$$SV(s) = \sum_u \omega(u) * \varphi(s,u) \quad \cdots \text{(식9)}$$

여기서 시스템의 상태집합 {S}가 정의되고, 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 중요시하는 특별한 서비스가 있다면 이의 가중치는 매우 높을 것이며, 이 서비스에 대한 생존성은 가벼운 손상을 입을 지라도 낮게 될 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 완전 고장, 1은 완전한 정상을 의미한다.

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 손상 기대치 E[y(u,m)]를 계산할 수 있다.

여기서 $0 \le y \le 1$로 가정할 때,

$$E[y(u,m)] = \int_0^1 y * p_{um}(y)\,dy \quad \cdots \text{(식10)}$$

이고, 생존성을 다음과 같이 계산할 수 있다.

$$SV \mid m = \sum_u \omega(u) * (1 - E[y(u,m)]) \quad \cdots \text{(식11)}$$

ω(u)는 기능이나 서비스의 중요도와 이용도를 반영한다. 또한 기능이나 서비스가 얼마만큼 이용되는지에 관계없이 "필수적인" 것을 구분할 필요가 있다. 따라서, 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 서비스의 집합을 나타낸다. 그러면 생존성은 다음과 같이 계산된다.

$$SV(s) = [\prod_u \varphi(s,u')^{\omega(u')}] * [\sum_u \omega(u) * \varphi(s,u)] \quad \cdots \text{(식11)}$$

또는

$$SV(s) = \frac{1}{2} * \{ [\prod_u \varphi(s,u')^{\omega(u')}] * [1 + \sum_u \omega(u) * \varphi(s,u)] \} \quad \cdots \text{(식12)}$$

여기서 u는 {U_0, U_1, U_2}에 u'는 {U_3}의 값이다. 곱하기 형식은 필수적인 기능이나 서비스가 고장나면, 즉 모든 k'에 대해 φ(s,u')=0이면 생존성이 0이 되도록 한다. SV(s)에 대한 식(11)은 집합 {U_3}에 있는 모든 기능이나 서비스가 완전히 고장났을 경우에 집합 {U_0}, {U_1}, {U_2}에 있는 모든 기능이나 서비스가 약간 생존할 때 생존성이 항상 0으로 되지 않도록 한다.

3. 시뮬레이션 및 결과 분석

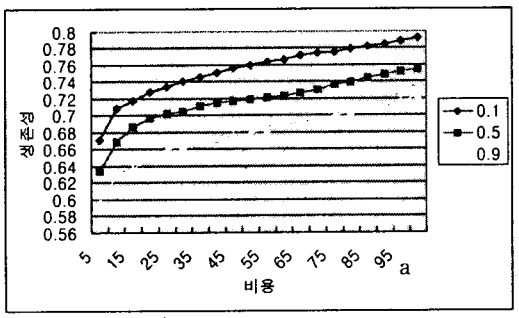
제안된 시뮬레이션 모델은 사고 발생에서 시작하여 피해 시스템이나 사이트의 반응을 통해 주어진 방어

장치에 따른 평균 생존성까지의 과정을 시뮬레이션 한다. 이를 통해 비용/효과 분석을 할 수 있다.

시뮬레이션은 공격 유형의 확률과 방어장치의 비용 변화, 그리고 시스템이 다양한 상태로 변환할 수 있는 확률 사이의 관계에 대해 수행되었다.

[그림 3]은 심각하거나 가벼운 사고의 상대적 확률이 변화할 때 생존성에 미치는 영향을 조사한 그래프이다.

변환확률과 비용에 대한 관계로부터 추정되듯이 생존성은 방어장치 비용에 따라 증가하며, 심각한 사고 발생 확률이 증가함에 따라 감소한다. 다른 p(r,s)의 집합을 가지고 계산하면, p(m)들에 대해 생존성의 민감도가 증가하는 것을 알 수 있다.

