通信情報保護學會論文誌
第 11 券 第 2 號, 2001. 4

# SES/MB 프레임워크를 이용한 네트워크 보안 모델링 및 시뮬레이션*

지 승 도**, 박 종 서***, 이 장 세**, 김 환 국***, 정 기 찬**, 정 정 례**

# Network Security Modeling and Simulation Using the SES/MB Framework

Sung-do Chi, Jong-sou Park, Jang-se Lee,
Hwan-kuk Kim, Ki-chan Jung, Jeong-rye Jeong

## 요 약

본 논문은 계층 구조적이고 모듈화 된 모델링 및 시뮬레이션 프레임워크를 이용한 네트워크 보안 모델링과 시뮬레이션 기법의 연구를 주목적으로 한다. 최근, Howard와 Amoroso는 사이버 공격, 방어 및 결과에 대한 원인-결과 모델을 개발하였다. 또한, Cohen은 원인-결과 모델을 이용하여 단순한 네트워크 보안 시뮬레이션 방법론을 제안한 바 있으나, 복잡한 네트워크 보안 모델과 모델 기반의 사이버 공격에 대한 시뮬레이션은 불가능한 실정이다. 따라서, 본 논문에서는 인공지능의 기호적 형식론과 시뮬레이션의 동역학적 형식론을 체계적으로 통합한 System Entity Structure/Model Base(SES/MB)을 통하여 계층 구조적이고 모듈화 된 네트워크 보안 모델링 및 시뮬레이션 방법론을 제안하고 사이버 공격 시나리오를 이용한 사례연구를 통하여 타당성을 검증하였다.

## ABSTRACT

This paper presents the network security modeling methodology and simulation using the hierarchical and modular modeling and simulation framework. Recently, Howard and Amoroso developed the cause-effect model of the cyber attack, defense, and consequences. Cohen has been proposed the simplified network security simulation methodology using the cause-effect model, however, it is not clear that it can support more complex network security model and also the model-based cyber attack simulation. To deal with this problem, we have adopted the hierarchical and modular modeling and simulation environment so called the System Entity Structure/Model Base(SES/MB) framework which integrates the dynamic-based formalism of simulation with the symbolic formalism of AI. Several simulation tests performed on sample network system verify the soundness of our method.

**keyword** : *SES/MB, Network Security Modeling, Cyber Attack Simulation*

* 본 연구는 한국정보보호센터 위탁과제(연구2000-001)로 수행하였습니다.
** 한국항공대학교 컴퓨터공학과 지능시스템연구실(sdchi@mail.hangkong.ac.kr, jslee2@mail.hangkong.ac.kr, prayccc@mail.hangkong.ac.kr, harusali@mail.hangkong.ac.kr)
*** 한국항공대학교 컴퓨터공학과 네트워크보안연구실
(jspark@mail.hangkong.ac.kr, rinyfeel@mail.hangkong.ac.kr)

## Ⅰ. 서 론

정보화의 진전에 따라 사회시설 전반이 정보통신 기반 기술을 이용하여 자동화되고, 정보시스템 및 정보통신망에 의존도가 높아지고 있다. 또, 이러한 기반시설들이 국가의 경제 및 안보에 막대한 영향을 미치므로 해킹 및 사이버테러 등 주요 정보기반구조 침해 위협을 방지하기 위하여 주요 정보기반구조를 소유, 운영 및 관리하는 국가, 공공기관 및 산업체의 보호 노력이 절실히 요구된다.[1,2] 복잡한 주요 정보기반구조의 취약 요소 평가, 피해 파급 효과 분석, 보안 대책의 적절성 등의 평가는 필수적이며 이를 위해서는 물리적인 기반구조를 대상으로 직접적인 시험을 시행해야 한다. 그러나, 실제의 기반구조를 대상으로 시험을 시행할 경우 비용, 시간, 피해의 책임문제, 피해 배상 등의 많은 문제를 내포함에 따라 정보보호의 관점에서 시뮬레이션 접근은 정보기반구조에서의 보안 대책 및 취약 요소 분석을 위한 필수 불가결한 요소로 인식되고 있다. 모델링과 시뮬레이션 기법은 시스템 설계 및 분석을 위하여 여러 분야에서 적용되고 있으나, 정보 보호 분야의 경우 사이버 공격과 방어의 복잡성, 방대한 탐색 공간, 공격과 방어에 대한 데이타의 부족 등으로 다른 분야에 비하여 연구가 미흡한 실정이다.[3] 최근에 Cohen[3]은 보안관련 모델링과 시뮬레이션 수행시 모델의 정확성, 데이터의 정확성 및 방대한 시뮬레이션 스페이스 등의 제한이 문제가 된다고 지적하고 노드와 링크만으로 표현되는 네트웍 모델, 원인-결과 모델, 특성함수들(분석가에 의해 준비되는), 의사 난수 발생기만으로 구성되는 단순한 네트웍 모델을 제안하여 주목받은 바 있으나 단순화에 따른 실제 적용의 어려움이 있으며 Amoroso[4]는 침입 탐지 모델에 대한 연구를 통하여 침입 모델의 표현 방법을 제시하였으나 보안 메커니즘 중심의 표현으로 시뮬레이션 분석 및 활용에 대한 연구가 미흡하다. Nong Ye[5]는 사이버 공격 방어를 위한 프로세스 제어 접근에 대한 연구를 통하여 복잡한 사이버 공격 모델을 추상화하고 기능 단계의 모델링을 제안하였으나 이를 적용한 모델링 및 시뮬레이션 기법에 대한 구체적인 제시가 없는 실정이다. 한편, 현존하는 범용의 정보통신기반 시스템 모델링 도구들의 경우 시스템 이론적 모델링 기법보다는 기존의 해석적 기법을 중심으로 모델링 되어져서 복잡 다양화 그리고 대규모화의 경향을 갖는 정보기반구조를 표현하는데는 한계를 갖고 있으며 S/W 공학적 관점에서 계층구조적 모듈화 개념이 취약하여 융통성 있는 시스템 설계 및 분석이 곤란하다.[6,7] 또한, 정보보증의 관점에 있어서 대부분의 도구들이 일반적인 성능분석 중심의 모델링 환경을 제공함으로써 정보보호를 위한 보안관련 모델링의 융통성이 결여된 단점이 있다. 이러한 문제를 해결하기 위하여 본 논문에서는 첫째, SES/MB 프레임워크를 이용하여 복잡한 정보기반구조를 체계적으로 표현하고 둘째, 보안 요소를 고려하여 사이버 공격에 대한 명령어 수준의 모델링을 수행함으로써 사이버 공격에 대한 세밀한 분석이 가능한 네트워크 보안 모델링 및 시뮬레이션 방법론을 제안한다. 본 논문은 다음과 같이 구성된다. 1장의 서론에 이어 2장에서는 SES/MB 프레임워크에 대하여 설명하고 3장에서는 네트워크 보안 모델링 및 시뮬레이션 방법론에 대하여 논한다. 4장에서는 사례연구로서 임의의 가상 네트워크에 대한 사이버 공격 시뮬레이션을 통하여 제안한 방법론의 타당성을 검증한 뒤 5장에서 결론을 맺는다.

## Ⅱ. SES/MB 프레임워크

Zeigler에 의하여 제안된 System Entitly Structure/Model Base(SES/MB)는 시스템의 구조와 동역학적인 표현을 동시에 가능하게 하는 형식론으로 기존의 동역학적 방법론과 AI의 기호적 방법론을 체계적으로 결합시킨 시스템 모델링 및 시뮬레이션 환경을 제공한다.[8,9] SES/MB는 다음의 두 가지로 구성된다: System Entity Structure(SES)와 Model Base(MB).

