자가치유 메커니즘을 활용한 침입감내시스템의 취약성 분석

(A Vulnerability Analysis of Intrusion Tolerance System using Self-healing Mechanism)

박 범 주 † 박 기 진 †† 김 성 수 †††
(Bumjoo Park) (Kiejin Park) (Sungsoo Kim)

요 약 네트워크 기반 컴퓨터 시스템이 외부 침입이나 혹은 내부 침입에 의해 부분적으로 손상(Partially Compromised)이 되더라도 최소한의 필수 서비스를 지속적으로 제공할 수 있게 해주는 침입감내시스템(Intrusion Tolerance System) 설계에 요구되는 중요한 요소 기술 중의 하나는 컴퓨터 시스템의 정량적 신인도(Dependability) 분석이라 할 수 있다. 본 논문에서는 침입감내시스템의 방어능력을 확보하기 위해 자율컴퓨팅(Autonomic Computing)의 핵심 기술인 자가 치유(Self-healing) 메커니즘을 적용하였다. 주 서버와 보조서버로 구성된 침입감내시스템의 상태천이(State Transition)를 자가치유 메커니즘의 두 가지 요소(결함모델 및 시스템반응)를 활용하여 분석하였으며, 시뮬레이션 실험을 통해 침입감내시스템의 가용도(Availability)를 계산한 후, 두 가지 경우의 취약성(Vulnerability) 공격에 대한 사례 연구를 진행하였다.

키워드 : 침입감내시스템, 자가치유, 취약성, 가용도

Abstract One of the most important core technologies required for the design of the ITS(Intrusion Tolerance System) that performs continuously minimal essential services even when the network-based computer system is partially compromised because of the external or internal intrusions is the quantitative dependability analysis of the ITS. In this paper, we applied self-healing mechanism, the core technology of autonomic computing to secure the protection power of the ITS. We analyzed a state transition diagram of the ITS composed of a primary server and a backup server utilizing two factors of self-healing mechanism (fault model and system response) and calculated the availability of ITS through simulation experiments and also performed studies on two cases of vulnerability attack.

Key words : Intrusion Tolerance System, Self-healing, Vulnerability, Availability

1. 서 론

네트워크 침입 사례 증가에 따른 침해사고의 예방 및 대응에 관련된 컴퓨터 보안 기술들이 활발히 연구되고 있으나, 방화벽, 백신, 침입탐지(Intrusion Detection) 등의 다양한 보안 기술들은 이미 알려진 공격에 대해서는 탐지, 예방 및 치료가 가능하지만, 의도적이든 의도적이지 않던 아직까지 알려지지 않은 공격이나 결함에 대해서는 취약(Vulnerability)하다는 단점을 지니고 있다. 또한, 최근에 발견되는 공격 도구의 특징을 종합해 보면 은닉화(Stealth), 분산화(Distributed), 에이전트(Agent)화 그리고 자동화(Automation)의 특징을 가지고 있어, 그 문제는 더욱 심각해지고 있다. 이를 해결하기 위한 방법으로써, 예방 기술과 탐지 기술로 미처 발견하지 못한 네트워크 기반 컴퓨터 시스템 대상의 각종 공격이나 침입이 발생하는 경우에도 서비스의 정상적인 제공이 가능한 정보보호기술인 침입감내(Intrusion Tolerance) 기법이 활발히 연구되고 있다.

침입감내는 기존의 결함허용(Fault-tolerant) 기술과 최근의 컴퓨터 보안기술(침입차단, 침입탐지 등)이 결합된 형태로 해당 시스템이 서비스 거부(DoS: Denial of Service) 공격과 같은 외부 침입이나 혹은 내부 침입에

· 이 논문은 2004년도 1학기 정착연구비 지원에 의하여 연구되었음
† 정 회 원 : 삼성전자 첨단기술연수소
bumjoo@samsung.com
†† 종신회원 : 아주대학교 산업정보시스템공학부 교수
kiejin@ajou.ac.kr
††† 종신회원 : 아주대학교 정보통신전문대학원 교수
sskim@ajou.ac.kr
논문접수 : 2004년 10월 6일
심사완료 : 2005년 4월 29일

의해 부분적으로 손상(Partially Compromised)이 되더라도 최소한의 필수 서비스를 지속적으로 수행하는 개념이다[1]. 즉, 모든 악의적 공격을 반드시 실패하도록 보증하기보다는, 침입에 성공한 악의적인 몇몇 공격이 시스템 일부에 일정 부분의 손상을 가하더라도 신인도(Dependability: Reliability, Availability, Safety, Maintainability 등)를 갖는 침입 감내구조에 의해 서비스를 지속적으로 제공한다[2]. 이러한 침입 감내구조의 신인도를 향상시키키 위해서는 시스템이 제공하는 서비스의 품질 요구사항을 만족시키거나 서비스의 품질저하를 방지하면서 빠른 시간 안에 정상적인 서비스를 제공해야 하는데 이를 위해서는 예방(Prevention), 탐지(Detection)기술이 선행되고 최후에 감내(Tolerance)기술이 적용되어야 한다. 그림 1은 침입감내를 위한 단계별 구조를 나타내고 있으며, 감내단계에서는 중복 시스템(Redundant System), 결함복구(Fault Recovery) 및 재활(Rejuvenation)과 같은 요소기술들이 사용된다.