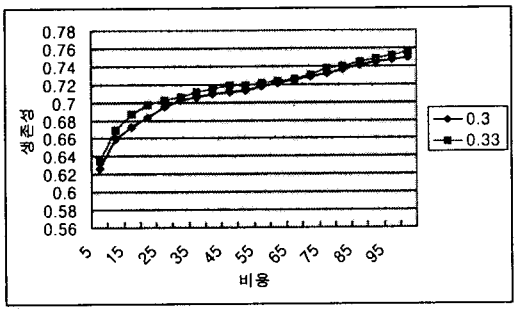


a=1.5, π_1=0.15, μ_1=0.08, π_3=0.15, μ_3=0.08
[그림 3] 예상 생존성과 P(m)

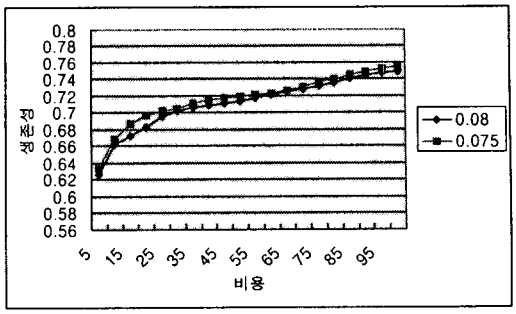
[그림 4]와 [그림 5]는 π_3와 μ_3를 각각 변화시킬 때의 영향을 나타낸 그래프이다.

π_3는 비용이 변할 때 변환 확률 p(1,1)의 수준을 결정한다. 그래서 π_3의 값이 높을수록 시스템이 정상 상태에 있을 확률이 높아지고, 그래서 생존성이 더 높아진다.

μ_3의 값은 커지면 낮은 생존성 값으로 된다. μ_3의 변화가 매우 작고 방어비용에 대해 영향이 일정하다.

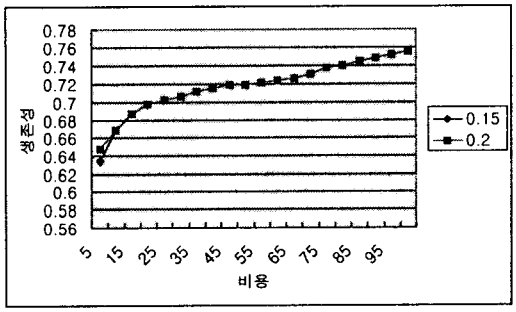


p(1)=0.5, a=1.5, π_1=0.15, μ_1=0.08, μ_3=0.75
[그림 4] 예상 생존성과 π_3



p(1)=0.5, a=1.5, π_1=0.15, μ_1=0.08, π_3=0.33
[그림 5] 예상 생존성과 μ_3

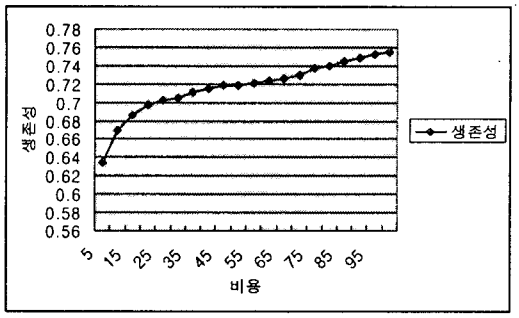
단위시간당 평균 피해는 총 피해량을 시뮬레이션동안 경과된 총시간으로 나누어 계산되며, 사고 발생률에 따른 평균피해는 사고발생률에 비례하고, [그림 6]과 같이 생존성에는 큰 차이가 없다.



p(1)=0.5, a=1.5, π_1=1.5, μ_1=0.008, π_3=0.33, μ_3=0.75
[그림 6] 평균 피해와 도착률 a

[그림 7]은 P(1)=0.5일 때 비용에 따른 예상 생존성을 보여준다. 비용이 증가함에 따라 처음에는 생존성이 급속히 증가하다가 점점 조금씩 증가한다. 이 그래프는 시스템 관리자들에게 자신의 회사에 가장 적합한 방어 수준을 결정할 수 있는 기준을 제공한다.

