네트워크 기반 컴퓨팅에서 주-백업 침입감내시스템의 생존성 분석

박기진* 남궁미정 0** 박미선**
아주대학교 공과대학 산업정보시스템공학부* 안양대학교 문리과학대학 컴퓨터학과**
kiejin@ajou.ac.kr* {mjmj201 0, oooooo82}@anyang.ac.kr**

A Survivability Analysis of Primary-Backup Intrusion Tolerant System for Network Computing

Kiejin Park* Mijung Namgung 0** Misun Park**
Division of Industrial & Information Systems Engineering, Ajou University*
Department of Computer Engineering, Anyang University**

요 약

고속 네트워크와 이질적인 자원의 결합으로 구성되어 보안에 취약할 수 밖에 없는 네트워크 기반 컴퓨팅 환경을 대상으로 내·외부적 공격이나 결함이 발생하더라도 중요한 서비스를 지속적으로 제공하여, 시스템의 피해를 최소화하는 침입감내시스템(Intrusion Tolerant Systems)에 대한 연구가 활발하다. 본 논문에서는 주-백업 구조를 갖는 침입감내시스템 구조를 제안하였으며, 마코브 분석(Markov Analysis)을 통해, 시스템 생존성을 정량적으로 정의하였다.

1. 서 론

최근 네트워크 침입 사례 증가에 따른 침해사고의 예방 및 대응에 관련된 정보보호 기술들이 활발히 연구되고 있으며, 방화벽, 백신, 침입탐지(Intrusion Detection) 및 침입방지(Intrusion Prevention) 등의 다양한 보안 기술들은 알려진 취약점(Vulnerability)에 대한 공격에 대해서는 탐지, 예방 및 치료가 가능하나, 의도적이든 의도적이지 않던 알려지지 않은 공격이나 결함에 대해서는 취약하다는 단점을 가지고 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.

따라서 네트워크 기반 컴퓨팅에서의 침입에 대한 예방 및 대응 방식으로 침입감내(Intrusion Tolerance) 기술이 비교적 최근에 활발히 연구되고 있다.

침입감내기술은 결함허용(Fault Tolerance) 기술과 컴퓨터 보안(Computer Security) 기술이 결합된 형태로 중요한 서비스를 제공하는 시스템에 결함이나 악의적 공격이 발생했을 경우 원래의 시스템이 제공해야 하는 정상적인 서비스를 일정한 시간동안 지속적으로 제공하기 위한 기술이다. 최근 유럽에서는 FP5 의 IST 프로그램을 통한 연구를 진행하였으며[1], 미국에서도 DARPA 의 OASIS 프로그램을 통한 HACQIT, SITAR, Willow, ITUA, AITDB 등의 침입감내시스템 관련 프로젝트가 수행 중에 있다[2].

본 논문에서는 주-백업 구조를 갖는 침입감내시스템 구조를 제안하였으며, 마코브 분석을 통해 시스템 생존성을 정략적으로 분석하였다. 본 논문의 2 장에서는 현재 진행중인 침입감내시스템(ITS: Intrusion Tolerant Systems) 관련 프로젝트들의 특징을 언급하고, 3 장에서 침입감내를 위한 모델링 방법을 제시하였으며, 4 장에서는 제안한 방법의 성능 평가를 수행하고, 5 장에는 결론을 내렸다.

본 연구는 한국과학재단 목적기초연구(R05-2003-000-10345-0) 지원으로 수행되었음.

2. 관련 연구

악의적인 성격을 띤 침입자들에 대한 예방 및 대응 방법으로 결함허용 개념이 적용된 침입감내기술이 미국과 유럽을 중심으로 최근 활발히 연구되고 있다. SITAR[3]는 분산서비스, 특히 COTS(Component off the Shelf) 서버를 위한 침입감내 구조를 제시함으로써, 취약성을 보강하고 필수 응용에 대해 최소한의 서비스 제공이 가능하도록 하였으며, COTS 서버를 변경 없이 적용하여 투명하다는 장점이 있으나, 과도한 지연 가능성 및 복잡한 구조로 인해 구현 비용이 증가되는 단점이 있다. HACQIT[4]는 사용자 25%이상의 저하를 방지하면서 네 시간 동안의 침입감내 제공을 목표로 하며, 감내하고자 하는 대상으로는 소프트웨어 오류에 관한 것만 다룬다. 또한, MAFTIA[5]는 유럽에서 지원하고 있는 침입감내시스템으로 악성 프로그램 및 결함에 의한 결함허용과 정보보증을 목적으로 한다.