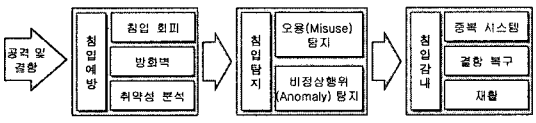


그림 1 침입감내를 위한 단계별 구조

한편, 신인도를 갖는 침입감내시스템의 구현을 위해 자율컴퓨팅의 4가지 핵심 기술 중의 하나인 자가치유(Self-healing) 메커니즘을 활용하는 접근 방법이 제시되고 있다[3]. 자가치유 기술은 결함허용 기법처럼 시스템의 신인도와 관련된 다양한 요소를 내포하고 있으나, 자가치유는 자가최적화(Self-optimization), 자가구성(Self-configure), 및 자가보호(Self-protect) 등과 함께 시스템 내외부의 예상하지 못한 다양한 공격에 대해 적절히 대응할 수 있는 기술을 제공한다는 측면에서 기존의 결함허용 기법보다는 폭넓은 방식이라 할 수 있다[4].

본 논문에서는 주서버와 보조서버로 구성된 침입감내 시스템의 상태 천이를 자가치유 메커니즘의 두 가지 요소(결함모델 및 시스템반응)를 활용하여 분석하였으며, 제안된 상태 천이도 모델의 검증을 위하여 시뮬레이션 실험을 통해 가용도(Availability)를 계산한 후 이를 향상하기 위한 방안을 강구하였으며, 두 가지 경우의 취약성 공격에 대한 사례 연구를 진행하였다. 서론에서는 문제를 정의하였으며, 2장에서는 관련 연구 결과를 분석하였고, 3장에서는 자가치유 메커니즘을 활용한 침입감내 시스템의 상태천이도 모델을 통해 가용도 모델을 정의하였다. 4장에서는 제안된 모델의 시뮬레이션 실험 및 사례연구를 수행하였고, 결론에서는 제안된 방법의 활용방안 및 향후 연구에 대해 논하였다.

2. 관련 연구

유럽에서는 침입감내시스템 개발을 위해 IST(Information Society Technologies)의 MAFTIA(Malicious- and Accidental-Fault Tolerance for Internet Applications) 프로젝트를 진행해 왔으며[5], 악성 프로그램과 결함에 의한 결함허용 및 정보보증을 주요 목적으로 하고 있다. 미국에서도 DARPA(Defense Advanced Research Projects Agency)의 OASIS(Organically Assured and Survivable Information System) 프로그램을 통해 다수의 침입감내시스템 관련 프로젝트들이 수행되고 있다. 이중에서 HAQUIT(Hierarchical Adaptive Control of Quality of Service for Intrusion Tolerance) 프로젝트의 경우 사용자 성능이 25% 이상 저하되는 것을 방지하면서 네시간 동안의 침입감내를 제공하는 것을 목표로 하고 있고, SITAR(Scalable Intrusion Tolerant Architecture)는 분산 서비스, 특히 COTS(Commercial Off-the-Shelf) 서버를 위한 침입감내구조를 제시하고 있다[6-8]. 이밖에, ITUA(Intrusion Tolerance by Unpredictable Adaptation)와 AITDB (Adaptive Intrusion Tolerant Database System) 프로젝트를 통해 중복성 관리(Redundancy Management)기술 및 침입감내를 위한 데이타베이스 설계기술 개발이 진행되고 있으며[9,10], Willow 프로젝트를 통해 대규모 분산시스템의 생존성(Survivability)을 지원하는 시스템을 개발한 사례가 있다[11].

HAQUIT[6]에서는 오류 검출과 시스템 실패(Failure)를 방지하기 위해 중복성과 다양성을 복합적으로 이용하며, 구조가 매우 간단하기 때문에 일반 COTS 서버들로 비교적 쉽게 구현이 가능하다는 장점이 있는데 반해, 침입을 탐지하는 기능이 미약하고 확장하는데 한계가 있으며, 또한 사용자 요청이 응용 서버에 바로 전달되지 않기 때문에 시간적 추가 비용이 존재하는 문제점이 있다. 한편, 침입감내시스템의 결함허용 기능 강화를 위해 디자인 다양성(Design Diversity)을 채택하여, 주 서버와 보조서버가 각기 다른 운영체제와 웹 서버 응용을 갖도록 구성하였으나, 두 서버가 Hot-standby 방식으로 연동되었기 때문에 외부 공격으로 인해 서버 모두 동시 손상될 수 있는 문제를 내포하고 있다.

[12]에서는 침입 감내시스템이 외부공격 상황에서 갖추어야 할 동적인 이상거동을 상태천이도(State Transition Diagram)로 나타내고, 시스템이 가지는 취약성 및 위협 요소를 어떻게 모델링 할 수 있는가에 대한 침입감내 프레임워크에 관한 연구를 진행하였고, [13]에서는 [7]의 SITAR 시스템에 대해 다양한 상태천이도를 바탕으로 서비스 거부 공격 등 몇 가지 침입 유형별 정

량적 성능 분석을 시도하였다. 그러나, SITAR 시스템의 경우 기존 COTS 서버의 변경없이 적용 가능하고 사용자에게도 투명하다는 장점이 있으나, 대량의 COTS 서버 공격에 대응 보장 한계와 COTS 서버 이외의 구성 요소들은 공격의 취약성을 갖고 있지 않아야 하는 조건이 있다. 또한, 침입 대응 과정을 담당하는 기능이 분산되어 있어서 과도한 지연 가능성 및 복잡한 구조로 인해 구현 비용 증가가 예상된다.

