패킷 필터링을 사용한 네트워크 보안 시뮬레이션*

김태헌** · 이원영** · 김형종*** · 김홍근*** · 조대호**

Simulation of Network Security with Packet Filtering System

Kim, Tae Heon, Lee, Won Young, Kim, Hyung Jong, Kim, Hong Geun, Cho, Tae Ho

Abstract

네트워크 보안은 정보통신 및 인터넷 기술이 발전함에 따라 그 중요성과 필요성이 더욱 절실해지고 있다. 본 연구에서는 네트워크 보안의 대표적인 침입 차단 시스템의 패킷 필터 및 네트워크 구성요소들을 모델링하였다. 각 모델은 DEVS 모델을 참조한 MODSIM III 기반의 기본 모델(Basic Model)과 결합 모델(Compound Model)의 두 가지 유형으로 정의하였다. 기본 모델은 독립적인 기능을 수행하는 단위 모델을 표현하고, 결합 모델은 여러 개의 모델이 연동되어 상위 레벨의 시스템을 표현한다. 시뮬레이션을 위한 모델링과 그래픽 기능이 강력한 MODSIM III를 기반으로 모델들을 비롯한 시뮬레이션 환경을 구현하였다. 대상 네트워크 환경에서 사용한 공격은 서비스 거부 공격 형태인 SYN flooding 공격과 Smurf 공격을 발생하였다. 이 공격들에 대하여, 패킷 필터 모델에 다양한 보안 정책을 적용하여 시뮬레이션을 실행하였다. 본 연구에서의 시뮬레이션을 통하여, 과거의 단순 패킷 필터링에서 진일보한 Stateful Inspection의 우수한 보안 성능과, 보안 정책의 강도를 점점 높였을 때 보안 성능이 향상되는 점을 검증하였다.

1. 서론

네트워크 보안은 정보통신 및 인터넷 기술이 발전함에 따라 그 중요성과 필요성이 더욱 절실해지고 있다. 본 연구에서는 네트워크 보안의 대표적인 침입 차단 시스템의 패킷 필터 및 네트워크 구성요소들을 모델링하였다. 각 모델은 DEVS 모델을 참조한 MODSIM III 기반의 기본 모델(Basic Model)과 결합 모델(Compound Model)의 두 가지 유형으로 정의하였다. 기본 모델은 독립적인 기능을 수행하는 단위 모델을 표현하고, 결합 모델은 여러 개의 모델이 연동되어 상위 레벨의 시스템을 표현한다. 시뮬레이션을 위한 모델링과 그래픽 기능이 강력한 MODSIM III를 기반으로 모델들을 비롯한 시뮬레이션 환경을 구현하였다. 대상 네트워크 환경에서 사용한 공격은 서비스 거부 공격 형태인 SYN flooding 공격과 Smurf 공격을 발생하였다. 이 공격들에 대하여, 패킷 필터 모델에 다양한 보안 정책을 적용하여 시뮬레이션을 실행하였다. 본 연구에서의 시뮬레이션을 통하여, 과거의 단순 패킷 필터링에서 진일보한 Stateful Inspection의 우수한 보안 성능과, 보안 정책의 강도를 점점 높였을 때 보안 성능이 향상되는 점을 검증하였다.

이로 인해 막대한 자원의 손실과 사회적 신뢰의 손상이 발생할 수 있다는 점에서 심각한 사회문제로 이어지고 있고, 정보 보안에 대한 인식

* 본 연구는 2001년도 한국정보보호진흥원 시스템기술연구 위탁과제로 수행되었음.
** 성균관대학교 전기전자 및 컴퓨터공학과
*** 한국정보보호진흥원 기술단

과 필요성이 높아가고 있다. 특히 네트워크에 대한 보안 대책이 필요한 이유는 단지 일부 데이터를 악의적인 목적으로 탈취하려는 사람이 있기 때문만이 아니다. 조금 더 넓은 의미로 생각해 본다면, 데이터 통신이 자체적으로 내포하고 있는 위험들이 있기 때문이며, 이것은 데이터 통신을 구성하는 것이 사람이 아니라 컴퓨터이고 컴퓨터 그 자체가 안고 있는 위험 때문에 필요한 것이다[1].