침입감내시스템 프레임워크는 크게 계층기반과 복제기반로 나눌 수 있는데, 계층기반 구조는 단일 호스트에 적용되며 무결성이 강조되고, 복제기반 구조는 분산 컴퓨팅 환경에 적용되며 가용성 확대가 목적이나 복제 증가로 인한 기밀성에 대한 위협이 증가된다[6]. 또한, 침입감내시스템은 보안 손상 상태에서 정상 상태로 전환시키는 것이 기본적인 작업이기 때문에, 시스템의 침입 형태 및 현재 상태를 파악하여 이를 상태전이 모델로 표현할 경우 정량적인 성능 분석이 가능하다. 즉, 침입감내시스템은 공격자에 의해 취해지는 동적인 이상거동을 시스템 취약성 또는 위협 요소에 따라 대응하게 되므로, 이들의 상태 변화를 정확히 묘사해야한다.

3. 주-백업 침입감내시스템(Primary-Backup ITS)

본 연구에서 고려한 침입감내시스템은 결함허용시스템에서 주로 사용되는 주-백업 구조를 택하므로써, 가용도 향상 및 데이터 무결성을 달성하고자 한다. 주-백업 방식의 침입감내 시스템 설계에 적용된 가정은 아래와 같다.

- 주-백업 침입감내시스템간의 작업전이(Switchover)는 Cold Standby 방식을 따른다.
- Cold Standby 방식이기 때문에, 일정 시간을 주기로 주서버와 백업 서버는 동기화 된다.
- 주-백업 침입감내시스템의 각 상태에 머무를 시간은 일반 분포를 따른다.
- 시스템이 안정 상태에 있을 때만 침입이 가능하다. 즉 최초의 가동되는 시스템은 안정적이다.

3.1 침입감내시스템 상태 전이도

주-백업 침입감내시스템은 각각 S(Safe State), U(Unsafe State), A(Active Attack State), F(Failed State) 상태로 구성되며, 이들은 침입으로 인해 야기될 수 있는 시스템의 상태 변화를 표현할 때 사용된다(그림 1 참조).

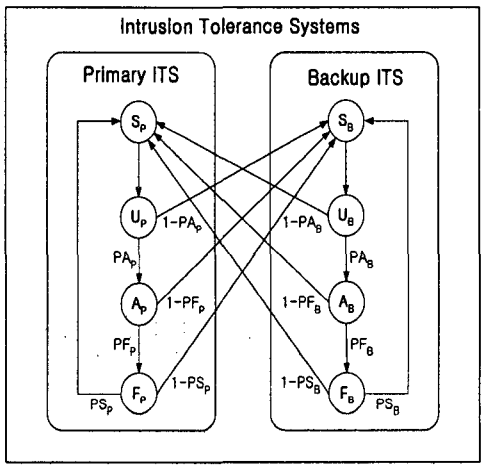

그림 1. 주-백업 침입감내시스템의 상태전이도

주 시스템은 안정 상태(S_P)에서 공격자가 권한없이 정보나 자원에 접근을 시도하는 등 취약성이 노출되면, 취약성이 노출된 U_P 상태로 전이되고, 이 상태에서 공격이 가해지기 전에 침입을 탐지하면, 현재 작동하고 있는 주 침입감내시스템에서 백업 침입감내시스템으로 작업전이되면서, $1-PA_P$ 의 확률로 S_B 상태에 진입하게 된다. 이 경우 이전 주 침입감내시스템이 Off-line 이 되므로 공격과는 무관하게 지속적인 서비스가 보장된다. 하지만 주 시스템의 취약성이 노출된 상태(U_P)에서 침입을 탐지하지 못하여, PA_P 의 확률로 공격이 성공할 경우, 주 시스템은 공격을 당하고 있는 A_P 상태로 전이되고, 시스템의 성능이 점차 저하된다. 침입자가 공격중인 상태(A_P)에서 이를 탐지하면 S_B 상태로 진입하여, 정상적인 서비스를 제공하나, 탐지하지 못했을 경우에는 F_P 상태로 전이된다. F_P 상태는 고장 상태로, 시스템이 재구성되어 안정 상태(S_P)로 복원되는데, 이 때 백업 침입감내시스템이 정상 가동 중이면, S_B 상태로 우선적으로 진입하게 된다. 백업 침입감내시스템은 주 서버를 대신하여, 서비스를 지속적으로 제공하게 된다. 만일 F_P 상태에서 백업 침입감내시스템이 가용하지 않을 경우, 주

침입감내시스템의 S_P 상태로 전이된다. 이와 같은 상태전이 작업들은 백업 침입감내시스템에서도 동일하게 이루어진다.