### 2.1 System Entity Structure (SES)

SES는 시스템의 구조를 나타내는 지식을 특정 형식으로 표현한 것으로서 선언적 특징을 가지며, 분할(decomposition), 분류(component taxonomies), 결합 관계(coupling specification), 제약조건(constraints) 등을 표현할 수 있는 구조체를 말한다. SES는 트리 형태로 계층적인 모델들을 정의하고 트리의 말단 노드는 모델 베이스의 모델로 나타내며 시스템의 구조를 표현하기 위하여 Entity, Aspect, 그리고 Specialization의 3가지 형태의 노드로 구성되어 있다.[10] Entity는 독립적으로 식별될 수 있거나 또는 다른 실세계 객체의 분할된 구

성원으로 간주될 수 있는 실세계 객체에 해당하며 여러 개의 Aspect와 Specialization을 질 수 있다. Aspect는 Entity의 분할적 표현을 담당하는 모드로서 여러 구성 부분들을 나타내며(한 줄의 수직선에 의해 표현), Specialization은 Entity의 분류적 표현을 담당하는 모드로 종류별 관계를 나타낸다(두 줄의 수직선에 의해 표현). 또, Multiple Entity는 동일한 속성을 가진 다수의 Entity들의 집합을 나타내는 것으로, 시스템에서 갯수가 가변적인 여러 개의 Entity를 표현할 때 사용된다(수직선 세 개에 의해 표현). 이러한 관계 표현들을 적절히 이용하면 대상 시스템의 모든 가능한 구조적 지식의 표현이 가능하며, SES로 표현되는 여러 가능한 구조 중에서 하나의 대상이 되는 구조를 선택하기 위해서 pruning이라는 과정을 적용할 수 있다. Pruning은 SES가 나타내는 여러 구조 중 하나의 구조를 선택하는 것으로서, 이 결과로 Pruned Entity Structure(PES)가 생성되며 Pruning의 과정은 더 이상의 *Specialization*이나 *Multiple Entity*가 없이 오직 *Aspect(decomposition)*으로만 구성하는 과정으로서 다음과 같이 진행된다.

① 여러 종류의 *Entity*를 의미하는 *Specialization*에서는 하나의 *Entity*를 선택한다.
② 동일한 속성을 갖는 다수의 *Entity*를 의미하는 *Multiple Entity*에서는 요구된 *Entity*의 갯수를 지정한다.
③ 시스템을 다양한 관점에서 분할하여 다수의 *Aspect*들이 존재할 경우 하나의 *Aspect*만을 택한다.

## 2.2 Model Base(MB)

절차적 특징을 가지는 MB는 시스템의 행위적 특성을 나타내는 것으로서 동역학적이고 기호적인 표현 수단을 제공하는 모델들로 구성된다. MB 환경에서의 이산 사건 모델은 시간베이스, 입력, 상태, 출력 그리고 함수들을 갖으며, 여기서 함수들은 현재 상태와 입력들에 근거하여 다음 상태와 출력들을 결정한다. MB의 각 모델들은 SES상의 leaf entity들로서, 주어진 coupling관계에 의해 상호 결합됨에 의해 전체 시뮬레이션 모델을 구성케 된다. 이산 사건 모델링을 위한 대표적인 형식론인 DEVS(Discrete Event System Specification) 모델은 연속적인 시간상에서 이산적으로 발생하는 사건들에 대하여 시스템의 행위를 측정하는 것으로 다음과 같은 집합에 의해 표현된다.[8,9]

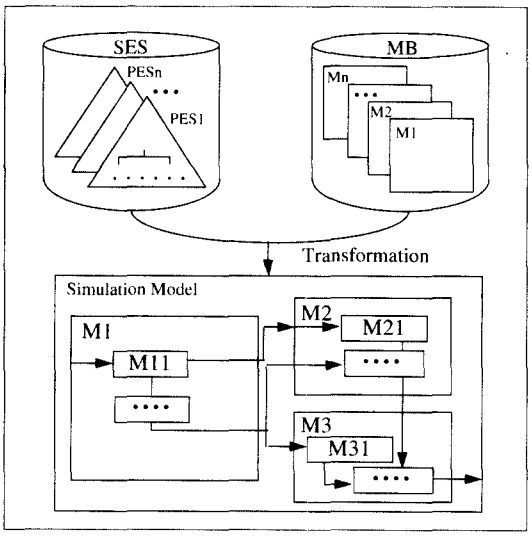
$$M=\langle X, S, Y, \delta_{int}, \delta_{ext}, \lambda, ta\rangle$$

여기에서

X : 입력 집합
S : 상태 집합
Y : 출력 집합
$\delta_{int}$ : $S\rightarrow S$, 내부상태 전이함수
$\delta_{ext}$ : $Q\times X\rightarrow S$, 외부상태 전이함수
$Q=\{(s,e)\mid s\in S, 0\le e\le ta(s)\}$
$\lambda$ : $S\rightarrow Y$, 출력 함수
ta : $S\rightarrow R^{+}_{0,\infty}$, 시간 진행 함수,
단, $R^{+}_{0,\infty}$는 음수를 제외한 실수 집합

입력 집합 X는 시스템 외부에서 발생하는 사건들의 집합을 의미하고, 출력 집합 Y는 출력 변수들의 집합을 나타낸다. 상태 집합 S는 상태 변수들의 각 정의 구역들의 곱집합을 의미하며 상태 s ($\in$S)는 시간 진행에 따른 시스템의 순차적인 snap shot 상태를 의미한다. 사건 진행 함수 ta(s)는 시스템이 외부 사건을 입력받지 않는 한 상태 s에 머물 수 있도록 허용한 시간으로 정의한다. 내부 상태 전이 함수 $\delta_{int}$는 외부의 사건이 없는 경우 시간 진행에 따라 모델의 상태변화를 설명해 주는 함수로 정의하고, 외부 상태 전이 함수 $\delta_{ext}$는 시스템 외부에서 발생한 사건에 의한 모델의 상태변화를 나타내는 함수로 정의한다. 출력 함수 $\lambda$는 상태 s에서 시스템의 출력으로 정의한다.

