침입탐지시스템에서 경보정보에 대한 대응 능력 모델링 및 성능분석

전 용 희[†] · 장 정 숙[††] · 장 종 수[†††]

요 약

본 논문에서는 악성 코드, 인터넷 웜과 같은 비정상 트래픽의 생성을 탐지하고 대응하는 침입탐지시스템 구조를 제안한다. 제안된 시스템의 경보정보 대응능력 성능분석을 위하여 시스템 모델링을 수행하고, OPNET을 이용하여 시뮬레이터를 설계하고 구현한다. 먼저 비정상적인 트래픽으로부터 초래되는 경보정보의 도착 프로세스를 모델링 한다. 경보정보가 집중적으로 발생하는 상황을 모델링하기 위하여 트래픽의 burstiness(군집성)를 잘 나타낼 수 있는 IBP(Interrupted Bernoulli Process)를 적용한다. 다음에 성능파라미터에 대한 시스템의 정량적인 이해를 위하여 모의실험을 수행한다. 성능분석 결과를 바탕으로 보안노드의 고속화를 저해하는 요인을 분석하고 성능을 향상시키기 위한 방안을 도출 하고자 한다.

키워드 : 침입탐지시스템, 성능평가, 시뮬레이션, 경보 정보

Modeling and Performance Analysis on the Response Capacity against Alert Information in an Intrusion Detection System

Jeon Yong-Hee[†] · Jang Jung-Sook[††] · Jang Jong-Soo[†††]

ABSTRACT

In this paper, we propose an intrusion detection system(IDS) architecture which can detect and respond against the generation of abnormal traffic such as malicious code and Internet worms. We model the system, design and implement a simulator using OPNET Modeller, for the performance analysis on the response capacity of alert information in the proposed system. At first, we model the arrival process of alert information resulted from abnormal traffic. In order to model the situation in which alert information is intensively produced, we apply the IBP(Interrupted Bernoulli Process) which may represent well the burstiness of traffic. Then we perform the simulation in order to gain some quantitative understanding of the system for our performance parameters. Based on the results of the performance analysis, we analyze factors which may hinder in accelerating the speed of security node, and would like to present some methods to enhance performance.

Key Words : IDS, Performance Evaluation, Simulation, Alert Information

1. 서 론

인터넷의 폭발적인 사용 증가로 인하여 개인정보의 불법적인 접근과 네트워크를 통한 공격에서 고속으로 탐지하고 대응하는 보안기술의 중요성이 높아지고 있다. 보안 기술의 시장 동향은 국내외를 비롯하여 그 시장규모가 확대되고 있다. 네트워크를 통한 공격의 방법도 지능화되어 인터넷 웜과 같이 비정상적으로 네트워크에 침입을 시도하여 정상적인 컴퓨터의 작동을 방해하고 네트워크의 트래픽의 양을 증가시켜 네트워크 전체를 마비시키는 사례가 발생되고 있다. 따라서 기가비트 이더넷 환경 같은 고속화와 대용량화로 네트워크 환경이 현실화 되고 있으며 정확한 탐지 나아가 예방까지 그리고 높은 성능을 기반으로 침입탐지 가능한 보안 분석기법들이 개발되고 있다[1, 2].

기가급 침입탐지시스템 개발을 위한 구조와 시스템 성능을 예측하기위하여 시스템 성능분석에 대한 연구가 중요하다. 시스템의 성능은 칩 상에 구현된 하드웨어 특성과 운영 소프트웨어에 의존한다. 침입탐지 노드의 시스템 성능분석으로 시스템의 병목 현상을 규명할 수 있고 이를 통하여 패킷 처리 과정의 문제점을 발견할 수 있으며 구조 개선이 가능하다. 아울러 효율적인 패킷 처리 알고리즘의 발견을 통한 침입탐지 성능의 개선이 가능하다.

† 종신회원 : 대구가톨릭대학교 컴퓨터정보통신공학부 교수
†† 준 회 원 : 대구가톨릭대학교 컴퓨터정보통신공학부 IT교수
††† 정 회 원 : 한국전자통신연구원 정보보호연구단
논문접수 : 2005년 3월 28일, 심사완료 : 2005년 8월 24일

본 논문에서는 인터넷 웜과 같은 비정상적이고 군집적인 트래픽을 탐지하고 대응하는 침입탐지시스템에 관하여 분석을 수행하고 모의실험을 수행하고자 한다. 먼저 고속 네트워크 환경에서 침입탐지 및 대응을 제공하기위한 기가비트 침입탐지시스템인 보안 노드를 제안하고 분석한다. 다음에 비정상적인 트래픽의 경보발생에 관하여 경보도착프로세스를 모델링한다. 경보 도착프로세스에서는 군집성의 영향을 분석하기위하여 IPP(Interrupted Poisson Process)의 이산모델인 IBP (Interrupted Bernoulli Process)를 적용하여 모델링한다[3]. 개발 중인 시스템 경보정보의 대응능력 성능분석을 위하여 OPNET을 이용한 시뮬레이터를 설계 및 구현하고 모의실험을 수행한다. 마지막으로 기가비트 이더넷 환경 같은 고속화와 대용량화의 네트워크 환경에서 보안노드의 고속화를 저해하는 요인을 분석하고 성능을 향상시키기 위한 방안을 제시한다.

논문의 나머지 구성은 다음과 같다. 2장에서는 관련연구로서 침입탐지시스템과 보안정책 그리고 표준 프로토콜과 정보보고 및 분석 형태에 대하여 기술하고, 3장에서는 기가비트 침입탐지시스템인 보안 노드의 구조를 제안하고 분석하며, 4장에서는 보안 노드 구조 분석을 기반으로 경보 정보 전달 메커니즘을 모델링하고 OPNET을 이용하여 시뮬레이터 설계하고 구현한다. 5장에서는 모의실험 결과를 기반으로 성능분석을 수행한다. 마지막으로 6장에서는 결론 및 향후 연구로서 끝을 맺는다.