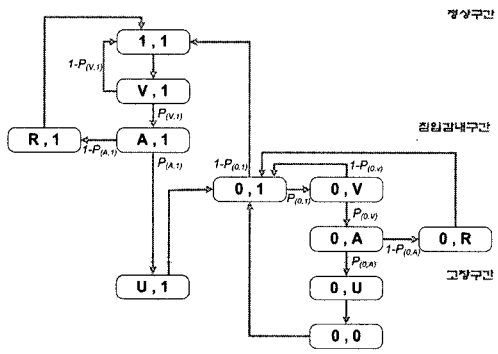
침입감내시스템 프레임워크는 크게 계층기반과 복제기반으로 나눌 수 있는데, 계층기반 구조는 단일 호스트에 적용되며 데이타 무결성이 강조되고, 복제기반 구조는 분산 컴퓨팅 환경의 가용성 확대가 목적이나 복제 증가로 인해 기밀성에 대한 위협이 증가된다[14]. 또한, [15]와 [16]에서는 각각 분산 임베디드 시스템의 신인도 향상 및 시스템에 대한 비정상행위 탐지 문제를 해결하기 위해 자가치유 기술을 적용한 예를 보여주고 있다.

신인도를 갖는 침입감내시스템 구성을 위한 기존의 연구들은 결함허용 기법에 기반한 연구가 주를 이루고 있다. 본 논문에서는 자가치유 기법의 요소를 활용한 침입감내구조를 제안함으로써 시스템 내/외부의 보다 다양한 공격에 대해 적절히 대응할수 있는 방안을 모색하였다. 이를 통해 침입감내시스템의 동적인 이상거동의 변화를 정량적으로 분석할 수 있고, 다양한 취약성 공격에 대한 상태천이 모델링을 통해, 보안 손상상태에서 정상상태로 전환되는 과정을 파악할 수 있다.

3. 자가치유 메커니즘을 활용한 침입감내시스템

자가치유는 외부침입이나 시스템 내부문제에 의해 발생된 결함이나 오류를 자동적으로 감지(Detect), 진단(Diagnosis) 및 치유(Repair) 함으로써 시스템의 오동작을 최소화하여 궁극적으로 시스템의 신인도를 향상시키는 자율컴퓨팅의 핵심기술이다[17]. 이러한 자가치유 기술이 시스템으로 완전하게 구현되기 위해서는 4가지 요소-결함 모델(Fault Model), 시스템 반응(System Response), 시스템 완전성(System Completeness) 및 디자인 문맥(Design Context)-에 대한 정의가 필요하다[10].

결함모델은 시스템이 감내해야 하는 결함의 특성을 정의하는 것이며, 시스템 반응은 외부침입 등에 의한 결함의 감지, 결함에 대한 대응방법 및 복구전략에 대한 세부적인 정의에 해당한다. 예를 들면, SYN Flood 및 Smurfing과 같은 서비스 거부공격의 경우, DNS (Domain Name Server)같은 특정 서버에 악의적인 HTTP(Hypertext Transfer Protocol) 요청을 대량으로 발생시켜 시스템 리소스의 성능 저하를 야기하지만, 이러한 상황에서도 시스템의 필수 서비스 기능을 보장해 주는 점진적 기능 퇴화(Gracefully Degradation) 개념이 시스템 반응의 요소에 포함될 필요가 있다. 한편, 시스템 완전성은 현실세계에서 시스템을 구현하는데 있어서 구조적인 불완전성을 극복하기 위해 갖추어야 할 요소에 대한 것이고, 디자인 문맥은 구현하고자 하는 시스템의 동질성(Homogeneity) 및 선형성(Linearity)을 확보하기 위한 자가치유 요소에 관한 것이다. 침입감내시스템이 자가치유적 기능을 갖게 하기 위해 위에서 기술한 4 가지 자가치유 구성요소 중에 결함 모델 및 시스템 반응에 관련된 세부 항목을 시스템의 상태천이도로 나타내었다.



상태 (주서버, 보조서버), V : 취약상태, A : 공격상태, R : 재활상태

그림 2 침입감내시스템의 상태천이도

그림 2는 자가치유 구성 요소가 반영된 Cold-standby 침입감내시스템의 상태천이를 나타내고 있으며, 서비스 거부 공격에 대응하는 결함 모델의 세부 요소와, 그에 상응하는 시스템 반응(결함감지(Fault Detection), 기능퇴화(Degradation), 결함반응(Fault Response) 및 결함복구(Fault Recovery)) 등의 세부 요소를 표현하였다. 침입감내시스템 모델링을 위해 적용한 가정은 아래와 같다.

- 주-보조서버 사이의 작업전이(Switchover) 메커니즘은 Cold-standby방식을 따른다.
- 침입감내시스템의 각 상태에 머무를 시간은 일반 분포를 따른다.
- 시스템은 초기상태(1,1)에 정상 가동되며, 초기상태에 있을때만 침입이 가능하다.
- 주-보조서버 사이의 작업전이 이후 보조서버가 정상상태(0,1)에서만 주서버로 작업전이 된다.