[그림 1]은 SES/MB 구조를 나타낸 것으로 시스템의 구조 및 결합관계를 가지고 있는 SES에 변환



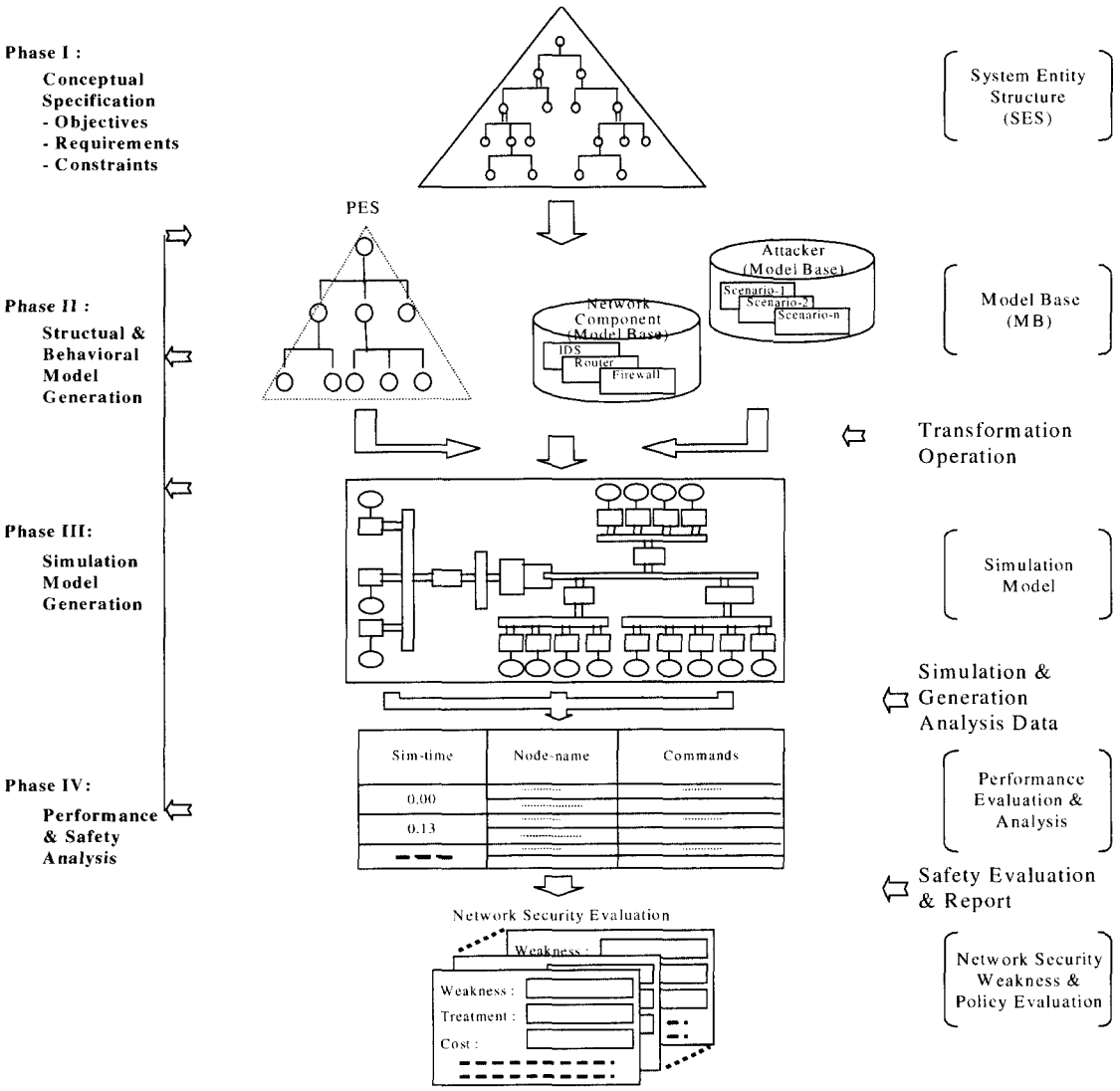

[그림 1] SES/MB 구조

함수(transformation)를 적용함으로써 MB에 저장된 모델들과의 결합을 통하여 계층 구조적 시뮬레이션 모델이 생성되는 것을 보여준다. 이러한 SES/MB는 시스템의 계층적 설계의 용이성을 제공하고 모듈러, 개체지향적 설계에 따른 모델의 재사용성과 구현이 용이해지는 장점이 있다.

## Ⅲ. 네트워크 보안 모델링 및 시뮬레이션 방법론

기존 네트워크 모델링은 지연시간, 대기패킷수, 일처리율, 활동수 등의 성능분석을 목적으로 모델링되는데 반하여 네트워크 보안 모델링은 해킹의 시나리오에 따른 구체적 행동특성의 표현 및 네트워크에 대한 취약성 등의 분석을 목적으로 모델링 되어야 하므로 컴포넌트 모델링 등에 있어서 전혀 다른 관점의 접근이 요구되어 진다. 따라서, 본 장에서는 [그림 2]와 같은 SES/MB 프레임워크를 이용한 네트워크 보안 모델링 및 시뮬레이션 방법론을 제안한다.

먼저, Phase Ⅰ은 개념 명세화 단계로서, 정보기반구조 네트워크의 전반적인 구조를 도식화하는 단계이다. 이 단계에서는 시스템의 구성관계, 구성원의 종류, 구성원들의 결합구조, 그리고 제약조건 등의 구조적 지식의 표현수단을 제공한다. Phase Ⅱ는 이미 라이브러리화 되어 있는 Attacker 모델베이




[그림 2] SES/MB를 이용한 네트워크 보안 모델링 및 시뮬레이션 방법론

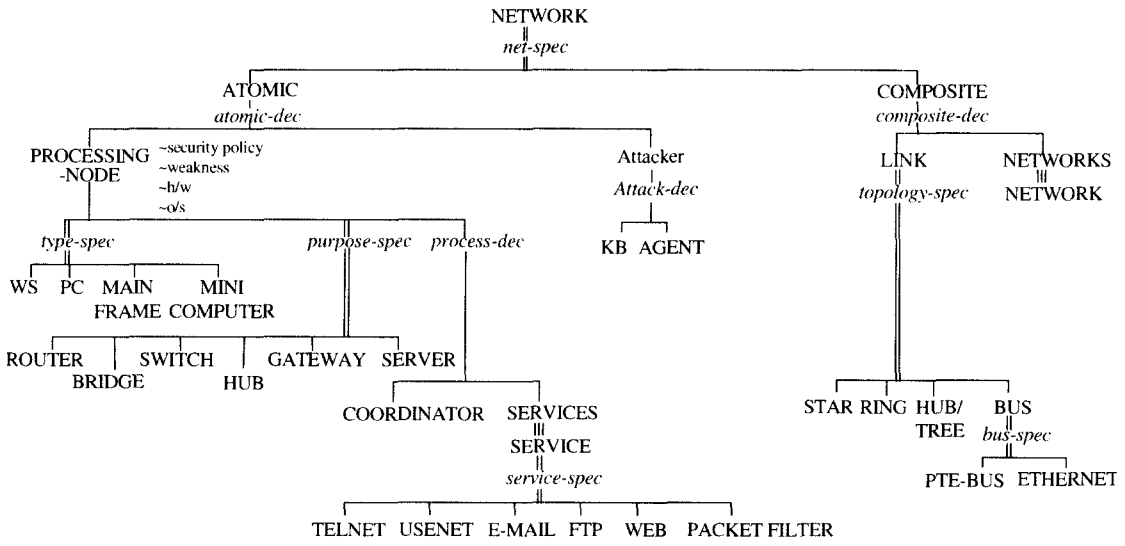
스의 각종 사이버 공격 시나리오 데이터와 컴포넌트 모델들을 Phase Ⅰ의 구조로부터 얻어진 PES 즉, 시뮬레이션 대상 네트워크 구조와 통합시키는 단계로서, 사이버 공격 시나리오 모델, 네트워크 컴포넌트 모델 등을 포함하고 있다. Phase Ⅲ는 이러한 데이터 그리고 구조적 및 동역학 모델들을 통합시킴에 의해 최종적 시뮬레이션 모델을 생성하고 명령어 수준의 사이버 공격 시나리오를 이용한 시뮬레이션을 수행한다. 시뮬레이션의 수행은 사이버 공격 시나리오의 명령어를 패킷 실어 대상 컴포넌트로 전달함으로써 이루어지며, 전달된 명령어는 명령어 선후행 조건에 따라 컴포넌트의 상태, 즉, 속성값, 취약성 값 등을 고려하여 실행된다. 마지막으로 Phase Ⅳ에서는 시뮬레이션 수행 결과로서 얻어진 명령어 수행에 따른 각 구성원에서의 변화된 속성값과 네트워크의 각 링크를 통하여 성공된 공격의 횟수를 제공함으로써 컴포넌트의 취약성과 취약한 경로의 분석을 수행한다. 또한, 보안 대책에 따른 다양한 구성 설정을 모델의 속성값으로 반영하여 시뮬레이션 함으로써 네트워크에 대한 다양한 위협 영향 평가는 물론 현재의 보안 대책의 평가 및 대안을 제시할 수 있다.

### 3.1 네트워크 구조 모델링

네트워크의 전반적인 구조는 시스템의 구성관계, 구성원의 종류, 구성원들의 결합구조, 그리고 제약조건 등의 구조적 지식의 표현수단인 SES를 통하여 모델링 한다.

〔그림 3〕은 네트워크 보안 모델의 SES를 나타낸다. 최상위 entity인 NETWORK은 단일 네트워크로 구성되는 ATOMIC과 다중 네트워크로 구성될 수 있는 COMPOSITE으로 분할된다. ATOMIC은 다시 PROCESSING-NODE와 가상 공격 시나리오를 통해서 공격을 수행하는 Attacker 모델로 분할되는데, PROCESSING-NODE는 COORDINATOR와 다수의 SERVICES로 분할되며 type과 purpose에 따라서 분류될 수 있다. COMPO-SITE은 여러 다중의 네트워크 그룹을 연결할 수 있는 multiple entity인 NETWORKS 노드와 이들을 연결시킬 수 있도록 LINK로 분할된다. 이와 같은 SES를 이용하게 되면 네트워크 보안을 고려한 어떠한 네트워크 망도 구성을 할 수 있다.