3.2 SMP(Semi Markov Process) 모델링 분석

제안된 상태전이 모델의 평형 상태(Steady State)에서의 생존 능력 척도 중의 하나인 가용도를 계산하기 위해 식 1 에서 각 상태에 대한 확률 과정을 정의하였으며, 이 때 각 상태에 머무는 시간(Sojourn Time)이 일반적 분포를 따르기 때문에, 그림 1 상태는 M/G/1 큐잉모델 기법을 적용한 SMP 로 모델링 될 수 있다.

$$X(t): \ t > 0,\ X_S = \{S_P, U_P, A_P, F_P, S_B, U_B, A_B, F_B\} \qquad (1)$$

침입감내시스템의 각 상태에 대한 SMP 의 평형 상태 확률 Π_i 는 식 2 와 같으며, h_i 는 각 상태에서의 평균 잔류 시간을 나타낸다. 또한 v_i 는 이산마르코프체인의 평형 상태 확률을 의미한다.

$$\Pi_i = \frac{v_i h_i}{\sum_i v_j h_j}, \quad i, j \in X_s \qquad (2)$$

주-백업 침입감내시스템에서의 가용도 A 는 F_P 상태와 F_B 상태가 배제되어 식 3 과 같이 정의된다.

$$A = 1 - (\Pi_{F_P} - \Pi_{F_B}) \qquad (3)$$

4. 성능 평가

침입감내시스템의 SMP 모델을 분석하여, 생존 능력의 수치적 검증을 위한 성능 평가를 위해 아래와 같은 파라미터를 사용하였다.

표 1 시뮬레이션 파라미터 정보

입력 변수	파라미터 값
평균 잔류 시간	h_A=0.25, h_U=0.33, h_F=1.0, h_S=0.5
전이 확률	PS_P, PA_B, PF_B, PS_B=0.5 0<PA_P, PF_P<1

그림 2 에서는 제안한 침입감내시스템의 생존 능력을 알아보기위해, PS_P, PA_B, PF_B, PS_B 의 확률 값을 고정시키고, PA_P 와 PF_P 의 확률 값을 변경시켜 가면서, 가용도를 측정하였다. PA_P, PF_P 가 1 에 접근할수록 가용도가 감소함으로써 시스템이 불안정해지는 반면에, 주 침입감내 시스템에서 건강한 상태(Healthy state)에 있는 백업 침입감내시스템으로 전이하는 과정($U_P \rightarrow S_B$, $A_P \rightarrow S_B$, $F_P \rightarrow S_B$, $U_B \rightarrow S_P$, $A_B \rightarrow S_P$, $F_B \rightarrow S_P$)의 확률이 높을 때는 시스템 가용도가 증가되는 것을 확인하였다. 따라서 취약성 또는 침입한 공격이 성공하기 전에 백업 침입감내시스템으로 전이시킴으로써, 시스템의 생존성을 높일 수 있다고 판단된다.

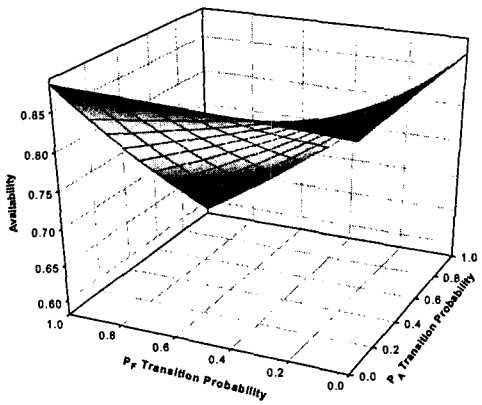

그림 2. 상태 전이에 따른 가용도 변화

5. 결론 및 향후 연구

본 논문에서는 침입감내기술의 주요 목적인 가용도와 데이터 무결성을 향상시키기 위해 주-백업 침입감내시스템을 제시하였으며, SMP 분석을 통해 시스템의 생존 능력 척도의 하나인 가용도를 분석하였다. 추후에는 소프트웨어 결함뿐 아니라 하드웨어의 자체 결함도 고려한 주-백업 침입감내시스템을 연구할 예정이다.

참고문헌

[1] http://www.romnet.net/conference/1/text2.html

[2] http://www.darpa.mil

[3] Feiyi Wang, et. al., "SITAR : A Scalable Intrusion-Tolerant Architecture for Distributed Services," Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, 2001.

[4] J. Just, et. al., "Intrusion Tolerance through Forensics-Based Attack Learning." Proc. Of the ICDSN 2002 Supplementary Vol., pp.C-4-1. June 2002 IEEE CS

[5] Paulo Verissimo. et. al., "The Timely Computing Base: Timely Actions in the Presence of Uncertain Timeliness." Proc. Of the ICDSN 2000, pp.533-542. IEEE CS

[6] 김기한, 최명렬, 이경환,. "생존성 강화를 위한 침입감내시스템의 분류와 통합 프레임워크 제안." 한국정보처리학회. 2003. pp.295-305