주서버와 보조서버가 모두 정상적으로 동작하는 상태(1,1)에서 취약성이 노출되면, 침입 감내시스템은 (V,1) 상태, 즉 주서버는 취약상태, 보조서버 정상상태로 천이된다. 침입감지 모듈이 네트워크 트래픽 및 IP 주소 분석 등을 통해 모든 취약성 공격(Attacks)을 방어하면

일정시간 이후 초기상태(1,1)로 복원되지만, 그렇지 못할 경우 $P_{(V,1)}$의 확률로 주 서버가 공격 당하는 (A,1) 상태, 즉 주서버 공격상태, 보조서버 정상상태로 바뀐다. 주서버 공격 상태가 일정시간 지속되면 시스템 손상이 누적되며, 이때 침입 진단(Diagnosis) 모듈이 시스템의 CPU 부하 및 메모리 상태를 분석하여, 유의할 수준의 성능저하가 1- $P_{(A,1)}$의 확률로 감지될 경우 주서버를 재활상태 (R,1), 즉 주서버 재활상태, 보조서버 정상상태로 전이시키지만, 성능저하를 감지하지 못할 경우 감지불능(Undetected) 상태인 (U,1)로 전이되어 최종적으로 보조서버가 주서버 기능을 대신하도록 (0,1) 상태, 즉 주서버 고장상태, 보조서버 정상상태로 작업전이 된다. 외부 공격에 의해 주-보조서버가 동시에 다운되는 상태를 방지하기 위해 Cold-standby 구성을 채택하였으며, 이 경우 작업전이에 필요한 시간이 길어지게 된다. 보조서버가 주서버 역할을 대신하는 (0,1) 상태에서 보조서버가 다운되는 (0,0) 상태, 다시말하면, 주서버와 보조서버 모두 고장 상태로 전이하는 과정은 초기상태(1,1)에서 주 서버가 보조서버로 작업전이 되는 과정과 동일하다.

전체적으로 그림 2에서 정상구간((1,1), (V,1))은 시스템의 기능 저하가 전혀 일어나지 않은 구간이고, 침입감내구간((A,1), (R,1), (0,1), (0,V), (0,A), (0,R))은 일정한 손상이 존재하지만 시스템이 제공해야 하는 서비스는 지속적으로 수행되고 있는 구간이며, 고장구간((U,1), (0,U), (0,0))은 침입감내시스템 작동에도 불구하고 서비스를 하지 못하는 상태로써 주서버가 회복되지 못한 상태에서 보조서버까지 서비스 불가한 상태이다.

제안된 침입감내시스템의 평형상태(Steady-State)의 가용도를 계산하기 위해 그림 2의 상태천이도상에서 11가지 이산상태(Discrete-state) X_S에 대한 확률과정(Stochastic Process) $X(t)$를 식 (1)과 같이 정의하였으며, 서비스 시간이 일반적인 분포인 M/G/1을 적용한 세미마르코프 프로세스(SMP: Semi-Markov Process) 분석을 통해 각 상태에 머무는 확률을 계산하였다.

$$X(t) : t > 0 \tag{1}$$

$$X_S = \{ (1,1), (V,1), (A,1), (R,1), (U,1), (0,1), (0,V), (0,A), (0,R), (0,U), (0,0) \}$$

그림 2에 표시된 모든 상태는 상호 도달 가능하므로 더 이상 줄일 수 없으며(Irreducible), 주기성을 갖지 않고 한정된 시간 내에 특정 상태로 회귀할 수 있으므로 Erogodicity(Aperiodic, Recurrent, Nonnull) 특성을 만족하게 된다. 따라서, 침입감내시스템 각 상태에 대한 SMP의 안정상태 확률이 존재하고 해당 SMP는 각 상태에서의 전이확률을 이용한 임베디드(Embedded) 이산 마르코프 체인(DTMC : Discrete-time Markov Chain)에 의해 유도할 수 있다[18].

SMP의 각 상태에서의 평균 잔류시간(Mean Sojourn Time)을 h_i 라 하고, DTMC 평형상태 확률을 d_i 라 할 때, SMP의 각 상태에 대한 평형상태 확률 π_i를 식 (2)와 같이 나타낼 수 있다[19].

$$\pi_i = \frac{d_i h_i}{\sum_j d_j h_j}, \qquad i, j \in X_S \tag{2}$$

이때, DTMC의 평형상태 확률 d_i들은 식 (3)과 식 (4)의 관계를 갖게 된다.

$$\vec{d} = \vec{d} \cdot P \tag{3}$$

$$\sum_i d_i = 1 \quad i \in X_S \tag{4}$$

여기서, $\vec{d} = [\, d_{(1,1)}\ d_{(V,1)}\ d_{(A,1)}\ d_{(R,1)}\ d_{(U,1)}\ d_{(0,1)}\ d_{(0,V)}\ d_{(0,A)}\ d_{(0,R)}\ d_{(0,U)}\ d_{(0,0)}\,]$이며, P는 그림 2의 X_S의 각 상태에서의 전이확률 $p_{(i,j)}$에 의해 표현되는 DTMC 전이확률 행렬(Transition Probability Matrix)이다. 이들로부터 DTMC의 평형상태 확률을 구하면 식 (5)와 같다.