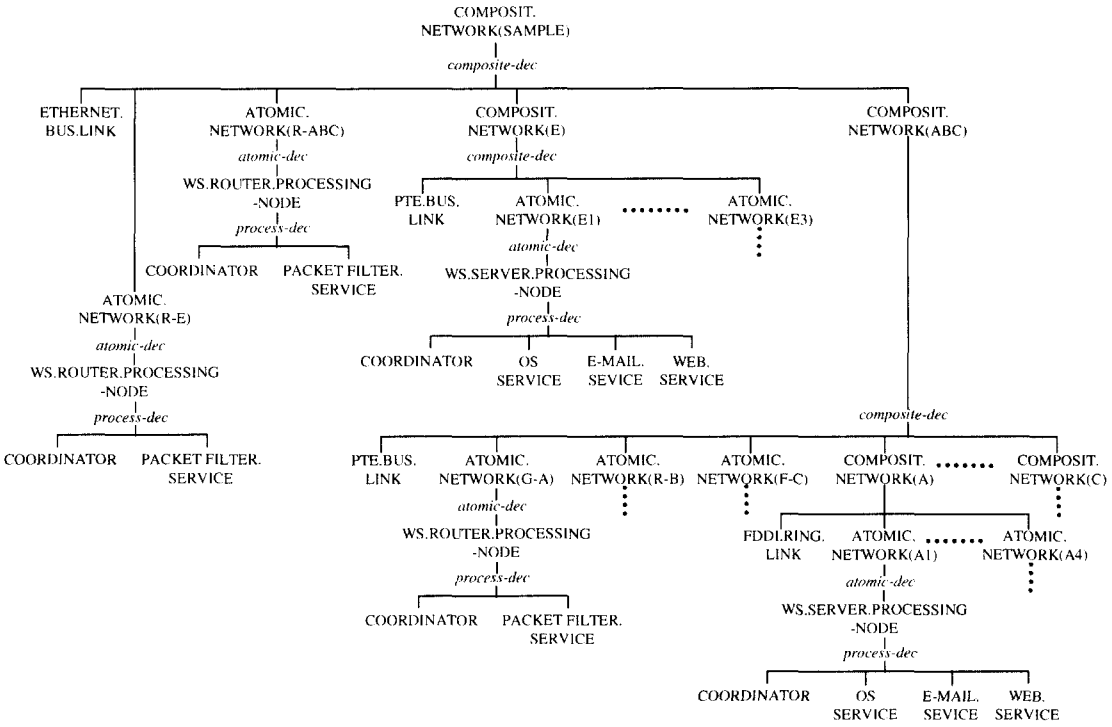
〔그림 4〕는 〔그림 3〕과 같이 구축된 SES에 pruning 과정을 적용하여 얻어진 하나의 네트워크의 구조를 나타낸 것으로 COMPOSIT.NETWORK(SAMPLE)은 ETHERNET.BUS.LINK, 두 개의 ATOMIC.NETWORK와 두 개의 COMPOSIT.NETWORK으로 분할된다. 또, 두 개의 ATOMIC.NETWORK은 COORDINATOR와 PACKET FILTER.SERVICE로 구성되어 라우터 역할을 하는 WS.ROUTER. PROCESSING-NOD E로 이루어지며 첫 번째의 COMPOSIT. NETWORK은 PTE.BUS.LINK와 3개의 ATOMIC. NETWORK로 분할되며 각각은 다시 OS. SERVICE, E-MAIL.SERVICE



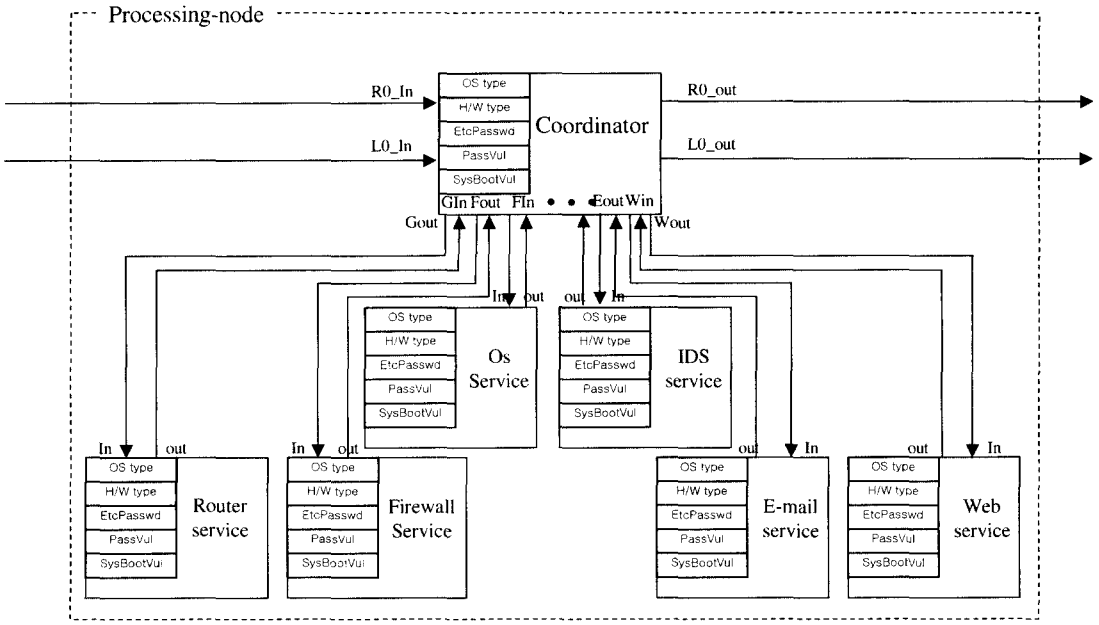

〔그림 3〕 네트워크 보안 모델의 SES

및 WEB.SER-VICE로 분할되어 telnet, e-mail 과 web 서비스가 가능한 워크스테이션 서버인 WS. SERVER. PROCESSING-NODE로 구성된다.

두 번째 COMPOSIT.NETWORK은 PTE.BUS. LINK, 3개의 ATOMIC.NETWORK과 3개의 COMPOSIT.NETWORK으로 분할된다. ATOMIC. NET-




〔그림 4〕 네트워크 보안 모델의 PES




〔그림 5〕 네트워크 구성원 구조(프로세스 노드)

WORK들은 각각 라우터, 게이트웨이, 방화벽 역할을 하는 노드로 구성되며 COMPOSIT.NETWORK들은 링 또는 버스로 연결된 구조의 내부 망을 구성한다. 이러한 방법으로 생성된 대상 시뮬레이션 구조상에 존재하는 각 단말 노드마다 동역학 모델이 합성됨에 의해 최종적 시뮬레이션 모델이 구축된다.

### 3.2 네트워크 구성원 모델링

네트워크 상에 존재하는 다양한 네트워크 구성원을 프로세스 노드의 동일한 형태로 표현하고 구성원들의 다양한 기능을 서비스 모델로서 모델링 한다.

〔그림 5〕는 네트워크 구성원을 프로세스 노드의 형태로 나타낸 것이다. 프로세스 노드는 여러 가지 서비스들을 공통된 형태의 모델로 표현함으로써 다양한 모델들에 대한 동일한 형태를 제공한다. 모든 네트워크 구성원들은 모두 동일한 프로세스 노드의 형태를 가지게 되며 프로세스 노드 안에 포함된 서비스만 차이를 가지게 되기 때문에 프로세스 노드가 제공하는 서비스의 추가, 삭제만으로 다양한 네트워크 구성원을 표현할 수 있다는 장점을 가질 수 있다. 또, 프로세스 노드는 노드마다 O/S type, H/W type, Address, Account list, 시스템 파일, 구성원의 취약성 같은 여러 상태 변수를 가지며 각각의 변수는 서비스를 수행하면서 변경됨으로써 구성원의 상태를 나타내게 된다.

### 3.3 명령어 모델링

사이버 공격 시나리오에 대한 네트워크 구성원들에 명령어 수준에서의 분석을 위하여 각 서비스에 대한 명령어를 그룹화하고 특성화한다.