2. 관련 연구

2.1 침입탐지시스템

침입(intrusion)은 컴퓨터가 사용하는 자원의 무결성(integrity), 기밀성(confidentiality), 가용성(availability)을 저해하는 일련의 행위들의 집합 또는 컴퓨터 시스템의 보안정책(SP : Security Policy)을 파괴하는 행위로 규정한다. 침입 탐지 시스템(IDS : Intrusion Detection System)은 대부분 침입 차단 시스템과 연계하여 네트워크 단계 혹은 호스트 단계에서 비정상적인 사용, 오용 등의 침입을 관리자가 실시간으로 탐지를 할 수 있는 시스템이며 침입탐지 유형에 따라 비정상 탐지(Anomaly Detection), 오용 탐지(Misuse Detection) 등으로 구분한다. 일반적으로 접근 시 정해진 모델을 벗어나는 경우를 탐지하는 것을 비정상 탐지라 하며, 침입이라고 정해진 모델과 일치하는 경우를 오용 탐지라 한다. 또한, 웹 서비스와 같은 호스트에 설치되어 설치된 호스트만을 대상으로 침입탐지를 하는 것을 호스트-기반 IDS라고 하며 일정 부분의 네트워크 전체를 대상으로 침입탐지를 하는 것을 네트워크-기반 IDS라고 한다[2, 4-5].

2.2 보안 정책

보안 정책 시스템(SPS : Security Policy System)은 중요한 정보와 다른 자원들이 특정한 시스템에서 관리되어 분산되는 방법을 규제하는 법 혹은 규칙을 설정한다. 보안 정책 시스템은 보안 정책 데이터베이스(SPD : Security Policy Database), 보안 정책 서버(SPS : Security Policy Server) 그리고 정책 클라이언트(PC : Policy Client)로 구성되며 보안 정책 프로토콜(SPP : Security Policy Protocol)을 사용하여 정보를 교환한다. 정책의 한 예로, 규칙-기반 정책은 IP 주소, 시간, 프로토콜, 그리고 차단, 로그인, 경고 혹은 통과 허용 같은 조치를 명시하기 위한 지시와 같은 qualifier를 사용하여 보안 정책을 자동으로 시행하도록 해준다[6-8].

2.3 정보 보고 및 분석

현재 IDMEF의 메시지로는 두 가지가 정의되어 있다: Alert와 Heartbeat[9, 10].

2.3.1 경보(alert) 클래스

일반적으로 분석기(analyzer)가 조사하도록 배치되어 있는 어떤 이벤트를 탐지할 때마다, 자신의 매니저에게 경보 메시지를 보낸다. 경보 메시지는 단일 탐지 이벤트 혹은 복수의 탐지 이벤트일 수 있다. 경보는 외부 이벤트에 대응하여 비동기적으로 발생한다. 현재 경보는 다음과 같이 세 가지로 분류된다.

- ToolAlert 클래스 : 공격 도구 혹은 트로이 목마 같은 악성 프로그램의 사용에 관련되는 추가적인 정보를 가지며, 이러한 도구들을 식별할 수 있을 때 분석기에 의하여 사용될 수 있다.
- CorrelationAlert 클래스 : 경보 정보의 상호관련(correlation)에 관련되는 추가적인 정보를 가진다. 한 개 이상의 이미 전송된 경보를 함께 그룹하기 위함이다.
- OverflowAlert 클래스 : 버퍼 오버플로 공격에 관련되는 추가적인 정보를 가진다. 분석기로 하여금 오버플로 공격 자체에 대한 상세한 내용을 제공하도록 하기 위함이다.

2.3.2 Heartbeat 클래스

매니저에게 분석기의 현재 상태를 나타내기 위하여 사용된다. Heartbeat는 정기적인 기간에 전송되도록 되어있다. 분석기로부터의 Heartbeat 메시지의 정기적인 수신은 분석기가 현재 운영 중임을 매니저에게 나타내며, 메시지가 없을 경우 분석기 혹은 네트워크 연결이 실패되었다는 것을 지시한다.

현재의 보안 시스템은 시스템 간의 상호 운용성이 부족하여 대규모 망에서 효과적인 침입 탐지를 수행하는데 어려움이 있다. 이에 따라 대규모 분산 시스템에서의 침입 탐지 시스템 사이의 정보 교환 등에 대한 기술 개발이 절실히 요구된다.

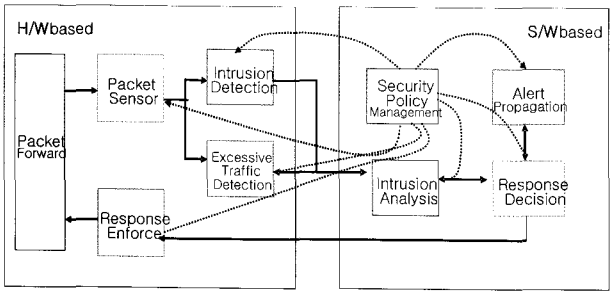
3. 제안된 보안 노드 구조 분석

3.1 노드 구조

인터넷의 폭발적인 사용의 증가로 정보통신 인프라는 기가비트 이더넷 환경 같은 고속화와 대용량화로 네트워크 환경이 현실화되고 있으며 정확한 탐지, 나아가 예방까지 그리고

높은 성능을 기반으로 데이터를 처리할 수 있는 보안 기법들이 연구 중에 있다[11-14]. 네트워크 속도의 증가에 따른 침입탐지 기술도 상응하는 고속침입탐지 기술이 요구되며, 이에 따라 10G급 이상의 보안 어플라이언스 및 보안 엔진의 개발이 요구된다. 그러므로 개발 중인 시스템의 구조에 따른 성능 분석 연구는 매우 중요하여 필수적으로 수행되어야 한다.

본 장에서는 고속 네트워크 환경에서 침입탐지 및 대응을 수행하기 위하여 현재 개발 중인 기가비트 침입탐지시스템의 보안 노드에 대한 구조를 모델링을 위하여 간략히 분석한다. (그림 1)은 고속으로 침입탐지 및 대응기능을 제공하는 기가비트 침입탐지시스템의 보안 노드 구조의 시스템 블록 다이어그램이다.