본 연구의 목표는 패킷 필터에 다양한 보안 정책을 적용하여, 보안 시스템 성능과 보안 성능 향상을 검증하는 것이다. 본 연구의 범위는 네트워크 보안의 대표적인 침입 차단 시스템을 분석하고 보안 정책을 적용할 수 있도록 모델링하는 것, 그리고 최근의 대표적인 공격과 추상화한 모델들로 구성된 시뮬레이션 환경을 구축하는 것이다.

2. 모델링 및 시뮬레이션의 배경 이론과 환경

본 연구에서는 이산 사건 모델링 기법을 이용하여 복잡한 네트워크 구조를 계층적으로 명확하게 표현하고, 네트워크 구성원의 동적 특성을 객체지향 개념에 따라 독립적이고 재사용이 용이하게 표현하기 위한, 구조적베이스(Structural Base)와 동적베이스(Behavioral Base)를 이용하여 표현한다.

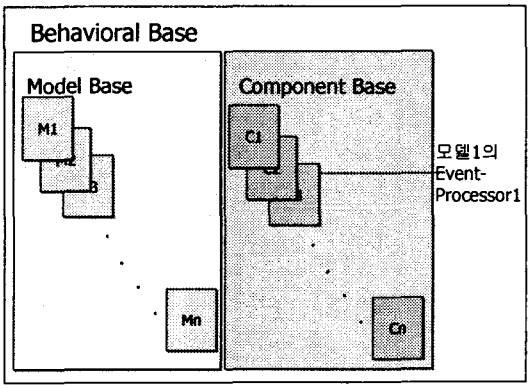
2.1 구조적베이스와 동적베이스

System Entity Structure(SES)는 시스템의 구조적 지식을 효과적으로 표현하기위한 방법의 하나로 Zeigler가 제안한 개념이다[3]. SES에서는 엔터티와 엔터티들의 연관관계를 세 가지 형태로 정의하고 있다. 엔터티는 모델 정의를 위한 실제의 개념적 구성요소를 표현하는 것이며, 이들의 관계성은 [표 1]과 같이 표현된다.

[표 1] SES에서의 구조적 지식 표현

연관관계	설명
Entity-aspect(Ⅰ)	엔터티와 그것의 구성요소 관계 표현
Entity-specialization(Ⅱ)	엔터티와 그것의 종류 관계 표현
Multiple entity(Ⅲ)	복수개의 엔터티가 또 다른 엔터티가 되는 관계 표현

동적베이스는 시스템의 동적 특성을 표현한 집합들로, 본 연구에서는 (그림 1)과 같이 모델 베이스(Model Base)와 구성요소 베이스(Component Base)로 구성된다. 모델 베이스는 시뮬레이션 대상이 되는 시스템의 가장 작은 표현인 모델 단위의 집합이고, 구성요소 베이스는 모델 베이스 내에서 각 모델들을 구성하는 요소의 동적 특성을 나타내는 구성요소 단위의 집합이다.



(그림 1) 동적베이스

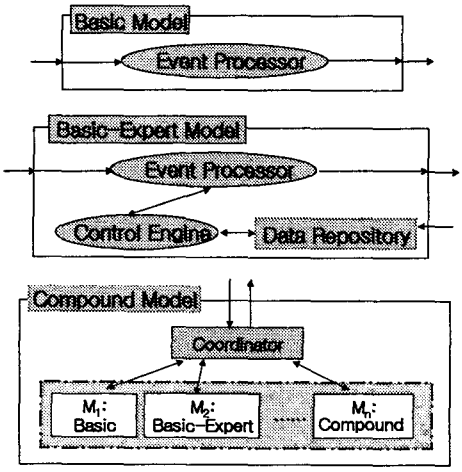
2.2 모델의 종류

연속적인 시간상에서 발생되는 이산 사건을 처리하는 시스템을 시뮬레이션하기위해 이론적으로 정립된 모델링 방법론인 DEVS(Discrete EVent system Specifications) 형식론[3,4]을 참조하여 [표2]와 같이 MODSIM Ⅲ 기반의 기본모델(Basic Model)과 결합모델(Compound Model)의 두 가지 유형으로 정의하였다.