〔표 1〕은 OS 서비스 명령어를 선행조건과 결과, 후행조건으로 분류한 선후행조건 모델링의 예이다.

〔표 1〕에서 1) 선행조건은 명령어가 실행되기 위한 조건에 대한 내용, 2) 결과는 명령어의 처리로 나오는 결과 내용, 3) 후행조건은 명령어를 수행한 후에 그 명령어로 인해서 변경되는 노드나 서비스의 속성에 대한 내용을 나타낸다. 예를 들어서 rmdir 명령어를 사용하려면 선행조건으로 삭제하려는 디렉토리가 있는지 확인하여야 하고 그 결과로 디렉토리 제거라는 결과가 반환이 되며, 후행조건으로 디렉토리의 속성을 변경하게 된다. 노드에서 필요한 명령어를 〔표 1〕과 같은 형태로 분류, 모델링 함으로써 사이버 공격 시나리오에 대한 시뮬레이션에 있어서

〔표 1〕 OS 서비스 명령어의 선후행조건 모델링의 예

| 명령어 | 선행조건 | 결과 | 후행조건 |
|---|---|---|---|
| more | | 파일들의 리스트 출력 | |
| pwd | 작업 디렉토리 확인 | 현재의 작업 디렉토리 출력 | |
| rmdir | 디렉토리 확인 | 디렉토리 제거 | 디렉토리 속성 변경 |
| cd | 디렉토리 존재 여부 확인 | 디렉토리 이동, 변경 | 디렉토리 속성 변경 |
| vi | 파일 존재 여부 확인 | 파일 편집 | 파일관련 속성 변경 |
| mv | 파일 존재 여부 확인 | 파일 이름 바꾸기 | 파일관련 속성 변경 |
| rm | 파일 존재 여부 확인 | 파일 삭제 | 파일관련 속성 변경 |
| chmod | 파일 존재 확인 | 파일의 허가권 변경 | 파일 소유 변경 |

정형화된 방법을 제공할 수 있는 장점을 가진다.

### 3.4 취약점 모델링

구성원은 자신이 가지는 취약성 항목이 존재하게 된다. 구성원의 취약성은 크게 두 가지로 나눌 수 있으며, 첫째, 시스템이 소프트웨어의 버그로 인한 취약성, 둘째, 관리자의 잘못된 시스템 설정으로 인한 취약성이 존재하게 된다.

〔표 2〕는 네트워크 구성원이 가지는 시스템 설정상의 잘못으로 인해서 발생하는 취약성 모델링의 예를나타낸 것으로서 취약성 항목에 대해서 3단계로 설정을 하고 그 단계에 대한 조건을 명시한 것이며 각 단계의 조건은 보안 정책 등에 따라서 변경되어질 수 있다. 예를 들어서 패스워크 취약성 항목의 경우 "안전" 단계는 패스워드와 아이디가 같은 사용자가 하나도 없는 상태, "주의" 단계는 패스워드와 아이디가 같은 사용자가 5명 이내로 존재하는 상태, "취약" 단계는 그 시스템에 대하여 패스워드와 아이디가 같은 사용자가 5명 이상으로 존재하는 상태를 각각 나타낸다. 이 취약성 항목은 구성원의 취약성을 나타내며, 시뮬레이션 수행시 취약성 항목의 값에 따라서 명령어의 처리가 이루어진다. 이와 같이 취약성과 명령어의 연관을 통하여 네트워크 구성원 모델에 보안 요소를 고려할 수 있다.

〔표 3〕은 기존의 모델링 방법들과 제안된 방법을 비교한 것으로서 제안된 방법론은 복잡한 네트워크

〔표 2〕 네트워크 구성원의 취약성 모델링의 예

| 취약점 항목 | 필요한 상태 변수 | 단계 | 조건 |
|---|---|---|---|
| 패스워드 | 아이디와 비밀번호가 같은 인원수 | 안전 | 없음 |
| | | 주의 | 5명 이내 존재 |
| | | 취약 | 5명 이상 존재 |
| 시스템 부팅 패스워드 | 시스템 부팅 패스워드 변수 | 안전 | 등록됨 |
| | | 주의 | |
| | | 취약 | 등록 안됨 |
| 패스워드 파일 | /etc/passwd 파일의 권한 소유자 인원수 | 안전 | root만 권한 |
| | | 주의 | root외 권한 3명 이하 |
| | | 취약 | root외 권한 3명 이상 |
| 사용자 파일 | .login, .profile, .cshrc, rhosts 등의 파일에 대한 접근자 인원수 | 안전 | 모든 사용자 접근 안됨 |
| | | 주의 | root외 권한 3명 이하 |
| | | 취약 | root외 권한 3명 이상 |
| 시스템 관리자 권한 도용 | setuid 파일의 소유 권한자 인원수 | 안전 | root 만 소유 |
| | | 주의 | root외 권한 2명 이하 |
| | | 취약 | root외에 권한 2명 이상 |
| 원격접속 및 명령어 | 제공되는 원격접속 명령어 갯수 | 안전 | 제공안됨 |
| | | 주의 | 일부 제공(1개 이하) |
| | | 취약 | 원격접속 명령어 5개 이상 |
| 파일 시스템 | 현재 마운트 되어 있는 파일 시스템의 소유자 인원수 | 안전 | root만 권한 |
| | | 주의 | root외 권한 3명 이하 |
| | | 취약 | root외 권한 3명 이상 |

〔표 3〕 기존 방법들과 제안된 방법 비교

| 방법 / 항목 | Amoroso | Cohen | Nong-Ye | 제안된 방법 |
|---|---|---|---|---|
| 계층구조적 모듈화 | 비적용 | 비적용 | 비적용 | **적용** |
| 모델 정밀도 | 낮음 | 낮음 | 높음 | **높음** |
| 적용대상 | 기존에 알려진 해킹을 다룸 | 기존에 알려진 해킹을 다룸 | 기존에 알려진 해킹을 다룸 | **기존에 알려진 해킹 및 향후 발생 가능한 해킹까지 다룸** |
| 시뮬레이션 수행 여부 | 시뮬레이션 접근에 대한 연구 미흡 | 단순한 시뮬레이션 수행 | 시뮬레이션 기법에 대한 제시 없음 | **다양한 시뮬레이션 수행 가능** |
| 특징 | 침입 탐지를 위한 침입 모델 | 원인-결과 모델을 이용한 단순한 네트워크 모델링 및 시뮬레이션 | 사이버 공격 방어를 위한 기능 단계의 모델 | **SES/MB 프레임워크를 이용한 다양한 모델링 및 시뮬레이션 환경 제공** |

표현 및 모델링을 위하여 계층구조적 모듈화 기법이 적용되었으며 명령어 레벨의 모델링을 통하여 해킹의 시나리오에 따른 구체적 행동 특성을 다룰 수 있다. 또한 다양한 모델링 및 시뮬레이션을 통하여 향후 발생 가능한 해킹 및 네트워크 취약성 분석이 가능하다.

## Ⅳ. 사례 연구

본 장에서는 임의의 가상 네트워크에 대한 사이버 공격 시나리오를 시뮬레이션 함으로써 제안한 방법론의 타당성을 검토하였다.

### 4.1 네트워크의 구조

[그림 6]은 시뮬레이션을 수행할 네트워크 예를 나타낸다. 가상 네트워크의 구성은 여러 대의 컴퓨터와 서버로 이루어진 LAN, 그리고 Ring, bus같은 형태로 컴퓨터가 연결이 되어 있는 topology, 여러 개의 LAN으로 이루어진 WAN이 인터넷을 사이에 두고 Router를 통해서 연결되며, 각 노드는 다양한 운영체제로 구성이 되어 있다. 본 연구에서는 간단하게 4가지의 운영체제에 대해서 구성을 하였다. 그림의 왼쪽 하단에 있는 Attacker는 가상 공격 시나리오에 따라서 공격을 하게 된다.