(그림 1) 제안된 보안 노드의 블록 다이어그램

보안 노드는 하드웨어를 기반으로 하여 침입에 대해 고속 시그너처(signature) 탐지를 하는 이더넷 인터페이스 보안 카드를 사용함으로써 네트워크 유해 트래픽의 검출 및 차단을 가속화시키며 기가비트 네트워크 속도 지원이 가능하다. 또한 트래픽 모니터링뿐만 아니라 실시간 대응 기능을 지원하며 네트워크상에서 스텔스(stealth) 형태의 동작으로 자체 시스템 보안이 용이하다. 침입분석 후 유해한 트래픽이라 판정되면 피해를 최소화 하도록 즉각적인 대응 체계를 갖는 구조이다.

3.2 통신 메커니즘 구조 분석

3.2.1 경보 메시지 형식

분산 침입탐지시스템의 침입탐지와 분석을 통해 근원지 주소와 포트, 목적지 주소와 포트 그리고 프로토콜의 다섯 가지의 튜플을 기반으로 (그림 2)와 같은 경보 형식으로 탐지정보를 전달한다[15].

Attack Type	Sour.Dest IP addr.	Sour.Dest port	Protocol	Content

(그림 2) 경보 메시지 전달 형식

경보 메시지 형식은 공격 종류, 근원지와 목적지 주소, 근원지와 목적지 포트, 프로토콜 그리고 컨텐츠의 형식으로 구성된다.

3.2.2 과다 트래픽 메시지 형식

과다 트래픽 정보 데이터는 트래픽의 측정을 통하여 BPS (Bit Per Second)와 PPS(Packet Per Second) 그리고 패킷 수신 시간 정보의 수집으로 각 트래픽의 특성에 따라 분류하여 저장하고 임계치와 연관성을 분석하여 DoS(Denial of Service)같은 공격의 판단에 이용한다. DDoS의 경우는 분산된 네트워크 전역에서 공격대상 호스트를 집중 공격하는 경향이 대부분이다. 이러한 경우 과다 트래픽은 공격 대상 호스트가 위치하는 네트워크의 인입점에 위치하는 경계라우터의 보안 노드로 집중될 가능성이 크다. 즉, 임계치로 설정한 트래픽의 변동 율을 감지 할 수 있다. 이러한 트래픽 변동 특성 및 네트워크 탐지정보의 경보를 모니터링하여 감지함으로 네트워크 보안이 가능하다.

과다 트래픽 탐지는 두 단계로 나누어 흐름 관리 기능을 수행한다. 먼저 집합 흐름 관리 기능을 통해 이상 징후가 예상되는 흐름들을 먼저 감지한다. 감지되어 의심되는 흐름에 대해 프리미티브 흐름 관리기능을 이용하여 상세히 관리한다[15].

가. 집합 흐름 관리기능

일반적으로 과다 트래픽은 하나 또는 다수의 시스템이 특정 시스템으로 많은 트래픽을 유입시키거나, 하나의 시스템이 다수의 시스템을 스캔하는 형식으로 이루어지기 때문에 동일한 근원지 IP주소, 동일한 목적지 그리고 목적지 포트를 기준으로 분류하고 각각에 대한 초당 패킷 수와 초당 비트 수를 관리하여 과다 트래픽 탐지의 판단 근거로 사용한다(그림 3 참조).

Source IP addr.	BPS	PPS	Ifindex

Dest. IP addr.	Dest. port	BPS	PPS	Ifindex

(그림 3) 집합 흐름 관리 메시지 형식

나. 프리미티브 흐름 관리기능

집합 흐름 관리 기능 모듈로부터 통보 받은 의심스러운 집합 흐름에 해당하는 흐름만 별도로 수집 및 관리하여 5개의 필드 즉 근원지 IP주소, 목적지 IP주소, 근원지 포트 번호, 목적지 포트 번호, 그리고 프로토콜의 패턴을 상세히 분석하고 분석된 각각의 트래픽에 대해 초당 비트 수, 초당 패킷 수 그리고 최종 패킷 수신 시간을 관리한다(그림 4 참조).

Sour. IP addr.	Sour. IP	Dest. IP addr.	Dest. IP	Prot ocol	BPS	PPS	If Index	Time Stamp

(그림 4) 프리미티브 흐름 관리 메시지 형식

프리미티브 흐름 관리기능을 통해 과다 트래픽이라 분석되면 (그림 5)와 같은 과다 트래픽 메시지 형식으로 탐지정보를 전달한다.

SGS ID	Abno. Traf. Descript	Sour. IP addr.	Sour. port	Dest. IP addr.	Dest. port	Prot ocol	BPS	PPS	Time Stamp

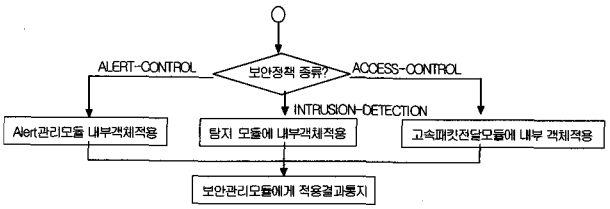
(그림 5) 과다 트래픽 메시지 형식

과다 트래픽 메시지 형식은 보안 노드 번호, 비정상 트래픽에 대한 기술, 근원지와 목적지 주소, 근원지와 목적지 포트, 프로토콜, BPS, PPS 그리고 패킷 수신시간의 형식으로 구성된다.

3.3 보안정책과 대응관리

3.3.1 보안정책 관리

보안정책관리 및 적용은 보안관리 시스템으로부터 전달 받은 보안에 관한 정책 정보를 저장하고 해당 모듈에 적용한다. 보안 노드는 보안관리 시스템에게 보안정책 정보를 요구할 수 있다. 보안관리 시스템으로부터 전달 받은 보안정책 정보를 저장하고 해당 모듈에 적용한다(그림 6 참조)[8].

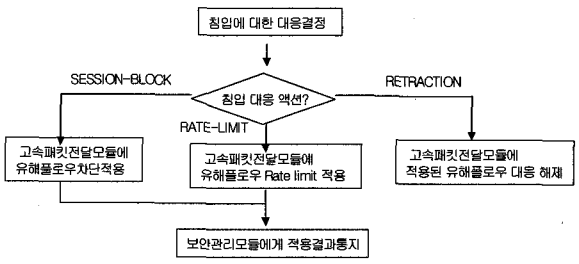


(그림 6) 제안된 보안정책 처리 과정

보안정책의 종류로는 경보 통제 정책, 침입탐지 정책 그리고 접근 통제 정책이 있다.