[표 2] MODSIM III 기반 모델

	모델유형	모델 구성 요소
MODSIM III 기반모델	Basic Model	M = < X, S, Y, δ, λ > X : 입력 이벤트 집합 S : 상태 집합 Y : 출력 이벤트 집합 δ : 상태 전이 함수, S? → S λ : 출력 함수, S → Y
	Compound Model	CM = < Mi , Ii , Zij > Mi : 구성 모델 Ii : 모델 i와 연관된 모델의 집합 Zij : 모델 i와 모델 j간의 연결함수, Zij : Si → Xj

기본 모델(Basic Model)은 독립적인 기능을 수행하는 단위 시스템을 표현하는 모델로서, (그림 2)와 같이 기본 모델이 구성되어있고, 이벤트 처리기(Event Processor)는 모델 단위의 이벤트 처리에 관련된 내용 즉, 모델 단위의 상태 변화, 시간 흐름에 따른 스케쥴, 데이터 흐름 제어 등을 수행한다. 기본-전문가 모델(Basic-Expert Model)에서는 입력되는 조건과 정보를 보관하는 데이터 저장소(Data Repository)와 제어 엔진(Control Engine)이 추가되어, 여기에 보안 정책이 표현되고 이에 따른 의사 결정이 이루어진다.



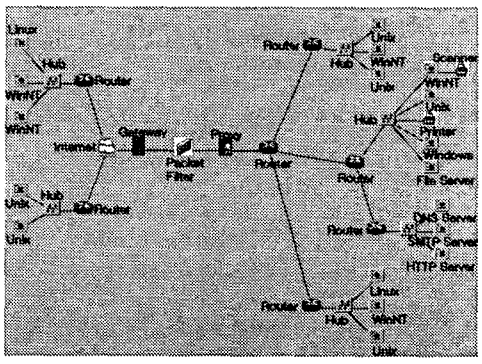
(그림 2) 모델 유형과 구성요소

결합 모델(Compound Model)은 여러 개의 모델이 연동되어 상위 레벨의 시스템을 표현하기 위한 모델로서, 결합 모델의 구성요소는 (그림 2)와 같이 연동될 기본 모델 또는 결합 모델 집합과 모델들 간의 상호작용 및 외부와의 인터페이스를 위한 조정자(Coordinator)로 구성된다.

2.3 MODSIM III 기반 시뮬레이션

MODSIM(MODular SIMulation language)은 시뮬레이션을 하기 위한 모델링 언어 및 그래픽 도구를 제공하는 소프트웨어이다[7]. MODSIM은 다음과 같은 특징을 가지고 있기 때문에 본 연구에 있어 중요한 의미를 갖는다. 첫째, MODSIM은 범용 시뮬레이션 언어로 대상 시스템을 특정 도메인으로 제한하지 않기 때문에 어떤 시스템도 모델링이 가능하다. 둘째, 모듈 개념을 사용하여 시스템을 표현하고, 이를 프로그램에 그대로 반영하기 용이하도록 모듈화 구조를 제공한다. 셋째, 객체 지향 프로그래밍 언어이다. 넷째, 시뮬레이션의 여러 형태 중 연속된 시간상에서 이산적으로 사건(event: 시스템의 상태를 변화시키는 일)이 발생되는 시스템을 시뮬레이션 하는데 적합하다. 다섯째, 애니메이션 기능으로 시뮬레이션의 과정 및 결과를 움직이는 그래픽 객체들을 통해 관찰할 수 있어, 모델 검증 및 시뮬레이션 확인 작업을 용이하게 한다. 여섯째, MODSIM이외의 프로그래밍 언어(C/C++) 코드를 추가할 수 있도록 지원한다.