생존성이 중요하지 않을 때, 그 회사는 균형곡선에서 낮은 점을 선택할 수 있다. 그러나 생존성이 중요할 때에는 높은 점을 선택하는 것이 유리할 것이다. 이 곡선이 차이가 없는 곡선으로 평가될 경우에도 이 곡선에서 최적 또는 최선의 지점을 실제적으로 선택할 수 있다. 그러나 최적의 결과를 목표로 하지 않을지라도 이 곡선을 사용하여 비용과 생존성 사이의 가장 적합한 균형점을 찾을 수 있다.



[그림 7] 비용에 대한 예상 생존성

5. 결론

본 논문에서는 네트워크 정보시스템에 대한 전체적인 공격과 시스템의 반응을 통하여 정보시스템의 생존성을 관리하는 모델을 제안하였다. 네트워크 시스템의 생존성에 대해 공격과 관련된 다양한 상황을 분석하는데 사용될 수 있는 틀을 제안하였으며, 공격 유형, 사고 발생률과 사고 유형 사이의 상호관계 등과 같은 공격 사고에 관하여 방어비용에 따른 시스템의 예상 생존성을 시뮬레이션 하였다.

본 모델은 시스템 관리자들이 시스템 안전을 관리하는데 유용하게 비용/효과 분석을 할 때 사용될 수 있으며, 적은 비용으로 생존성을 효과적으로 향상시킬 수 있도록 지원한다.

향후 연구과제는 다음과 같다. 생존성 관리에서 중요한 것은 관리자들이 생존성과 보안성에 대해 더 잘 평가하고, 비용/효과 측면에서 효과적인 방어 전략을 결정할 수 있도록 많은 실제 데이터를 수집하는 것이다. 특히, 구성에 대한 함수로서 다른 시스템에 대한 반응 확률에 관한 데이터가 필요하며, 변환 시간뿐만 아니라 시스템이 공격당했을 때 시스템이 거치는 중간 상태에 대한 데이터가 필요하다.

사고 과정, 반응 행렬, 그리고 생존성 척도를 포함하는 전반적인 모델에서 생존성과 많은 매개 변수와의 관계를 연구하기 위해 더 많은 시뮬레이션을 하여야 한다.

[참고문헌]

[Basawa 80] Basawa, I.V. & Prakasa, B.L.S, "Statistical Inference for Stochastic Processes". New York, NY: Academic Press, 1980.

[Cohen 99] Cohen, F. "Simulating Cyber Attacks, Defenses, and Consequences", Fred Cohen & Associates 1999.

[CSI 98] Computer Security Institute. "Computer Security Issues and Trends". 4, 1(Winter 1988.)

[Daley 88] Daley, D.J. & Vere-Jones, D. "An Introduction to the Theory of Point Processes". New York, NY: Springer-Verlag, 1988.

[Ellison 97] 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.

[Fisher 99] 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. New York: IEEE Computer Society Press,1999.

[Howard 95] Howard, J. "An Analysis of Security Incidents on the Internet(1989-1995)". Ph.D. Dissertation, Carnegie-Mellon University, Pittsburgh, PA, 1995.

[Howard 98] Howard, J. & Longstaff, T. "A Common Language for Computer Security Incidents.(SAND98-8667)". Livermore, CA: Sandia National Laboratories, 1998.

[Law 82] Law, A.M. & Kelton, W.D. "Simulation Modeling and Analysis". New York, NY: McGraw-Hill, 1982.

[Lilen 92] Lilen, G.L.:Kotler, P.; & Moorthy, K.S. "Marketing Models". Englewood Cliffs, NJ: Prentice Hall, 1992.

[Linger 98] 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.

[Moitra 97] 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.

[Snyder 91] Snyder, D.S. & Miller, M.I. "Random Point Processes in time and Space". New York, NY: Springer-Verlag, 1991