3.3.2 침입대응 관리

침입탐지에 따른 대응 결정에서는 트래픽 측정과 이벤트 분석 정보를 기반으로 침입분석과 대응을 결정하여 각 모듈로 전달한다. (그림 7)에서는 본 논문에서 제안한 대응처리 전달과정을 보여준다. 보안관리 시스템으로부터 침입에 대한 대응이 결정되면 보안 노드의 해당 모듈에게로 전달한다. 대응결정 종류로는 세션 차단, rate limiting, 그리고 이벤트 재분석이 있다[15].



(그림 7) 제안된 대응 결정 처리 과정

3.4 경보 축약

분산 침입탐지시스템에서의 경보 축약은 시스템의 처리 부하를 감소시키기 위하여 많은 양의 경보 데이터 발생량을 필터링과 집단화를 통해서 줄여주는 것이다. 축약 처리 과정은 먼저 경보 데이터를 수집하고 가공하여 저장한다. 저장된 많은 양의 경보 데이터 분석을 통하여 필터링은 주소, 프로토콜, 포트 번호, 그리고 헤더 정보를 기반으로 경보를 삭제 혹은 허가 할 수 있다. 집단화는 동일하게 생성되는 경보데이터에 대하여 하나의 경보 메시지에 카운터 정보를 추가하여 전송함으로써 축약 기능을 수행하고 과다 트래픽에 대한 정보를 분석할 수 있는 기법을 제공한다. 축약 방법은 다음 <표 1>과 같다[16, 17].

〈표 1〉 축약방법

방 법	형 식	의 미
축약(Compression)	[A, A, A, ..., A] => A	여러 번 발생한 경보를 하나의 경보로 대치
억제(Suppression)	[A, B, p(A)<p(B)] => ϕ	우선순위가 높은 경보는 우선순위가 낮은 경보를 억제하여 보다 먼저 전달
카운터(Count)	[n X A] => B	하나의 경보발생 회수가 임계치로 정의한 횟수와 같으면 여러번 발생한 경보는 새로운 경보 대치
일반화(Generalization)	[A, A⊂B] => B	하나의 경보가 그것의 상위 클래스에 의해 참조
특수화(Specialization)	[A, A⊃B] => B	경보 일반화 방법과 반대의 개념으로 많은 특정한 하위 클래스 경보에 의해 경보의 대치를 제공

4. 모델링 및 시뮬레이터 구현

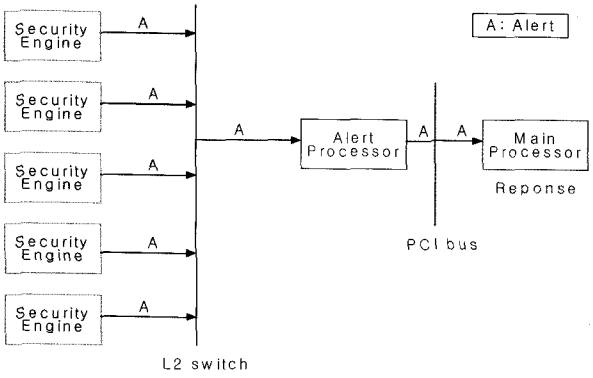
본 장에서는 보안 노드 구조 분석을 기반으로 성능 평가를 수행하기위해 시스템을 모델링하고 시뮬레이터를 구현한다.

4.1 보안 노드 모델링

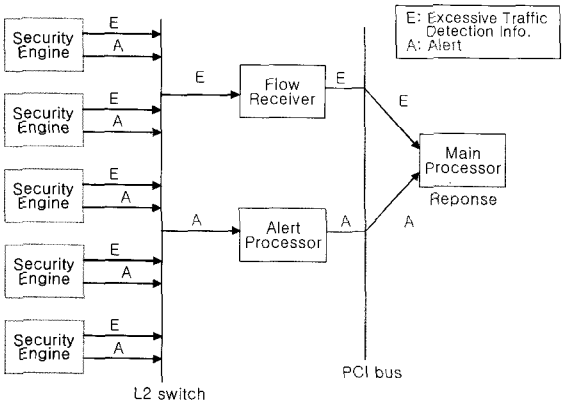
보안 노드의 성능을 평가하기 위해서 기가비트 침입탐지시스템인 보안 노드의 성능을 저하시키는 원인을 분석할 필요가 있다. 따라서 본 논문에서는 보안 노드에 관한 분석을 토대로 성능을 평가하기위해서 시스템을 모델링하고 시뮬레이터를 구현한다.

보안 노드 모델링은 두 단계에서 수행하였다. 먼저, 하드웨어기반에서 고속으로 모든 이벤트를 탐지하여 생성하는 경보를 대응능력에 따라 평가하는 모델과 둘째, 과다 트래픽을 분석하여 요약한 정보를 토대로 DoS공격의 분석 자료로 사용하는 과다 트래픽과 경보의 통합 모델에서 성능을 평가하도록 모델링 하였다.

(그림 8) (a)은 보안엔진에서 경보를 생성하여 주 프로세스의 대응능력에 따른 평가 모델이며, (그림 8) (b)는 과다 트래픽과 경보의 통합 모델이다. 과다 트래픽 정보를 생성하는 트래픽의 량은 적을 것으로 예상되어 네트워크의 성능에는 경미한 영향을 미칠 것이므로 경보 모델을 주 대상으로 하여 성능 평가를 수행하였다.



(a) 경보 모델



(b) 과다 트래픽과 경보 통합 모델

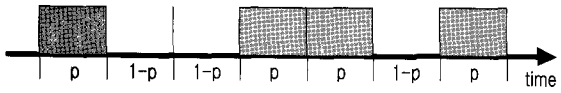
(그림 8) 경보 평가 모델

4.2 경보 도착 프로세스 모델링

경보 도착 프로세스 모델링을 위해 먼저 포아송(Poisson) 프로세스의 이산 모델인 랜덤 프로세스 모델을 이용하였다. 랜덤 프로세스는 베르누이(Bernoulli) 프로세스에 의해 표현된다. 또한 군집성(burstiness)의 영향을 분석하기위해서 IPP (Interrupted Poisson Process)의 이산 모델인 IBP(Interrupted Bernoulli Process) 모델을 사용하였다[3, 18].