3. 시뮬레이션 대상 네트워크 환경 및 모델링 대상 시스템 특성과 보안 정책



(그림 3) 대상 네트워크 구조

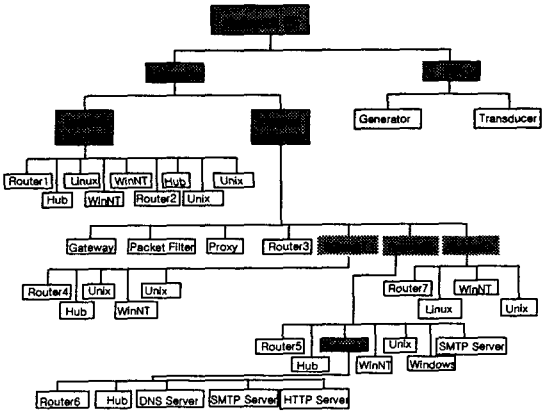
본 연구에서는 (그림 3)과 같은 네트워크 구조와 서비스 거부 공격 형태인 SYN flooding 공격과 Smurf 공격을 사용하여[1,6,7], 대상 네트워크 환경을 구성하였다. SYN flooding 공격은 많은 수의 반연결(half-open) TCP 연결을 시도(SYN 패킷 전송)하여 상대 호스트의 연결 대기 큐를 가득 채움으로써 정상적인 TCP 서비스 연결을 거부되게 한다. Smurf 공격도 서비스 거부 공격의 형태로 ICMP echo reply 패킷으로 인해 시스템 부하가 증가되거나 마비된다.

모델링 대상 시스템으로는 시뮬레이션 대상 네트워크 환경을 고려하여, 네트워크 보안에 있어서 대표적인 침입 차단 시스템의 패킷 필터로 정하였다. 침입 차단 시스템은 외부 네트워크의 침입에 대해 내부 네트워크를 보호하기 위한 네트워크 구성요소 중의 하나로서, 외부의 불법 사용자의 침입으로부터 내부의 전산자원을 보호하기 위한 정책 적용을 지원하는 하드웨어와 소프트웨어를 말한다[6,8]. 패킷 필터는 패킷의 헤더 및 데이터 정보를 분석하고, 규칙 테이블을 적용하여 패킷의 흐름을 제한한다. 정적 패킷 필터링은 필터링 규칙이 정적으로 관리자의 입력에 의해 정해지고, 네트워크 계층의 헤더 정보만으로 개별적인 패킷의 필터링을 수행하여 허용 여부를 결정한다. 동적 패킷 필터링은 필터링 규칙이 입력되는 패킷에 의해 동적으로 정해지고, 네트워크 계층의 헤더를 포함한 상위 모든 계층의 정보를 고려하여 필터링을 수행한다. 보안 정책에 따라 요구되는 관찰 대상 정보를 추출하여 동적 상태 테이블(Dynamic State Table)에 유지하고, 이 테이블을 근거로 연속되는 패킷들의 연관성을 고려하여 필터링을 수행한다[9,10].

패킷 필터에 적용한 정책으로 다음과 같은 것들이 있다[1,9,11,12]. 신뢰 도메인으로부터의 패킷 통과, 내부 IP 주소로 위장한 패킷 차단, ICMP echo request 패킷 차단, 취약한 서비스 포트 차단, SYNDefender Relay와 SYNDefender Gateway 기능, 그리고, Committed Access Rate (CAR) 기능이 있다.