$$d_{(1,1)} = \frac{1 - p_{(0,1)}}{2(1 + p_{(V,1)})(1 - p_{(0,1)}) + p_{(V,1)} p_{(A,1)} (1 + p_{(0,1)} + 2p_{(0,1)} p_{(0,V)} + p_{(0,1)} p_{(0,V)} p_{(0,A)})}$$

$$\begin{aligned}
d_{(V,1)} &= d_{(1,1)} \\
d_{(A,1)} &= d_{(V,1)} p_{(V,1)} \\
d_{(R,1)} &= d_{(A,1)} (1 - p_{(A,1)}) \\
d_{(U,1)} &= d_{(A,1)} p_{(A,1)} \\
d_{(0,1)} &= d_{(U,1)} + d_{(0,V)} (1 - p_{(0,V)}) + d_{(0,R)} + d_{(0,0)} \\
d_{(0,V)} &= d_{(0,1)} p_{(0,1)} \\
d_{(0,A)} &= d_{(0,V)} p_{(0,V)} \\
d_{(0,R)} &= d_{(0,A)} (1 - p_{(0,A)}) \\
d_{(0,U)} &= d_{(0,A)} p_{(0,A)} \\
d_{(0,0)} &= d_{(0,U)}
\end{aligned} \tag{5}$$

한편, 식 (5)에서 구한 DTMC 평형상태 확률을 식 (2)에 대입하면 궁극적으로 SMP의 각 상태에 대한 평형상태 확률 π_i 를 구할 수 있으며, 평형상태에서 시스템의 가용도는 상태천이도상의 X_S 각 상태에서 (U,1), (0,U) 및 (0,0) 상태에 있을 확률을 배제한 경우로 식 (6)과 같이 정의된다.

$$Availability = 1 - (\pi_{(U,1)} + \pi_{(0,U)} + \pi_{(0,0)}) \tag{6}$$

4. 성능 평가

4.1 기본 SMP 모델의 시뮬레이션 분석

침입감내시스템의 SMP모델을 분석하기 위해서는 전이확률과 각 상태에서의 평균 잔류시간에 대한 파라미

표 1 시뮬레이션 파라미터

입력변수	설정값
평균 잔류시간	$h_{(1,1)} = 0.5, h_{(V,1)} = 1/3, h_{(A,1)} = 0.25, h_{(U,1)} = 0.5, h_{(R,1)} = 0.2, h_{(0,1)} = 0.5$ $h_{(0,V)} = 1/3, h_{(0,A)} = 0.25, h_{(0,R)} = 0.2, h_{(0,U)} = 0.5, h_{(0,0)} = 0.5$
전이확률	5개 전이확률 $(p_{(V,1)}, p_{(A,1)}, p_{(0,1)}, p_{(0,V)}, p_{(0,A)})$ 중에서 3개는 고정하고 2개 값을 변화(0부터 1까지) (예 : $p_{(A,1)} = p_{(0,V)} = p_{(0,A)} = 0.5, \quad 0 < p_{(V,1)}, p_{(0,1)} < 1$)

터 설정이 이루어져야 한다. 본 논문에서는 표 1의 설정값을 기준으로 시뮬레이션을 수행하였다[20]. 각 상태에서의 평균 잔류시간이 일반분포를 따르므로 값은 상대적인 차이로서의 의미만 존재하며, 상태천이도에 나타난 5개 분기점에서의 전이확률 각각이 침입감내시스템의 가용도에 독립적으로 미치는 영향을 분석하기 위해 초기 전이확률의 설정값을 0.5로 균등하게 설정하였다.

그림 3은 외부의 악의적인 공격상황에서 침입감내시스템의 초기대응 능력이 가용도 변화에 미치는 영향을 파악하기 위해 주서버가 취약성을 감지 못하여 공격 당하는 확률($P_{(V,1)}$)과 보조서버가 취약성에 노출될 확률($P_{(0,1)}$)의 변화에 따른 시스템의 가용도 변동추이를 보여주고 있다.

그림 2를 통해 제안된 Cold-standby 침입감내시스템을 구성하면 주-보조서버가 각각 공격상황 및 취약한 상황에 노출되기 전의 초기상태에서 시스템의 이상거동을 감지할수록 가용도가 극대화된다는 것을 알 수 있다. $P_{(V,1)}$과 $P_{(0,1)}$의 값이 커지면서(즉, 초기상태 감지능력의 저하) 시스템의 가용도는 급속히 감소하게 되지만, $P_{(V,1)}$값이 0.5 보다 크며, 동시에 $P_{(0,1)}$의 값이 커질수록 가용도가 오히려 증가하는 현상을 보여주고 있다. 그 이유는 $P_{(V,1)}$의 값이 커질수록 주서버가 서비스 불능상태인 (U,1)에 놓일 확률이 상대적으로 증가하게 되므로, 보조서버로 작업전이 되더라도 주서버의 즉각적인 복구를 통한 서비스보다는 보조서버가 (0,V)와 (0,A) 상태에서의 침입감내를 통해 서비스를 지속하는 편이 시스템을 (U,1)에 놓이게 할 가능성을 줄여줄 수 있기 때문이라 판단된다.

