침입 감내시스템의 고가용성 자가치유 메커니즘

박범주[0]* 박기진** 김성수*
아주대학교 정보통신전문대학원* 아주대학교 공과대학 산업정보시스템공학부**
{bjpark, sskim}@ajou.ac.kr* kiejin@ajou.ac.kr**

Highly Available Self-healing Mechanism for Intrusion Tolerant System

Bumjoo Park* Kiejin Park** Sungsoo Kim*
Graduate School of Information And Communication, Ajou University*
Division of Industrial & Information Systems Engineering, Ajou University**

요 약

네트워크 기반 컴퓨터 시스템이 각종 악의적 공격에 의해 손상되더라도, 지속적인 서비스를 제공할 수 있게 해주는 침입 감내시스템(Intrusion Tolerance Systems) 설계기법의 중요한 요소 기술 중의 하나는 컴퓨터 시스템의 정량적 신인도(Dependability) 분석이라 할 수 있다. 본 논문에서는 침입 감내시스템의 신인도를 분석하기 위해 자율컴퓨팅(Autonomous Computing)의 핵심 기술인 자가 치유(Self-healing) 메커니즘을 적용하였다. 즉, 주서버와 보조서버로 구성된 이중계 침입 감내시스템의 상태천이(State Transition)를 자가치유 메커니즘의 두 가지 요소(결함모델 및 시스템반응)를 활용하여 분석하였으며, 시뮬레이션 실험을 통해 침입 감내시스템의 가용도(Availability)를 정량적으로 정의하였다.

1. 서 론

침입감내(Intrusion Tolerance)는 침입감지(Intrusion Detection)와는 달리 해당시스템이 서비스 거부(DoS:Denial of Service) 공격과 같은 외부 침입이나 혹은 내부 침입에 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 부분에 손상을 가하더라도 신인도(Dependability : Reliability, Availability, Safety, Maintainability, ...)를 갖는 침입 감내구조에 의해 서비스를 지속적으로 제공한다.

최근, 이러한 신인도를 갖는 시스템을 구현하기 위해 자율컴퓨팅의 4가지 핵심 기술 중의 하나인 자가치유(Self-healing) 메커니즘을 활용하는 접근 방법이 제시되고 있다[2]. 자가치유 기술은 결함허용(Fault-tolerant) 기법처럼 시스템의 신인도와 관련된 다양한 요소를 내포하고 있으나, 자가치유는 자기최적화(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[3].

2. 관련연구

[4]에서는 침입 감내시스템의 결함허용 기능 강화를 위해 디자인 다양성(Design Diversity)을 채택함으로써, 주서버와 보조서버가 각기 다른 운영체제와 웹서버 응용을 갖도록 구성하였으나, 두 서버가 Hot-standby 방식으로 연동되었기 때문에 외부 공격으로 인해 서버 모두 동시 손상되는 문제를 내포하고 있다. [5]에서는 침입 감내시스템이 외부공격 상황에서 갖추어야 할 동적인 이상거동을 상태천이도(State Transition Diagram)로 나타내고, 시스템이 가지는 취약성 및 위협 요소를 어떻게 모델링할 수 있는가에 대한 침입감내 프레임워크에 관한 연구를 진행하였고, [6]에서는 다양한 상태천이도을 바탕으로 서비스 거부 공격 등 몇 가지 침입 유형별 정량적 성능 분석을 시도하였다.

한편, [7]에서는 분산 임베디드 시스템의 신인도를 향상시키기 위해 자가치유 기술을 적용한 사례를 보여주고 있다. 본 논문에서는 주서버와 보조서버로 구성된 이중계 침입 감내시스템의 상태 천이를 자가치유 메커니즘의 두 가지 요소(Fault Model 및 System Response)를 활용하여 분석하였으며, 시뮬레이션 실험을 통해 침입 감내의 가용도(Availability)를 정량적으로 정의하였다.

3. 자가치유 메카니즘을 활용한 침입감내시스템

자가치유 시스템 요소 기술 중에 결함모델 및 시스템 반응에 관련된 세부 항목을 침입 감내시스템의 상태천이도로 나타낼 수 있다. 즉, 서비스 거부 공격에 대응하는 결함모델의 세부요소와, 그에 상응하는 시스템 반응(결함감지(Fault Detection), 기능퇴화(Degradation), 결함반응(Fault Response) 및 결함복구(Fault Recovery)) 등을 그림 1에 표현하였다.