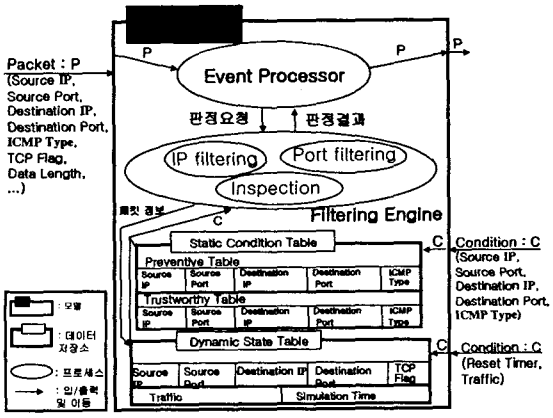
4. 모델 디자인

(그림 4)는 본 연구에서 사용한 대상 네트워크 망의 구조를 SES 기법[3]으로 나타낸 대상 네트워크의 시스템 구조이다.



(그림 4)

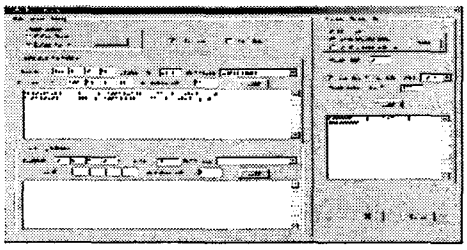
패킷 필터의 기능적 특성을 추상화하여 나타낸 모델의 기능 명세를 (그림 5)에 나타내었다.



(그림 6)

5. 시뮬레이션

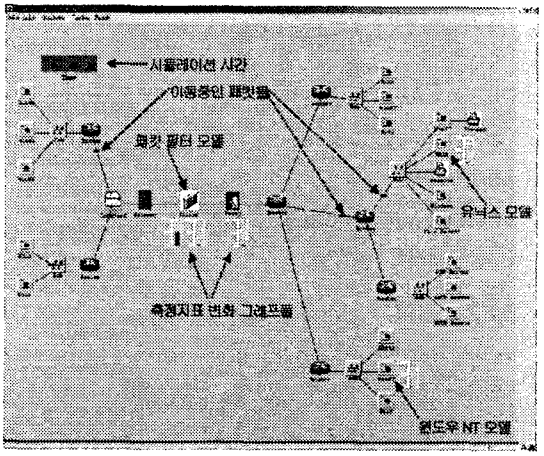
패킷 필터 모델에서는 보안 정책에 따른 파라미터를 (그림 6)과 같이 설정할 수 있다.



(그림 6) 패킷 필터 모델 파라미터 설정

5.1 실행

본 시뮬레이션은 두 가지 공격에 대하여, 패킷 필터 모델에, 총 8개의 보안 정책을 조합한 7개의 시나리오를 구성하여 실행하였다. 공격 및 정상 패킷은 각 공격에 따른 8가지씩의 패킷 유형을 균일 분포로 발생하였으며, 패킷의 발생 시간 간격(inter-arrival time)은 네트워크에서의 일반적인 패킷의 흐름을 나타내는 지수 분포를 사용하였다[13]. 측정 시간은 시뮬레이션 실행 전 모델에서의 파일럿 수행을 통하여 얻은 적정 수준의 값인 단위 시간 600000을 사용하였다. 단위 시간 1000이 실제 시간 1초에 해당한다. 각각의 시나리오에 대하여 5번씩 다른 seed 값, 1, 3, 5, 7, 9를 사용하여 시뮬레이션을 실행하였다. 시뮬레이션을 실행하면 (그림 7)과 같이, 발생된 패킷이 이동하고 패킷의 정보와 보안 시스템 모델의 정책에 따라 측정 지표의 변화를 동적으로 보여준다.



(그림 7) 동적 시뮬레이션 실행

SYN flooding 공격과 Smurf 공격에 대해, [표 3]과 같은 패킷 필터 모델에서의 적용 가능 정책과, [표 4]와 같은 시나리오를 구성하였다.