그림 4는 공격에 노출된 상황에서 시스템의 대응 능력을 판단하기 위해, 주서버와 보조 서버에 대한 공격성공 확률 $P_{(A,1)}$과 $P_{(0,A)}$의 변화에 따른 가용도 변화 추이를 보여주고 있다. 그래프로부터 초기상태의 이상거동 감지능력에 관련된 전이확률$P_{(V,1)}$과 $P_{(0,1)}$의 크기에 무관하게 $P_{(A,1)}$이 0일 경우 가용도가 이상적인 값(1.0)을 가짐을 알 수 있다. 즉, 주-보조서버가 공격 상황에 노출된 상태인 (A,1)과 (0,A)에서 침입감내시스템의 진단기능을 통해 유의할 만한 성능저하를 즉각적으로 감지할 수 있다면 재활모드로의 전환을 통해 초기상태로 복귀시킴으로써 가용도를 보장할 수 있게 된다. 그러나, $P_{(A,1)}$과 $P_{(0,A)}$가 1에 근접하게 되면 시스템이 서비스 불능상태인 (U,1), (0,U) 및 (0,0)에 놓일 확률이 동시에 증가하면서 가용도가 감소하게 된다.

한편, 그림 3과 그림 4에서 $P_{(A,1)}$과 $P_{(0,A)}$가 1일 경우의 가용도가 $P_{(V,1)}$과 $P_{(0,1)}$이 시스템에 가장 불리한 값을 가진 경우의 가용도에 거의 근사한 결과를 보이고

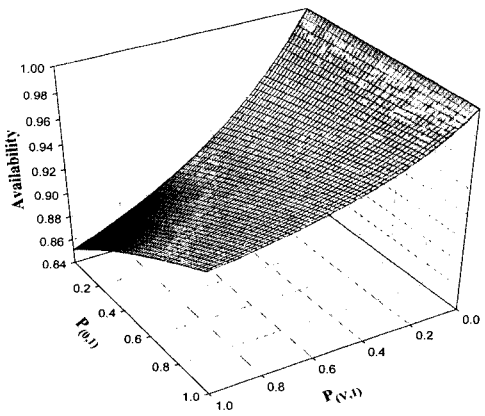


그림 3 $P_{(V,1)}$과 $P_{(0,1)}$의 변화에 따른 가용도 분석

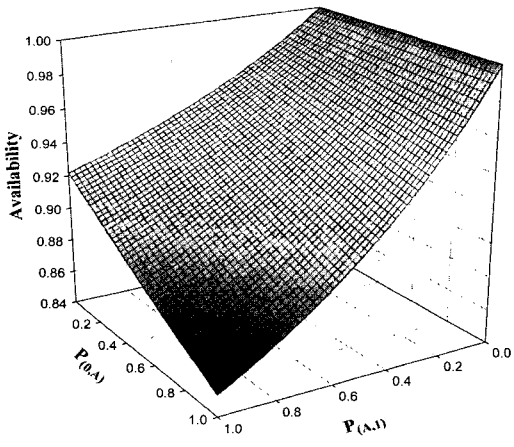


그림 4 $P_{(A,1)}$과 $P_{(0,A)}$의 변화에 따른 가용도 분석

있음을 알 수 있다. 이는 초기상태에서 이상거동을 감지하지 못하더라도 단일시스템에 비해 Cold-standby 침입감내시스템의 구조가 외부의 악의적 공격 상황에서도 작업전이, 복구, 재활 등의 다양한 감내 기능에 의해 시스템이 서비스 불가하거나 다운되는 상태에 놓일 확률을 최대한 줄여줌으로써 가용도 저하를 방지해 주기 때문이라 할 수 있다.

4.2 취약성 공격 사례별 분석

침입감내시스템의 기본 SMP모델을 실제 공격 사례에 적용하기 위해 [12]에서 제시한 두 가지 공격 유형인 Active Server Page(ASP) 취약성 및 Common Gateway Interface(CGI) 취약성을 채택하여 분석을 수행하였다.

첫번째 사례로써 ASP 취약성은 Internet Information Server(IIS) 서버의 파일 중에서 showcode.asp가 악의적인 공격자에게 노출되는 경우 발생되는 취약성 공격 유형이다. 즉, 공격자가 특정 URL (http://target/msadc/samples/SELECTOR/showcode.asp ? source=/path/file)을 활용하여 웹서버의 소스파일을 임의대로 볼 수 있게 됨으로써 기밀성(Confidentiality)에 심각한 손상을 야기시키게 된다. 이 경우 주-보조서버가 각각 공격상태에서 진단모듈에 의해 침입을 능동적으로 감지하기 어렵기 때문에 재활상태로 진입할 수 없게 되므로 $P_{(A,1)}$과 $P_{(0,A)}$가 1인 특수한 사례에 해당한다.

그림 5는 이러한 ASP 취약성 경우에 대해 SMP 모델 적용 결과를 분석하기 위해 $P_{(A,1)}$과 $P_{(0,A)}$를 1로 고정시킨 후 $P_{(V,1)}$과 $P_{(0,1)}$의 값을 변화시켜 가면서 시스템의 가용도 변화를 분석한 결과를 보여주고 있다. 이 경우 그림 3의 결과와 마찬가지로 주-보조서버가 각각 공격상황 및 취약한 상황에 노출되기 전의 초기상태에서 시스템의 이상거동을 감지할수록 가용도가 극대화된다는 것을 알 수 있다. 그러나, 그림 3과 비교해 볼 때 그림 5에서의 가용도 최소값은 $P_{(V,1)}$=1과 $P_{(0,1)}$=0일 때 약 10% 정도 더 작아지는 것을 알 수 있다. 즉, 주-보조서버가 각각 (R,1) 상태 및 (0,R) 상태를 통한 침입감내 기능을 활용하지 못한 것으로 인해 야기되는 가용도 손실치라 판단된다.