그림 1은 자가치유 구성 요소가 반영된 이중계

· 이 논문은 2004년도 1학기 정착연구비 지원에 의하여 연구되었음.

Cold-standby(CS) 침입감내 상태천이를 나타내고 있으며, 모델링의 위해 사용된 가정은 아래와 같다.

- 각 상태에서의 평균잔류시간은 특정분포를 따르지 않는다.
- 주서버 가동 중에 보조서버는 고장나지 않는다.
- 보조서버가 정상상태(0,1)에서만 주서버로 작업전이(1,1) 된다.
- 보조서버가 공격상태(0,A) 일 때는 재활상태를 거친 후에 초기상태(1,1)로 전이된다.

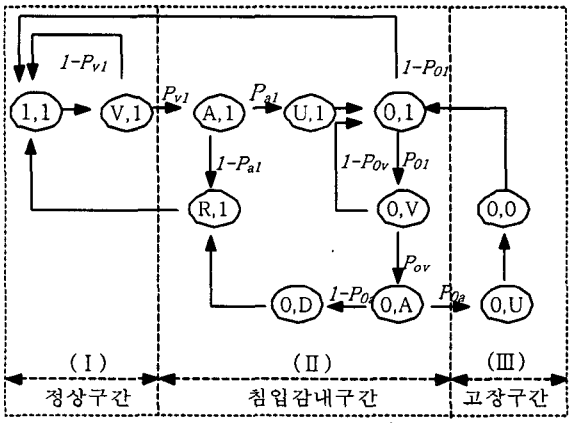

그림 1. 침입 감내시스템의 상태 천이도

주서버와 보조서버가 모두 정상적으로 동작하는 상태(1,1)에서 취약성(Vulnerability)이 노출되면, 침입 감내시스템은 (V,1)으로 천이된다. 침입감지모듈이 네트워크 트래픽 및 IP 주소 분석 등을 통해 모든 공격(Attacks)을 방어하면 일정시간 이후 초기상태로 복원되지만, 그렇지 못할 경우 p_{v1}의 확률로 주서버가 공격당하는 상태(A,1)로 바뀐다. 주서버 공격 상태가 일정시간 지속되면 시스템 손상이 누적되며, 이때 침입 진단(Diagnosis) 모듈이 시스템의 CPU 부하 및 메모리 상태를 분석하여, 유의할 수준의 성능저하가 $1-p_{a1}$의 확률로 진단될 경우 주서버를 재활상태(R,1)로 전이시키지만, 성능저하를 진단하지 못할 경우 감지불능(Undetected) 상태인 (U,1)상태로 전이되어 최종적으로 보조서버가 주서버 기능을 대신하도록 (0,1) 상태로 작업전이(Switchover)된다. 외부 공격에 의해 주·여분서버가 동시에 다운되는 상태를 방지하기 위해, CS 구성을 채택하였으며, 이 경우 작업전이에 필요한 시간이 길어지게 된다.

보조 서버가 주서버 역할을 대신하는 (0,1) 상태에서 보조서버가 다운되는 상태까지의 과정은 초기상태에서 주서버가 보조서버로 작업전이 되는 과정과 유사하지만, 자가치유 요소 중 기능퇴화 상태, 즉 보조서버가 공격상태에서 유의할만한 성능저하가 감지되었을 때 주서버가 회복될 때까지 시스템이 제공해야 하는 최소한의 서비스를 지속적으로 진행해주는 상태가 보장되어야 한다.

특히, SYN Flood 및 Smurfing과 같은 서비스 거부 공격의 경우 DNS 서버와 같은 특정 서버에 악의적인 Http 요청을 대량으로 발생시켜 시스템 리소스를 장악하는 성능저하를 야기하므로 그림 1의 (0,A)상태에서 시스템의 필수 서비스 기능을 보장해주는 점진적 기능퇴하(Gracefully Degradation) 상태인 (0,D)로의 전이가 필요하게 된다. 즉, (0,D)상태를 거침으로써 시스템의 가용도를 어느 정도 보장해 주고 주서버가 정상 가동될 경우 보조서버도 재활상태(R,1)를 거쳐 초기상태로 진입하게 된다.