[표 5]에서와 같이 입력 데이터의 50%는 공격 패킷이고, 50%는 정상 패킷이며, 총 공격 패킷 중 50%는 Smurf 공격이며, 75%는 SYN flooding 공격이다.

[표 3] SYN flooding과 Smurf 공격에 대한 적용 정책

보안 모델	기능 모듈	적용 가능 정책	ID
패킷 필터	정적 패킷 필터링	아무런 정책을 적용하지 않음	FS-0
		내부 위장 패킷 차단	FS-1
		ICMP echo request 차단	FS-2
		신뢰 도메인으로부터의 패킷 통과	FS-3
	동적 패킷 필터링	아무런 정책을 적용하지 않음	FD-0
		SYNDefender Relay방식 사용	FD-1
		SYNDefender Gateway방식 사용	FD-2
		Committed Access Rate기능 사용	FD-3

[표 4] SYN flooding과 Smurf 공격에 대한 시나리오

시나리오	적용 정책
scenario_1	FS-0 + FD-0
scenario_2	FS-1
scenario_3	FS-1 + FS-2
scenario_4	FS-3
scenario_5	FS-3 + FD-1
scenario_6	FS-3 + FD-2
scenario_7	FS-3 + FD-2 + FD-3

[표 5] SYN flooding과 Smurf 공격에 대한 입력 유형

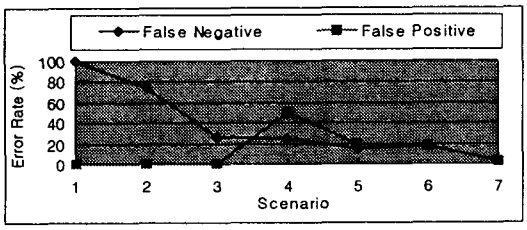
패킷 유형	source IP	tar-get IP	TCP flag	Prot-ocol	ICMP type	Data Length (KByte)	N/A	발생 비율 (%)
1	external	internal	-	ICMP	echo req.	30	공격	12.5
2	internal		syn	TCP	-	30	공격	12.5
3	external & trusty		syn	TCP	-	30	정상	12.5
4			ack	TCP	-	30		12.5
5			syn	TCP	-	30	공격	12.5
6	external & untrusty		syn	TCP	-	30	정상	12.5
7			ack	TCP	-	30		12.5
8			syn	ICMP	echo req.	30	공격	12.5

[표 5]의 패킷 유형에 따른 패킷 필터 모델에서의 결과를 예상하면 [표 6]과 같다.

[표 6] SYN flooding과 Smurf 공격에 대한 패킷 필터 모델에서의 예상 결과

패킷 유형	scenario 번호						
	1	2	3	4	5	6	7
1	허용	허용	차단	차단	차단	차단 가능	차단 가능
2	허용	차단	차단	차단	차단 가능	차단 가능	차단 가능
3	허용	허용	허용	허용	허용	허용	허용 가능
4	허용	허용	허용	허용	허용	허용	허용 가능
5	허용	허용	허용	허용	차단 가능	차단 가능	차단 가능
6	허용	허용	허용	차단	차단 가능	차단 가능	차단 가능
7	허용	허용	허용	차단	허용	허용	허용 가능
8	허용	허용	차단	차단	차단 가능	차단 가능	차단 가능

SYN flooding 공격과 Smurf 공격에 대한 패킷 필터 모델에서의 시뮬레이션 측정 지표는 False Negative와 False Positive를 사용하였다. (그림 8)에서 알 수 있듯이, 정적 패킷 필터링 기능을 사용했을 때 높은 False Negative와 False Positive가 동적 패킷 필터링 기능을 사용함으로써 떨어지는 것을 알 수 있고, 정책을 누진 적용할수록 False Negative가 떨어지는 것을 알 수 있다.