두번째 사례로써 CGI 취약성은 윈도우즈 NT 계열의 프락시 서버가 CGI 스크립트로 도스 방식의 파일을 사용함으로써 야기된 취약성이며, 네트워크상의 원격 공격자가 특정 URL을 이용하여 배치 파일을 도용함으로써 시스템 파일이나 사용자 계정등의 중요파일을 수정할 수 있게 되기때문에 기밀성 및 무결성(Integrity)에 심각한 문제를 야기시키게 된다. 그런데, 이 경우 시스템이 공격상태에 진입하기 전에 URL 필터링과 같은 취약성 감지 기능을 활용하기 어렵기 때문에 주-보조서버가 각각 (V,1) 및 (0,V) 상태에서 초기상태로 회복하지 못하고 바로 (A,1)과 (0,A)로 진행된다($P_{(V,1)}$=$P_{(0,V)}$=1).

그림 6은 CGI 취약성에 대한 가용도 분석 결과를 보여주고 있다. 여기서, $P_{(A,1)}$=0일 때는 $P_{(V,1)}$의 값에 무관하게 시스템이 고장구간에 놓일 확률이 0이므로 $P_{(A,1)}$과 $P_{(0,A)}$의 변화에 따른 가용도 변화 결과를 보여주는 그림 4와 동일한 결과를 보여주고 있으나, $P_{(A,1)}$과 $P_{(0,A)}$이 커지면서 가용도는 점진적으로 저하되게 되고, $P_{(A,1)}$=$P_{(0,A)}$=1일 경우 가용도가 가장 작은 값을 갖게 되는데 그림 4에 비해 약 12% 정도 줄어든 결과를 보여주고 있다. 이러한 현상은 주-보조서버가 각각 (V,1) 상태 및 (0,V) 상태에서의 침입감내 기능을 활용하지 못함으로 인해 야기된 가용도 저하가 극대화된 것이라 할 수 있으며, 두 가지 취약성 공격 사례적용 결과를 비교해 볼 때 초기상태의 침입감내 능력이 공격상태에서의 대응능력에 비해 가용도 측면에서 상대적으로 더 중

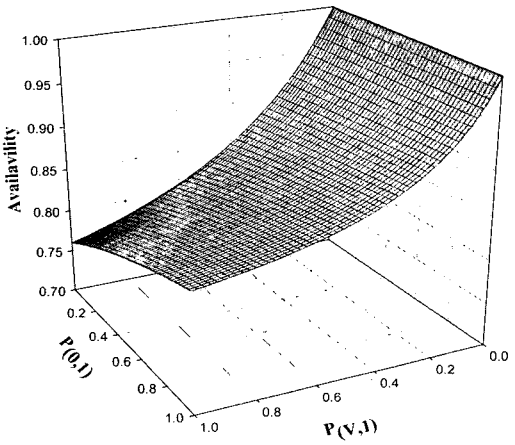


그림 5 ASP 취약성에 대한 가용도 분석

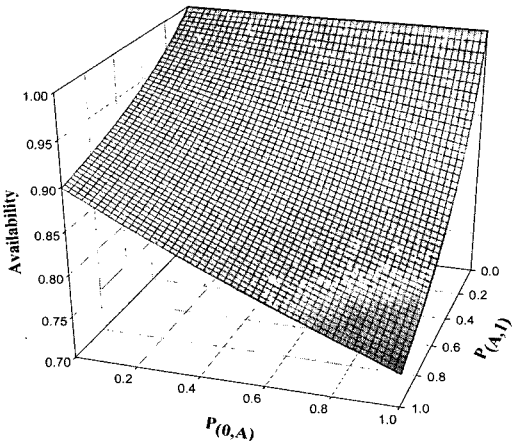


그림 6 CGI 취약성에 대한 가용도 분석

요함을 알 수 있다.

5. 결론 및 향후 연구방향

본 논문에서는 침입 감내시스템의 신인도를 분석하기 위해 자율컴퓨팅의 핵심 기술인 자가치유 메커니즘을 접목시키는 방안을 제시하였다. 주서버와 보조서버가 각 1대인 Cold-standby 방식의 침입감내시스템을 11가지 상태로 정의한 후 각 상태에서의 전이 확률 및 평균 잔류시간을 통해 DTMC 평형상태 확률 및 SMP 평형 상태 확률을 계산하여 시스템의 가용도를 계산하였고, 기본 SMP 모델에 대한 시뮬레이션 분석 및 두 가지 취약성 공격 사례(ASP Vulnerability, CGI Vulnerability) 분석을 통해 가용도 향상 방안을 기술하였다. 향후, 본 논문에서 고려한 자가치유 메커니즘의 두 가지 요소 이외에 시스템 완전성 및 디자인 문맥 등을 함께 고려한 모델링을 통해 침입감내시스템의 신인도를 향상시킬 수 있는 방안을 연구할 예정이다.

참 고 문 헌

[1] F. Wang, R. Uppalli, and C. Killian, "Analysis of Techniques for Building Intrusion Tolerant Server Systems," Proceedings of Military Communications Conference, pp. 729-734, Oct. 2003.

[2] A. Avizienis, J. Laprie, B. Randell, "Fundamental concepts of dependability," 3rd Information Survivability Workshop, pp. 7-12, Oct. 2000.