4.2.1 랜덤 프로세스

베르누이 프로세스에서 각 슬롯에서의 도착확률은 각 슬롯 사이가 독립적으로 p이다. (그림 9)에서는 랜덤 프로세스 모델에서의 시간 슬롯(time slot)을 보여주고 있다.

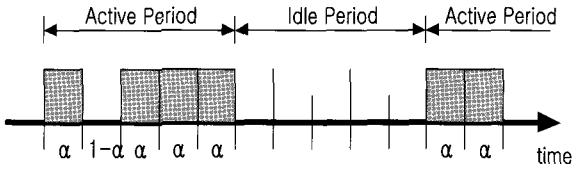


(그림 9) 랜덤 프로세스 모델에서의 시간 슬롯

4.2.2 버스티 프로세스

지수분포를 가지는 ON(active period) 상태와 또 하나의 다른 독립적인 지수분포를 가지는 OFF(silent period) 상태가 교대로 나타나는 포아송 프로세스(IPP) 모델은 ON-OFF 트래픽의 대표적인 모델이다. IPP의 이산 모델로 IBP가 있다.

IBP 모델에서의 시간은 슬롯화 되어있으며 그 크기는 매체에서 하나의 경보패킷 시간과 동일한 것으로 가정한다. 프로세스가 활동 상태에 있을 때 다음 슬롯에서 확률 p를 가지고 그 상태에 머물러 있거나 확률 1-p를 가지고 휴지 상태로 이동 할 것이다. 만약 프로세스가 휴지 상태에 있다면 확률 q를 가지고 휴지 상태에 계속 머물고 확률 1-q만큼 활동 상태로 변할 것이다. 일반적으로 프로세스가 활동기간 내에 있다면 각 슬롯은 확률 α만큼 경보를 포함할 것이다. (그림 10)은 버스티 프로세스 모델에서의 시간 슬롯을 보여준다. 본 논문에서는 α값을 1로 가정하였다.



(그림 10) 버스티 프로세스 모델에서의 시간 슬롯

IBP 프로세스의 전이 확률(transition probability) 행렬은 식(1)과 같이 주어진다.

$$\rho = \frac{1-q}{2-p-q} \tag{1}$$

π_A, π_I를 각각 활동 및 휴지 상태의 정상 상태(Steady State)확률로 정의하면 정상상태 방정식 $\pi P = \pi$로부터 다음과 같은 식 (2)을 구할 수 있다.

$$\pi_A = \frac{1-q}{2-p-q}$$
$$\pi_I = \frac{1-p}{2-p-q} \tag{2}$$

π_A는 평균 대역폭 혹은 평균 도착률(λ)이다.

d를 연속적인 경보들 간의 도착 간 시간이라 하고, d_i을 휴지 슬롯의 어느 슬롯에서 다음 도착 시간까지의 시간 간격이라 한다면 도착 간 시간의 제곱 변화 계수(squared coefficient of variation of inter-arrival times) C^2를 식 (3)과 같이 구할 수 있다.

$$C^2 = \frac{Var(d)}{[E(d^2)]} = \frac{(p+q)(1-p)}{(2-(p+q))^2} \tag{3}$$

본 논문에서는 파라미터 C^2를 경보 정보 도착 프로세스 군집성의 척도로 사용한다.

4.3 경보 도착 프로세스 구현

성능평가를 위한 시뮬레이터에서는 상기에서 기술한 모델들을 이용하여 경보 도착 프로세스를 모델링하였다. 다음은 구현한 경보 도착 프로세스 모델에 대하여 기술한다.

4.3.1 랜덤 프로세스 모델

랜덤 프로세스 모델에서는 각 이벤트 도착은 파라미터 event_load을 가지며 베르눌리 프로세스에 의해 생성된다. 여기서 event_load는 사용자 입력 파라미터이며 그 값은 0≤event_load≤1이다. event_load는 임의의 타임 슬롯에 이벤트가 생성될 확률이고(1-event_load)는 이벤트가 생성되지 않을 확률이다.

4.3.2 버스티 프로세스 모델

버스티 프로세스 모델에서는 IBP를 적용한다. IBP에서 사용자 입력 파라미터는 이벤트 부하 량과 군집성 C^2의 값, 그리고 활동 기간 슬롯마다 이벤트를 포함할 확률인 α이다. α 값에 따라 링크 이용률, 이벤트 손실률, 이벤트 지연 등이 다르게 된다. 파라미터의 값을 다양하게 설정해 버스티 특성을 분석할 수 있다.

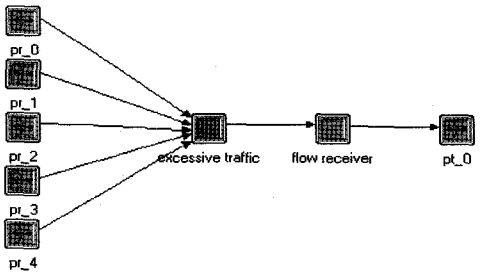
4.4 시뮬레이터 구현

4.4.1 구현환경

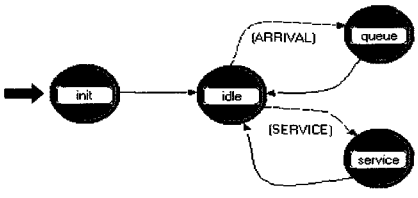
보안 노드의 모델링을 기반으로 시뮬레이터를 구현한다. 시뮬레이터 제작에는 현재 통신 망 시뮬레이션에 가장 많이 이용되고 있는 OPNET(Optimal NETwork)을 이용하였다. OPNET은 최근 이슈가 되고 있는 많은 프로토콜이 구현되어있다. OPNET 시뮬레이션 환경과 제작된 모형들은 그 신뢰성을 인정받아 IETF에서도 인정하고 있다.