(그림 8) 패킷 필터 모델에서의 측정 지표 경향

5.2 결과 및 고찰

보안 시스템 및 네트워크 구성 모델들과 공격으로 구성된 네트워크 환경에서의 시뮬레이션을 통하여 다음과 같은 사항을 검증할 수 있었다.

첫째, 패킷 필터링 기능 사용에 있어서, 정적 패킷 필터링만 사용할 때 보다 동적 패킷 필터링인 Stateful Inspection 기능을 추가 사용할 때 훨씬 뛰어난 보안 성능을 발휘한다는 것을 검증하였다.

둘째, 하나의 보안 시스템에, 보안 정책을 누적 적용했을 때 즉, 보안 강도를 높였을 때 보안 성능이 훨씬 높다는 것을 검증할 수 있었다.

6. 결론 및 향후 연구과제

본 연구를 통하여 달성한 내용으로는, 첫째, 침입 차단 시스템을 분석하였다. 둘째, 분석된 내용을 바탕으로 침입 차단 시스템의 대표적 기능인 패킷 필터링을 모델링하였다. 셋째, 최근의 두드러진 공격 형태인 서비스 거부 공격에 대해 다양한 보안 정책들을 분석 및 적용하여 시뮬레이션을 실행하였다. 본 연구의 시뮬레이션 실행을 통하여, 패킷 필터링 기능에 있어서 과거의 단순 패킷 필터링에서 진일보한 Stateful Inspection의 우수한 성능을 검증하였다. 또, 보안 정책을 점점 강화할수록 보안 성능이 향상되는 점을 검증하였다.

본 연구의 의의는 침입 차단 시스템의 분석 및 성능 검증을 통하여 보안 효율을 향상할 수 있다는 점이다. 또 향후 보안 시스템 모델링 및 네트워크 보안 시뮬레이션 연구의 기초 자료가 될 것이다. 그리고, 네트워크 보안 환경을 그래픽 유저 인터페이스로 편집함으로써 다양한 환경을 구성하여 시뮬레이션을 실행할 수 있는, 동적인 네트워크 보안 시뮬레이터 개발의 초석이 될 것으로 기대된다. 따라서, 향후 연구 과제로는 보안 시스템 모델링의 확장과 시뮬레이션에의 적용, 그리고 네트워크 보안 환경을 동적으로 구성할 수 있는 시뮬레이터 개발 진행이 필요할 것으로 판단된다.

참고문헌

1) Joel Scambry, "HACKING EXPOSED 2nd Ed. : Network Security Secrets & Solutions," McGraw-Hill, 2001.
2) F. Cohen, "Simulating Cyber Attacks, Defences, and Consequences," Computer & Security, Vol.18, pp. 479-518, 1999.
3) B. P. Zeigler, "Object-Oriented Simulation with Hierarchical, Modular Models," Academic Press. 1990.
4) B. P. Zeigler, H. Praehofer, T. G. Kim, "Theory of Modeling and Simulation," 2nd Ed., Academic Press, 2000.
5) CACI Company, MODSIM III Manual, 1997.
6) 한국정보보호진흥원, "정보보호 교육자료," http://www.kisa.or.kr
7) 정현철 외, "분산서비스거부공격 등 최근 해킹기법과 대응방안," 정보처리학회지, 7권 2호, 2000.
8) E. D. Zwicky, "Building Internet Firewalls," 2nd Ed., O'Relly & Associates, 2000.
9) Avolio and Blask, "Application Gateways and Stateful Inspection : A Brief Note Comparing and Contrasting," Trusted Information System, Inc., 1998.
10) http://www.checkpoint.com/products/technology/stateful1.html
11) 조기준, 김훈희, "보안시스템 전문가들이 공개하는 해킹과 방어 완전 실무", 구민사, 2001.
12) http://www.checkpoint.com/products/technology/stateful1.html, Stateful InspectionTM Firewall Technology - TECH NOTE
13) M. L. Law and W. D. Kelton, Simulation Modeling & Analysis, 2nd ed. New York: McGraw-Hill, 1991.