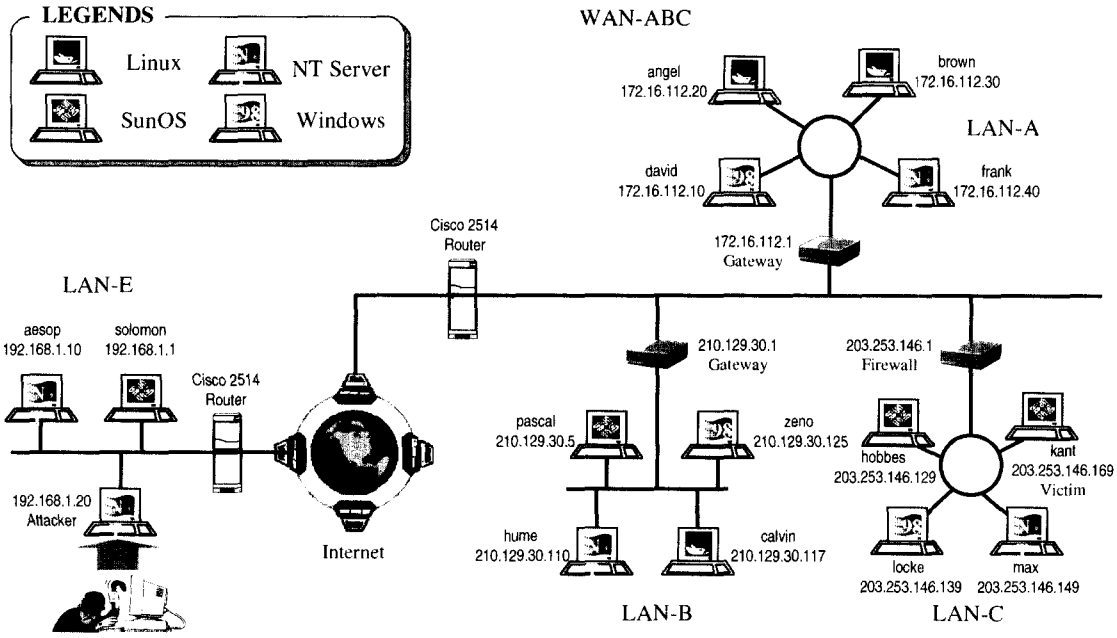
[그림 7]은 [그림 6]의 가상 네트워크망을 모델 구조도로 나타낸 것이다. 컴퓨터나 서버, 라우터나 게이트웨이는 앞에서 제안한 하나의 프로세스 노드(정사각형)로 표현이 될 수 있다. 그리고 노드와 노드 사이를 연결하는 링크(직사각형)인 토폴로지 모델이 있다. 노드마다 Attacker가 연결이 되어서 어떤 노드든지 가상 공격 패킷을 생성할 수 있으며 노드에 연결이 되어 있는 Attacker에서 패킷을 생성하게 되면 그 패킷은 노드 모델, 토폴로지 모델, Router 모델등을 통하여 목표 노드 모델로 이동하게 된다. 패킷을 받은 노드 모델은 그 패킷이 원하는 명령어에 대한 처리를 하고 다시 같은 방법으로 응답을 하게 된다. Analyzer 모델은 각 노드 모델에 연결이 되어 있는 모델로 연결되어 있는 모델에서 발생한 명령어의 처리 횟수와 실패한 명령어의 처리 횟수, 성공한 시나리오의 횟수, 성공한 링크의 경로 등 사이버 공격 시나리오를 통해서 발생하는 분석 자료들을 통합, 관리하는 모델이다.

### 4.2 시뮬레이션 테스트

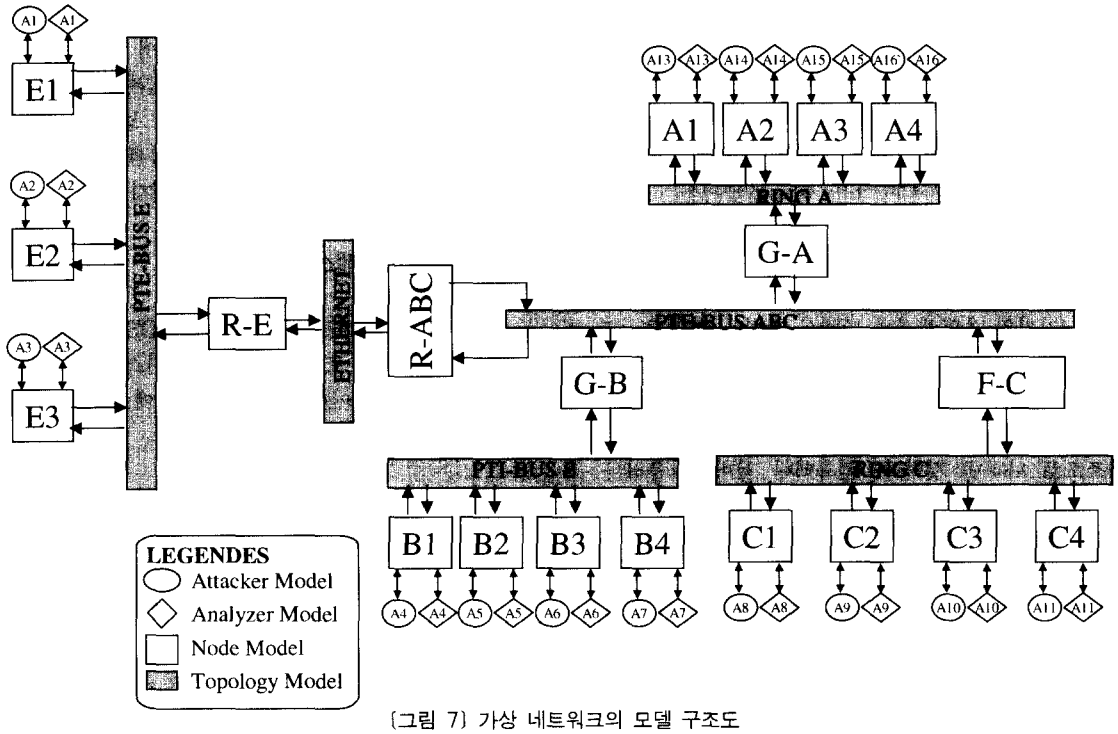
시뮬레이션 테스트를 위하여 MODSIM Ⅲ를 이용하여 네트워크 보안 시뮬레이션 시스템을 구현하였으며 다음의 사이버 공격 시나리오에 대하여 명령어 수준의 시뮬레이션을 수행하였다.

*시나리오 : "SYN flooding, IP spoofing과 SUN에서 오래된 버그를 통해 user account가 없는 시스템에 일반 계정을 획득하여 시스템에 액세스하기*[11,12,13,14,15]"

[표 4]는 SYN flooding과 IP spoofing을 통하여 자신의 IP를 속이고 대상 컴퓨터에 접속하여 시스템의 버그를 이용하여 일반 계정을 획득하는 일련의 사이버 공격 시나리오에 대한 시뮬레이션의 결과를 나타낸다. 여기서 Time은 시뮬레이션 시간을