4.4.2 요소 시뮬레이터 구현

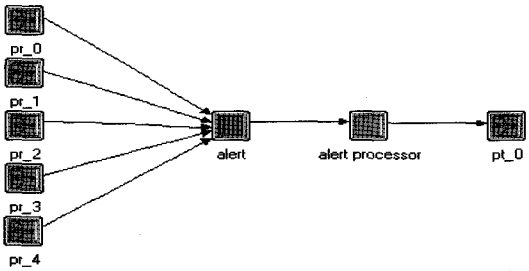
(그림 11)은 경보의 대응 능력을 평가하기위해 모델링 한 결과로써 5개의 보안 엔진으로부터 경보 메시지를 전달 받아 경보를 처리하는 노드 레벨과 프로세스 레벨을 모델링 한 결과이며 또한 과다 트래픽에 관한 메시지를 처리하는 노드 레벨과 프로세스 레벨을 나타낸다.



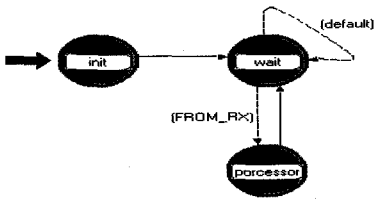
(a) 과다 트래픽 처리 노드 레벨



(b) 과다 트래픽 처리 프로세스 레벨



(c) 경보 처리 노드 레벨

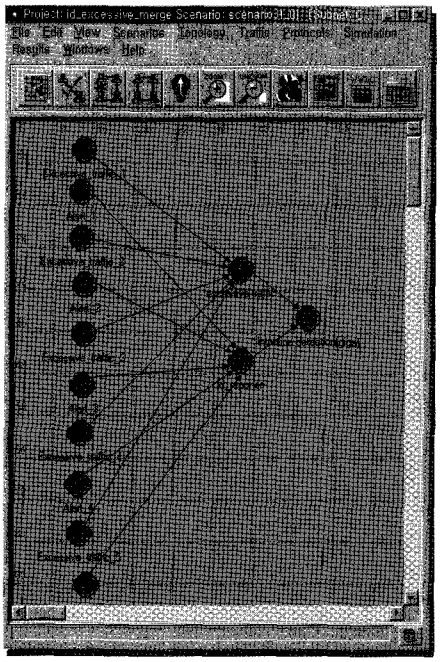


(d) 경보 처리 프로세스 레벨

(그림 11) 경보와 과다 트래픽 처리 프로세스 모델링

4.4.3 시뮬레이터 구현

(그림 12)는 완성된 시뮬레이터 외형도이다. 경보 도착 프로세스 구현과 (그림 11)의 경보와 과다 트래픽 처리 프로세스 그리고 싱크 프로세스를 이용하여 구성한 네트워크 레벨을 보여준다.



(그림 12) 보안 노드 시뮬레이터 구현

5. 성능 분석

5.1 성능분석 시나리오

고속 보안 노드는 하드웨어기반 보안 엔진(*Security Engine*)

의 사용으로 시그너처 기반의 탐지 데이터에 경보를 생성하여 커널 모듈로 전송한다. 커널 모듈과 응용 모듈에서 프로세스의 주 작업은 탐지정보의 상세한 분석 후 대응 정책 결정과 처리 및 관리이다. 즉, 주 프로세스는 보안 엔진에서 기가급으로 생성하는 경보에 대하여 정책을 기반으로 신속한 대응을 결정하고 처리하여야한다.

주 평가의 대상은 지연 성능과 손실 성능을 평가하였으며 지연 성능은 경보의 도착 프로세스에서 주 프로세스의 대응 서비스를 받을 때까지 계산된 시간이며, 손실 성능은 경보의 도착 프로세스에서 발생한 경보의 수를 측정하고 싱크 프로세스에서 도착한 경보의 수를 측정하여 측정한 수에 대한 차이를 이용하여 손실 성능을 계산하였다.

성능평가의 파라미터는 대응에 대한 처리 속도, 경보 정보 전달 율, 버퍼 크기 등을 기준으로 지연과 손실을 평가하였다. 보안 노드의 구조에서 적용할 시나리오는 <표 2>와 같다.

〈표 2〉 성능분석 시나리오

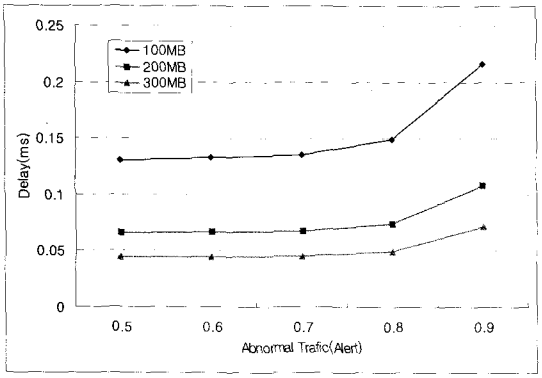
시나리오	성능 분석
1	기가비트 스위치를 이용한 경보의 전송 평가
2	PCI 버스를 이용한 경보의 전송 평가
3	버퍼 크기에 따른 경보의 전송 평가
4	과다트래픽과 경보 통합 전송 능력 평가
5	버스티 크기에 따른 경보의 전송 평가

성능 분석 모델에서는 5개의 보안 엔진에서 경보를 발생하며 경보 대응능력을 파라미터로 적용하여 평가하였다. 대응능력의 파라미터로는 100Mbps에서 300Mbps까지 적용하였으며, 버퍼의 크기는 1,000에서 4,000개로 설정하였다.

5.2 성능 분석

5.2.1 기가비트 전송 평가

(그림 13)은 평가모델의 5개의 보안엔진에서 생성하는 경보의 전체 부하량이 50%에서 90%까지에 대한 기가비트 스위치를 이용한 전송 성능을 평가한 것이다. 보안 엔진에서 기가비트 스위치를 이용하여 생성한 경보를 주 프로세서의 대응 능력에 따른 지연 성능을 나타낸다. 경보의 량에 따라 대응 유닛의 100Mbps 처리 속도에서 심각한 지연을 보여주고 있다.