전체적으로 그림 1에서 I 구간은 시스템의 기능 저하가 전혀 일어나지 않은 구간이고, (U,1)을 제외한 II 구간은 일정한 손상이 존재하지만 시스템이 제공해야 하는 서비스는 지속적으로 수행되고 있는 침입감내 구간이며, III은 침입 감내시스템 작동에도 불구하고 서비스를 하지 못하는 상태로써 주서버가 회복되지 못한 상태에서 보조서버까지 서비스 불가한 상태이다.

그림 1의 평형상태(Steady-State)의 가용도를 계산하기 위해 식 1의 확률과정을 정의하였으며, 서비스 시간이 일반적인 분포인 M/G/1을 적용한 세미마르코프 프로세스(SMP:Semi-Markov Process) 분석을 통해 각 상태에 머무는 확률을 계산하였다.

$$X(t) : t>0,\ Xs = \{ \text{그림1의 11가지 각 상태} \} \qquad (1)$$

그림 1은 모든 상태가 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, 침입 감내시스템 각 상태에 대한 SMP의 안정 상태 확률값이 존재하고 해당 SMP는 각 상태에서의 전이 확률을 이용한 임베디드 이산 마르코프체인에 의해 유도할 수 있다[8].

SMP의 각 상태에서의 평균 잔류시간을 h_i라 하고, 이산 마르코프체인 평형 상태 확률 ν_i를 구하면, SMP의 각 상태에 대한 평형 상태 확률 π_i를 식 2와 같이 계산할 수 있다[9].

$$\pi_i = \frac{\nu_i h_i}{\sum_i \nu_j h_j}, \quad i,j \in X_S \qquad (2)$$

평형 상태에서 시스템의 가용도 A는 ((U,1), (0,U), (0,0))를 배제한 경우로 식 3과 같이 정의하였다.

$$A = 1 - (\pi_{U1} + \pi_{00} + \pi_{0U}) \qquad (3)$$

4. 시뮬레이션 분석 및 가용도 향상 방안

침입 감내시스템의 SMP모델 분석 결과를 시뮬레이션하기 위해서는 전이 확률과 각 상태에서의 평균잔류시간(Mean Sojourn Time)에 대한 파라메타 설정이 이루어져야 한다. 본 논문에서는 표 1의 설정값을 기준으로 시

뮬레이션을 수행하였다[10]. 각 상태에서의 평균잔류시간이 특정분포를 따르지 않으므로 h_{ij}값은 상대적인 차이로서의 의미만 존재하며, 상태천이도에 나타난 5개 분기점에서의 전이확률 각각이 침입 감내시스템의 가용도에 독립적으로 미치는 영향을 분석하기 위해 초기 전이확률의 설정값을 0.5로 균등하게 설정하였다.

표 1. 시뮬레이션 파라미터

입력변수	설정값
Mean Sojourn Time	$h_{11}=.5, h_{V1}=1/3, h_{A1}=.25, h_{U1}=.5$ $h_{R1}=.2, h_{01}=.5, h_{0V}=1/3, h_{0A}=.25$ $h_{0D}=4, h_{0U}=2, h_{00}=2$
Transition Probability	5개 전이확률(p_{a1}, p_r, p_v, p_{a0}, p_d)중 4개는 고정하고 1개값을 변화(0부터 1까지) (예: $p_{v1}=p_{a1}=p_{01}=p_{0v}=0.5$, $0<p_{0a}<1$)

그림 2는 SMP모델의 상태천이도에서 정의된 5가지 전이확률 각각의 변화에 따른 시스템의 가용도 변동추이를 보여주고 있다.