[그림 6] 시뮬레이션 네트워크 예

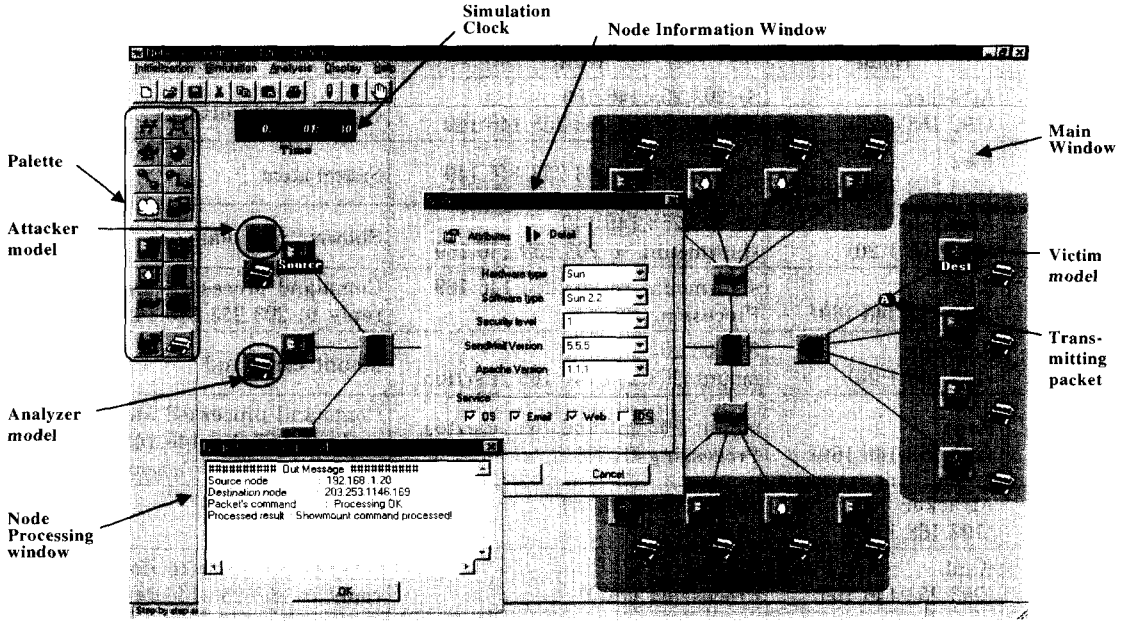



〔그림 7〕 가상 네트워크의 모델 구조도

의미하며 Node는 시뮬레이션 결과를 보여주는 노드의 이름과 IP address를 나타낸다. What은 노드에서 발생된 명령어 또는 노드에 입력된 명령어와 처리 결과를 나타내며 remarks는 What에 대한 설명을 나타낸다. 사이버 공격 시나리오에 대한 시뮬레이션 과정을 간략히 살펴보면, 먼저 사이버 공격 시나리오에 따른 명령어 하나하나는 공격자 모델로부터 시작하여 패킷에 실려 Link, Router, Gateway model 등을 거쳐 목적 노드로 전달된다. 목적 노드는 명령어의 실행 결과를 다시 패킷에 실어 공격자 모델로 응답함으로써 하나의 명령어 수행이 완료된다. 〔표 4〕에서 Attacker는 Max에게 SYN flooding 공격을 수행하고 SYN flooding 공격에 의하여 Max는 시스템이 다운된다. 이어서, Attacker는 source address를 Max의 IP로 위장하고 Kant에게 'showmount -e 203.253.146.169' 명령어를 패킷에 실어 보낸다. Kant의 시스템 버그로 인하여 입력된 명령어는 실행되고 Kant는 수행결과를 Attacker의 위장된 주소인 Max에게 보낸다. 계속적으로 Attacker는 자신의 주소를 위장하여 'mount 203.253.146.169:/usr/foo', 'echo prayccc:1230:10001:1::: >> passwd', 'echo 192.168.1.20 >>.rhosts' 등의 명령어를 순차적으로 수행하여 자신의 계정을 만듦으로써 일반 계정을 획득하게 된다. 마지막으로 attacker는 자신의 주소로 Kant에게 'rlogin 203.253.146.169' 명령어를 수행함으로써 공격이 성공하게 된다. 이와 같이, 제안된 방법론에 의한 사이버 공격 시나리오에 대한 시뮬레이션 결과는 단순한 형태로 표현되는 Cohen의 결과와는 달리 사이버 공격을 구성하는 일련의 명령어에 대한 생성과 처리 결과를 볼 수 있기 때문에 (i) 사이버 공격에 의한 시스템의 변화와 명령어의 결과를 상세히 알 수가 있고 (ii) 노드에 내포된 취약점의 변화를 분석할 수 있다는 장점이 있다. 〔그림 8〕은 MODSIM Ⅲ로 구현된 네트워크 보안 시뮬레이션 시스템을 나타낸다. 사용자는 Node Information Window를 이용하여 노드 상태 및 보안 정책등을 고려한 속성값을 설정할 수 있으며 Attacker 및 Analyzer model을 원하는 임의의 노드에 설정하여 다양한 시나리오에 대한 시뮬레이션 및 분석을 수행할 수 있다. 시뮬레이션 진행과정은 패킷 단위의 애니메이션을 통하여 확인할 수 있으며, Node Processing Window를 통하여 보다 상세한 상황을 확인할 수 있다. 시뮬레이션 결과는 각 노드의 취약성 값의 변화, Analyzer model에서 분석된 각 노드별 총 공격횟수, 이들 중 성공한 공격 횟수, 그리고 이를 통한 링크의 취약성 값 등으로 표현된다.

〔표 4〕 시뮬레이션 결과

| Time | Node | What | Remarks |
|---|---|---|---|
| 0 : 0 | Attacker<br>(192.168.1.20) | S) 203.253.146.169<br>SYN flooding 203.253.146.149 | SYN flooding attack |
| 0 : 2 | Max<br>(203.253.146.149) | SYN flooding 203.253.146.149 | *System down* |
| 0 : 9 | Attacker<br>(192.168.1.20) | S) 203.253.146.149<br>showmount -e 203.253.146.169 | Showmount command |
| 0 : 11 | Kant<br>(203.253.146.169) | showmount -e 203.253.146.169<br>Processing OK!!! | Command processed and<br>reply to 203.253.146.149 |
| 0 : 16 | Attacker<br>(192.168.1.20) | S) 203.253.146.149<br>mount 203.253.146.169:/usr/foo | Mount command |
| 0 : 18 | Kant<br>(203.253.146.169) | mount 203.253.146.169:/usr/foo<br>Processing OK!!! | Command processed and<br>reply to 203.253.146.149<br>- *Increased Mount Vulnerability* |
| 0 : 23 | Attacker<br>(192.168.1.20) | S) 203.253.146.149<br>cd /foo | Cd command |
| 0 : 25 | Kant<br>(203.253.146.169) | cd /foo<br>Processing OK!!! | Change directory to /foo and<br>reply to 203.253.146.149 |
| 0 : 30 | Attacker<br>(192.168.1.20) | S) 203.253.146.149<br>ls -alg | Ls command |
| 0 : 32 | Kant<br>(203.253.146.169) | ls -alg<br>Processing OK!!! | List up ==〉 -alg<br>Reply to 203.253.146.149 |
| 0 : 37 | Attacker<br>(192.168.1.20) | S) 203.253.146.149<br>echo prayccc:1230:10001:1::: 〉〉<br>passwd | Echo command |
| 0 : 39 | Kant<br>(203.253.146.169) | echo prayccc:1230:10001:1::: 〉〉<br>passwd<br>Processing OK!!! | Increased user number<br>Reply to 203.253.146.149 |
| 0 : 44 | Attacker<br>(192.168.1.20) | S) 203.253.146.149<br>ls -alg | Ls command |
| 0 : 46 | Kant<br>(203.253.146.169) | ls -alg<br>Processing OK!!! | List up ==〉 -alg<br>Reply to 203.253.146.149 |
| 0 : 51 | Attacker<br>(192.168.1.20) | S) 203.253.146.149<br>su prayccc | Su command |
| 0 : 53 | Kant<br>(203.253.146.169) | su prayccc Processing OK!!! | Changed user ID to prayccc and<br>reply to 203.253.146.149 |
| 0 : 58 | Attacker<br>(192.168.1.20) | S) 203.253.146.149<br>echo 192.168.1.20 〉〉 .rhosts | Echo command |
| 1 : 00 | Kant<br>(203.253.146.169) | echo 192.168.1.20〉〉 .rhosts<br>Processing OK!!! | Increased rhost number<br>Reply to 203.253.146.149 |
| 1 : 5 | Attacker<br>(192.168.1.20) | S) 192.168.1.20<br>rlogin 203.253.146.169 | Rhost command |
| 1 : 7 | Kant<br>(203.253.146.169) | rlogin 203.253.146.169<br>Processing OK!!! | Command processed and<br>reply to 192.168.1.20 |
| 1 : 12 | Attacker<br>(192.168.1.20) | S) 192.168.1.20<br>Bye | Finished |
| 1 : 14 | Kant<br>(203.253.146.169) | Attack Succeeded!!! | *Attack succeeded* and<br>reply to 192.168.1.20 |