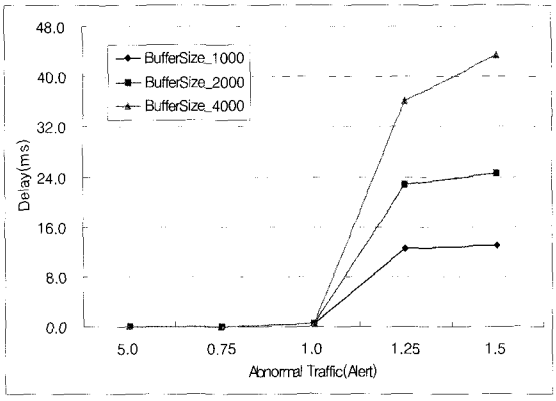
(그림 13) 기가비트 스위치를 이용한 경보 지연

5.2.2 PCI 버스 전송 평가

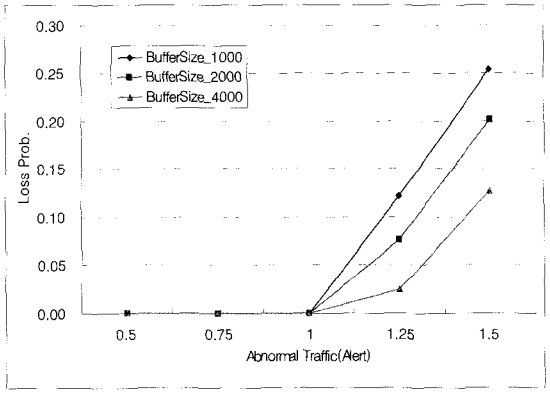
보안 엔진에서 생성한 경보의 전달을 PCI 버스를 통하여 주 프로세서로 전송하는 경우 그 대응 능력을 평가하였다. 그 결과, 기가비트 스위치를 이용한 전송결과와 거의 동일한 결과를 도출하였다. 경보 정보의 지연 성능은 대응 처리 속도와 가장 밀접하게 연관된 것으로 분석되었으며, 따라서 대응 프로세싱 속도를 향상시킬 수 있는 방안 연구가 필요하다고 하겠다.

5.2.3 버퍼 크기에 따른 평가

(그림 14)와 (그림 15)는 평가모델이 보안엔진에서 생성하는 경보의 전체 부하량이 50%에서 150%까지에 대하여 대응 유닛 300Mbps에서 기가비트 스위치 전송 시 버퍼 수에 따른 지연과 손실을 나타낸다. 버퍼의 수가 작을수록 지연은 감소하는 반면 손실은 증가하는 경향을 보인다. 그러나 손실 성능은 버퍼의 영향 보다는 대응 처리 속도에 더욱 의존되는 것을 알 수 있었다.



(그림 14) 버퍼 크기에 따른 경보 지연

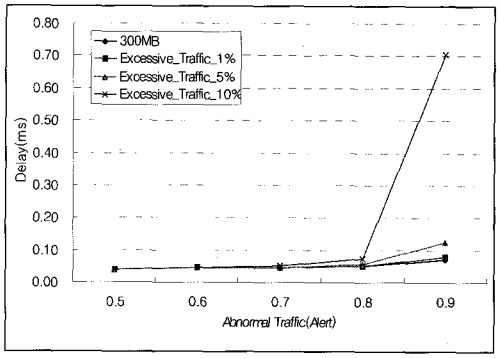


(그림 15) 버퍼 크기에 따른 경보 손실

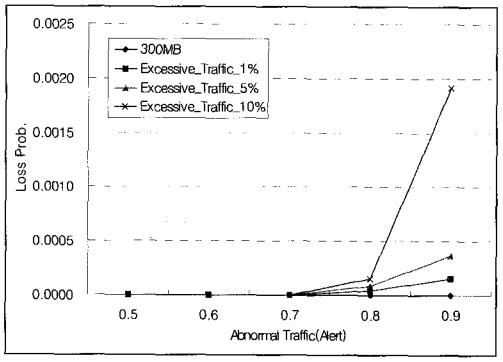
5.2.4 과다 트래픽과 경보 통합 전송 능력 평가

(그림 16)과 (그림 17)은 평가모델의 5개의 보안엔진에서 생성하는 경보의 전체 부하량이 50%에서 90%까지에 대한 기가비트 스위치를 이용한 전송에서 과다 트래픽 정보와 경보 생성을 함께 모델링하여 성능을 평가하였다. 과다 트래픽 정

보의 량을 각각 1%, 5% 그리고 10%씩 증가시키는 통합모델에서 대응 능력에 관하여 성능 평가를 수행하였다.



(그림 16) 과다 트래픽과 경보 전송 지연

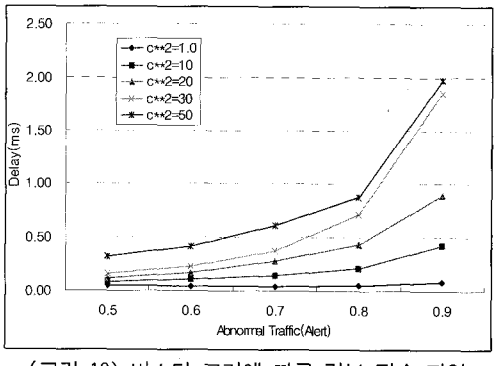


(그림 17) 과다 트래픽과 경보 전송 손실

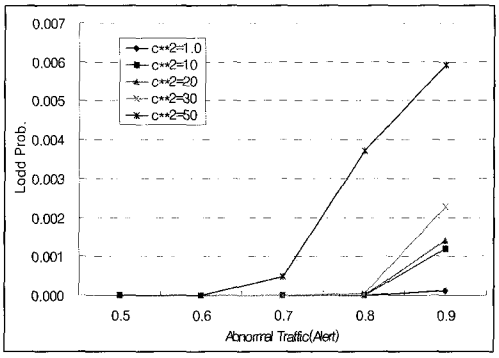
(그림 16)과 (그림 17)은 과다 트래픽 탐지정보량을 변화시키면서 대응 능력 300Mbps에서 지연과 손실의 차이를 나타낸다. 지연과 손실이 과다 트래픽 탐지정보의 량이 증가함에 따라 지연과 손실 전체 성능에 경미하게 영향을 미침을 나타내고 있다.

5.2.5 버스트 크기에 따른 전송 평가

(그림 18)과 (그림 19)는 평가모델의 보안엔진에서 생성하는 경보의 전체 부하량이 50%에서 90%까지에 대하여 군집성(C^2)의 값을 1에서 50까지의 범위에서 기가비트 스위치를 이용한 경보 전송 지연과 손실을 평가한 것이다.