[3] P. Koopman, "Elements of the Self-Healing System Problem Space," Workshop on Architecting Dependable Systems, pp. 31-36, May 2003.

[4] D. Chess, C. Palmer, and S. White, "Security in an Autonomic Computing Environment," IBM Systems Journal, Vol. 42, No.1, pp. 107-118, 2003.

[5] http://www.laas.research.ec.org/maftia/

[6] J. Reynolds, et. al., "On-line Intrusion Detection Attack Prevention Using Diversity Generate-and-Test, and Generalization," Proceedings of the 36th Annual Hawaii International Conferences on System Sciences, pp. 335-342, Jan. 2003.

[7] F. Wang, et. al., "SITAR: A Scalable Intrusion-Tolerant Architecture for Distributed Services," Proceedings of the Foundations of Intrusion Tolerant Systems, pp. 359-367, 2003.

[8] F. Wang and C. Killian, "Design and Implementation of SITAR Architecture : A Status Report," Proceedings of Intrusion Tolerant System Workshop, C-3-1, Supplemental Volume on International Conference on Dependable System & Networks, June 2002.

[9] T. Courtney, et. al., "Providing Intrusion Tolerance with ITUA," Proceedings of the International Conference on Dependable Systems & Networks, pp. C-5-1 - C-5-3, June 2002.

[10] P. Luenam and P. Liu, "The Design of an Adaptive Intrusion Tolerant Database System," Proceedings of IEEE Workshop on Intrusion Tolerant Systems, pp. C-2-1 - C-2-8, June 2002.

[11] J. Knight, et. al., "The Willow Architecture: Comprehensive Survivability for Large-Scale Distributed Applications," Technical Report CU-CS-926-01, Department of Computer Science, University of Colorado, December, 2001.

[12] K. Goseva-Popstojanova, et. al., "Characterizing Intrusion Tolerant Systems using a State Transition Model," DARFA Information Survivability Conference and exhibition, Vol. 2, pp. 211-221, June 2001.

[13] D. Wang, B. Madan, and K. Trivedi, "Security Analysis of SITAR Intrusion Tolerance System," Proceedings of the ACM Workshop on Survivable and Self-Regenerative Systems, pp. 23-32, Oct. 2003.

[14] G. Kim, M. Choi, and K. Lee, "Classification of the Intrusion Tolerant Systems and Integrated Framework for Survivability Enhancement," The Korea Information Processing Society Transactions, Vol. 10C, No. 3, pp.295-304, 2003.

[15] C. Shelton, P. Koopman, and W. Nace, "A Framework for Scalable Analysis and Design of System-Wide Graceful degradation in distributed Embedded Systems," Eighth IEEE International Workshop on Object-oriented Real-time Dependable Systems, pp.156-163, Jan. 2003.

[16] O. Raz, P. Koopman, and M. Shaw, "Enabling Automatic Adaptation in Systems with Under-Specified Elements," 1st Workshop on Self-Healing Systems, pp. 55-60, Nov. 2002.

[17] J. Kephart, and D. Chess, "The Vision of Autonomic Computing," IEEE Computer, Vol. 36, No. 2, pp. 41-50, 2003.

[18] L. Kleinrock, Queueing Systems: Volume 1 Theory, John Wiley & Sons, pp. 417, 1975.

[19] K. Trivedi, Probability and Statistics with Reliability Queueing and Computer Science Applications, John Wiley & Sons, Inc., pp. 472, 2002.

[20] B. Madan, et. al., "Modeling and Quantification of Security Attributes of Software Systems," International Conference on Dependable Systems and Networks, pp. 505-514, June 2002.

박 범 주

1989년 서울대학교 조선공학과(공학사) 1992년 포항공과대학교 산업공학과(공학석사). 1992년~1995년 삼성종합기술원 그룹CAE센타 주임연구원. 1995년~1998년 삼성전자 소그룹 전략기획총괄 첨단기술센타 과장. 1998년~현재 삼성전자(주) 첨단기술연수소 차장. 2002년~현재 아주대학교 공과대학 정보통신전문대학원 박사과정. 관심분야는 결함허용, 성능분석, 클러스터컴퓨팅, 소프트웨어재활, 침입감내시스템

박 기 진

1989년 한양대학교 산업공학과(공학사) 1991년 포항공과대학교 산업공학과(공학석사). 1991년~1996년 삼성종합기술원 기반기술연구소 전임연구원. 1996년~1997년 삼성전자(주) 소프트웨어센터 선임연구원. 1997년~2001년 아주대학교 컴퓨터공학과(공학박사). 2001년~2002년 한국전자통신연구원 네트워크장비시험센터 선임연구원. 2002년~2004년. 안양대학교 컴퓨터학과 전임강사. 2004년~현재 아주대학교 공과대학 산업정보시스템공학부 조교수. 관심분야는 Dependable Embedded Computing, Intrusion Tolerance Systems, Cluster Computing

김 성 수

1982년 서강대학교 전자공학과(공학사) 1984년 서강대학교 전자공학과(공학석사). 1995년 Texas A&M University 전산학과(공학박사). 1983년~1996년 삼성전자(주) 삼성종합기술원 수석연구원. 2002년~2003년 Texas A&M University 교환교수. 1996년~현재 아주대학교 정보통신대학 조교수/부교수/정교수. 관심분야는 Autonomic Computing, Ubiquitous Computing, Performance Evaluation, RFID/USN