〔그림 8〕 구현된 시뮬레이션 시스템

## V. 결 론

본 논문은 계층 구조적이고 모듈화 된 모델링 및 시뮬레이션 프레임워크를 이용한 네트워크 보안 모델링과 시뮬레이션 기법의 연구를 주목적으로 하였다. 최근 급증하고 있는 해킹 사고 등에 대처하기 위하여 정보기반구조의 취약 요소 파악 및 피해 파급 효과 등의 분석이 요구되며, 이를 위하여 물리적인 기반구조에 대한 직접적인 시험의 시행이 요구된다. 그러나 실제의 기반구조에 대한 시험은 많은 문제를 내포함에 따라 시뮬레이션 접근은 필수 불가결한 요소로 인식되고 있다. 이에 반하여 정보보호 분야에 있어서 사이버 공격과 방어의 복잡성, 방대한 탐색 공간, 공격과 방어에 대한 데이타의 부족 등으로 모델링 및 시뮬레이션에 대한 연구가 미흡한 실정이다. 또, 현존하는 범용의 정보통신기반 시스템 모델링 도구들의 경우 시스템 이론적 모델링 기법보다는 기존의 해석적 기법을 중심으로 모델링 되어져서 복잡 다양화 그 리고 대규모화의 경향을 갖는 정보기반구조를 표현하 는데는 한계를 갖고 있으며, 정보보증의 관점에 있어서 대부분의 도구들이 일반적인 성능분석 중심의 모델링 환경을 제공함으로써 정보보호를 위한 보안관련 모델링의 융통성이 결여된 단점이 있다. 이를 극복하기 위하여 본 논문에서는 첫째, SES/MB 프레임워크를 이용하여 복잡한 정보기반구조를 체계적으로 표현하고 둘째, 보안 요소를 고려하여 명령어 수준의 모델링을 수행함으로써 사이버 공격에 의한 구성원의 자세한 행위를 분석할 수 있는 네트워크 보안 모델링 및 시뮬레이션 방법론을 제안하였고, 가상 네트워크에 대한 사례연구를 통하여 타당성을 검증하였다. 본 논문에서 제안된 모델링 및 시뮬레이션 기법은 정보기반구조의 취약 요소 분석과 피해 파급효과 예측뿐만 아니라 보안 대책 수립 및 효용성 분석 등에 적용될 수 있을 것으로 기대되며 향후 연구로는 네트워크 구성원의 모델베이스에 대한 구체화와 더불어 취약성이나 해킹의 상태를 정량화 할 수 있는 방안에 대한 연구가 이루어져야 한다.

## 참 고 문 헌

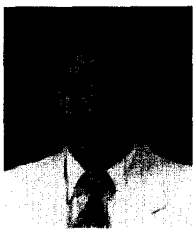
〔1〕 http://www.kisa.or.kr/K_trend/KisaNews/199904/4_7.htm, "정보통신기반구조보호동향", 이철원, *한국정보보호센터*, 4, 1999.

〔2〕 이철원, 김홍근, "정보보증:컴퓨터보안의 새로운 패러다임", *정보과학회지*, 제18권 제1호, pp. 53~61, 1월, 2000.

〔3〕 Fred Cohen, "Simulating Cyber Attacks Defenses, and Consequences", *1999 IEEE Symposium on Security and Privacy Special*

*20th Anniversary Program*, The Claremont Resort Berkeley, California, May 9-12, 1999.
[4] Edward Amoroso, *Intrusion Detection*, AT&T Laboratory, Intrusion Net Books, January, 1999.
[5] Nong Ye, Joseph Giordano, *CACS - A Process Control Approach to Cyber Attack Detection*, Communications of the ACM.
[6] 지승도, 이종근, 이장세, "캠퍼스 네트워크의 구성 및 성능분석 자동화 방법론", *한국시뮬레이션학회 논문지*, 제7권 제2호, 12, 1998.
[7] Kurose, J.F. and H.T. Mouftah, "Computer-Aided Modeling, Analysis, and Design of Communication Networks", *IEEE Jour. on Selected Areas in Communications*, Vol. 6, No. 1, pp. 130~145., 1988.
[8] Zeigler, B.P. *Object-oriented Simulation with Hierarchical, Modular Models: Intelligent Agents and Endomorphic systems*, Academic Press, 1990.
[9] Zeigler, B.P. *Multifacetted Modeling and Discrete Event Simulation*, Academic Press, 1984.
[10] Chi, S.D. *Modeling and Simulation for High Autonomy Systems*, Ph.D. Dissertation, Dept. of Electrical and Computer Engineering, Univ. of Arizona, 1991.
[11] Anonymous, *리눅스 보안의 모든 것*, 인포북, 2000.
[12] Welsh, Kaufman, *Running LINUX*, O-reilly, 1999.
[13] 김효원, *쉽고 빠른 레드햇 리눅스 6.1*, 컴앤북스, 1999.
[14] 다이구지 이사오, *통신 네트워크 시큐리티*, 도서출판 동서, 1998.
[15] 권인택, *해커를 위한 파워 핸드북*, 1999.

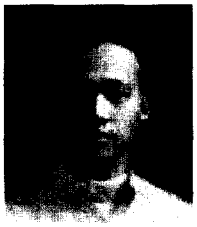
## 〈著者紹介〉



**지 승 도 (Sung-do Chi)**
1982년 2월 : 연세대학교 전기공학과 졸업(공학사)
1984년 2월 : 연세대학교 전기공학과 석사
1985년~1986년 : 두산 컴퓨터(현 한국 디지털)근무
1991년 : 미국 아리조나대학교 전기전산공학과 박사
1991년~1992년 : 미국 SIMEX Systems and S/W 회사 S/W담당자로 근무
1992년~현재 : 한국항공대학교 컴퓨터공학과 부교수
〈관심분야〉 이산사건 시스템 모델링 및 시뮬레이션, 컴퓨터 보안, 지능시스템 디자인 방법론, 시뮬레이션 기반 인공생명, 교통모델링.

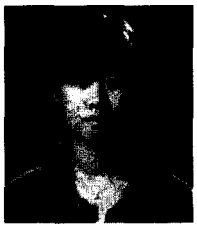
**박 종 서 (Jong-sou Park) 정회원**
1983년 2월 : 한국항공대학교 통신공학과 졸업
1987년 12월 : North Carolina State University 컴퓨터공학과 석사
1994년 8월 : Penn State University 컴퓨터공학과 박사
1996년 2월 : Penn State University 컴퓨터공학과 조교수
1996년 3월~현재 : 한국항공대학교 컴퓨터공학과 조교수
〈관심분야〉 Network Security, VLSI, 항공우주용 제어기설계

**이 장 세 (Jang-se Lee)**
1997년 2월 : 한국항공대학교 전자계산학과 졸업
1999년 2월 : 한국항공대학교 컴퓨터공학 석사
1999년 3월~현재 : 한국항공대학교 컴퓨터공학과 박사과정
〈관심분야〉 모델링 및 시뮬레이션, 네트워크 보안, 지능시스템 설계.



**김 환 국 (Hwan-kuk Kim) 학생회원**
1998년 2월 : 한국항공대학교 전자계산학과 졸업
2000년 8월 : 한국항공대학교 컴퓨터공학과 석사
2000년 8월~현재 : 이레스페이스 연구원
〈관심분야〉 네트워크 보안 모델링, 전자서명 인증, 암호IC 설계.

**정 기 찬 (Ki-chan Jung)**
1999년 2월 : 한국항공대학교 컴퓨터공학과 졸업
2001년 2월 : 한국항공대학교 컴퓨터공학과 석사
2001년 3월~현재 : SimTech 연구원
〈관심분야〉 모델링 및 시뮬레이션, 네트워크 보안



**정 정 례 (Jeong-rye Jeong)**
2001년 2월 : 한국항공대학교 컴퓨터공학과 졸업
〈관심분야〉 모델링 및 시뮬레이션, 네트워크 보안