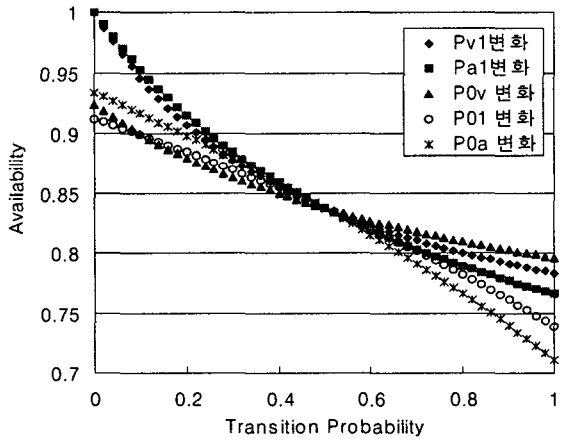

그림 2. 전이확률 변화에 따른 가용도 추이

전이확률 각각의 전체구간(0부터 1)에 대해 p_{a1}과 p_{0a}가 상대적으로 가장 큰 가용도 변화(약 24%) 요인으로 분석되었으며, p_{0v}는 약 14%로 가용도 변화에 가장 적은 영향을 미치고 있음을 알 수 있다. 즉, 주서버나 보조서버가 취약상태에서 공격상태로 전이된 경우 침입 감내 모듈의 진단기능이 유의할 수준의 시스템의 성능저하를 제대로 감지할 수 있어야만 (A,1) 및 (0,A) 상태에서 (R,1) 상태로 전이할 확률을 높여 시스템의 가용도 저하를 방지할 수 있게 된다. 한편, p_{v1}과 p_{a1}는 침입 감내시스템이 고장상태(Unavailable state)인 (U,1), (0,U) 및 (0,0)에 도달하기전의 전이확률이므로 초기값이 0일 때 다른 전이확률 값에 무관하게 시스템의 가용도는 1을 갖게 됨을 알 수 있다.

또한, 전이확률의 설정값이 1에 근접하게 되면 재활, 복구 그리고 취약성 감지 등을 통한 점진적 기능퇴화(Gracefully Degradation) 기능이 약해지므로 정상상태에서 보조서버가 고장상태로 이르기 직전인 (0,A) 상태로의 진행속도가 커지게 되므로 p_{0a}가 커질 경우 가용도 저하가 급속히 진행됨을 예상할 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 CS방식의 침입 감내시스템을 11가지 상태로 정의한 후 각 상태에서의 전이 확률 및 평균 잔류시간을 통해 이산 마르코프체인 평형 상태 확률 및 SMP 평형 상태 확률을 계산하여 시스템의 가용도를 분석하였다. 향후, 본 논문에서 고려한 자가치유 메커니즘의 두 가지 요소 이외에 시스템 완전성(System Completeness) 및 Design Context를 함께 고려한 모델링을 통해 시스템의 신인도를 향상시킬 수 있는 방안을 연구할 예정이다.

[참고문헌]

1. F. Wang, R. Uppalli, C. Killian, "Analysis of Techniques for Building Intrusion Tolerant Server Systems,"In proceedings of Military Communications Conference, Oct. 13-16, 2003.
2. P. Koopman, "Elements of the Self-Healing System Problem Space," ICSE WADS03, May 2003.
3. D.M. Chess, C. C. Palmer, S. R. White, "Security in an Autonomic Computing Environment," IBM Systems Journal, Vol. 42, No.1, 2003.
4. James. C. Reynolds, James. Just, Larry Clough, Ryan Maglich, "On-line Intrusion Detection Attack Prevention Using Diversity Generate-and-Test, and Generalization," Proc. of the 36th HICSS'03.
5. F. Goseva-Popstojanova, F. Wang, R. Wang, F. Gong, K. Vadyanathan, K. Trivedi, B. Muthusamy, "Characterizing Intrusion Tolerant Systems using a State Transition Model," DARFA Information Survivability Conference, pp. 211-221, 2001.
6. D. Z. Wang, B. B. Madan, and K. Trivedi ,"Security Analysis of SITAR Intrusion Tolerance System," ACM SSRS'03, 2003.
7. Charles P. Shelton, Philip Koopman, William Nace, "A Framework for Scalable Analysis and Design of System-Wide Graceful degradation in distributed Embedded Systems,"The Eighth WORDS03, Jan. 2003.
8. Leinard Kleinrock, Queueing Systems: Volume 1 Theory, John Wiley & Sons, 1974.
9. K. Trivedi, Probability and Statistics with Reliability Queueing and Computer Science Applications, p. 472, 2002.
10. Bharat B. Madan, K. Goseva-Popstojanova, K. Vadyanathon, K. Trivedi, "Modeling and Quantification of Security Attributes of Software Systems,"Int. Conference on Dependable Systems and Networks, pp.505-514, 2002.