(그림 18) 버스티 크기에 따른 경보 전송 지연



(그림 19) 버스티 크기에 따른 경보 전송 손실

(그림 18)과 (그림 19)는 군집성(C^2) 크기에 따라 네트워크 전송에 미치는 영향을 평가한 것으로서 (그림 18)에서는 랜덤 프로세스와 버스티 프로세스 사이 경보 지연이 커다란 차이가 있음을 보여준다. (그림 19)는 과다한 경보의 생성으로 인한 버퍼의 손실을 나타내며 군집성(C^2)의 크기에 따라 손실률이 증가함을 나타낸다. 특히 군집성(C^2)의 정도가 클수록 그리고 경보의 부하가 높아질수록 지연이 급격히 증가하고 손실이 증가함을 볼 수 있다.

따라서, 의도적으로 일정 시간 동안 분산 DoS(Denial of Service) 공격이 수행된다면 과다한 경보의 생성이 보안 노드의 성능에 크게 영향을 미치게 됨을 알 수 있다.

6. 결론 및 향후 연구

인터넷 사용의 폭발적인 증가는 일상적인 개인의 생활뿐만 아니라 사회생활 전반에 걸쳐 많은 변화를 가져왔으며 또한 주요한 수단으로 이용되고 있다. 네트워크를 통하여 업무서류, 금융거래 그리고 개인의 신상정보가 거래되고 있으며 불법적으로 침해되고 있어 이는 심각한 사회문제를 유발시키고 있다. 이러한 문제를 해결하기위해 시스템과 네트워크 차원의 보안에 대한 중요성이 증가되고 있으며 특히 불법적인 침입을 탐지하고 대응하는 침입탐지시스템에 대해 연구가 활발히 이루어지고 있다.

본 논문에서는 고속 보안 노드로서 기가비트 침입탐지시스템인 보안 게이트웨이의 구조를 제안하고 시스템을 모델링하여 성능을 평가하였다. 보안 노드 레벨에서 기가비트 보안 노드의 구조 분석을 통하여 성능의 병목점으로 예상되는 하드웨어 기반 컴포넌트와 소프트웨어 기반 컴포넌트 사이의 통신 메시지 전달 성능을 평가하였다. 침입 탐지 엔진에서 발생하는 경보 메시지와 과다 트래픽 탐지부에서 발생하는 과다 트래픽 정보의 도착 프로세스는 랜덤 프로세스와 버스티 트래픽 모델인 IBP 두 가지를 사용하여 비교분석하였다. 시뮬레이터 구현에는 OPNET을 이용하였으며 통신시스템의 기능성을 검정할 수 있는 여러 가지 인수들을 사용하여 성능 평가 매개 변수로 이용하였다.

보안 노드에서 하드웨어 기반의 고속 침입 탐지부에서는 고속의 침입 탐지를 수행하지만 이 탐지 정보를 기반으로 대

응 정책 결정부는 소프트웨어 기반의 처리가 이루어지기 때문에 전체적인 보안 노드의 성능이 대응 장치의 대응 처리 능력에 의하여 의존된다는 것이 분석되었다.

차세대 침입탐지시스템에서의 요구 안은 정확한 탐지 뿐만아니라 예방이 가능한, 결정적인 대응과 탐지 그리고 고성능 등을 제시하고 있다. 유해한 트래픽에 대해 하드웨어기반으로 기가비트급까지 침입 탐지를 수행하여 경보를 생성하지만 소프트웨어기반 대응 능력에 의해 기가비트급까지 처리되지 못하여 성능이 저하되는 것으로 분석되었으며, 효율적인 대응을 위해서 대응 능력에 관한 연구가 필요하다는 것이 본 분석을 통해서 도출 되었다.

대응에 관한 성능을 향상시키기 위해서는 3.4절에서 기술한 보안 경보의 필터링과 축약이 한 가지 방안으로 여겨지며, 고속 트래픽 모니터링 기술 연구 그리고 나아가 대규모 네트워크 환경에서의 협력 방안이 모색되어야 할 것으로 생각된다.

참 고 문 헌

[1] Jai Sundar Balasubramaniyan, Jose Omar Garcia Fernandez, David Isacoff, Eugene Spafford, and Diego Zamboni, "An architecture for intrusion detection using autonomous agents". In Proceedings of the Fourteenth Annual Computer Security Applications Conference, pages 13-24, *IEEE Computer Society*, December, 1998.

[2] Carl Endorf, Eugene Schultz, and Jim Mellander, Intrusion Detection & Prevention, McGraw-Hill, 2004.

[3] 한국전자통신연구소 최종연구보고서, 분산형 라우터 성능분석을 위한 Traffic Generator 구조에 관한 연구, 1995년 12월.

[4] Rajeev Gopalakrishna, "A Framework for Distributed Intrusion Detection using Interest-Driven Cooperating Agents", *CERIAS Tech.* Report 2001-44, Purdue University, 2001.

[5] Joseph Barrus and Neil C. Rowe. A distributed autonomousagent network-intrusion detection and response system. In Proceedings of Command and Control Research and Technology Symposium, Monterey, CA, pp.577-586, June, 1998.

[6] IETF, RFC 3084, "COPS Usage for Policy Provisioning (COPS-PR)", March, 2001.

[7] IETF, RFC 2251, "Lightweight Directory Access Protocol (v3)", December, 1997.

[8] IETF RFC 2748, "The COPS(Common Open Policy Service) Protocol", Jan., 2000.

[9] D. Curry, H. Debar, "Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language (XML) Document Type Definition", IETF Internet Draft, draft-ietf-idwg-idmef-xml-07.txt, Jun., 2002.

[10] H. Debar, D. Curry, B. Feinstein, "The Intrusion Detection Message Exchange Format", IETF Internet Draft, draft-ietf-idwg-idmef-xml-14, January, 2005.

[11] Kruegel, C., Valeur, F., Vigna, G. and Kemmerer, R. "Stateful intrusion detection for high-speed networks", In Proceedings of the IEEE Symposium in Security and Privacy, pp.266-274, 2002.

[12] ISS. RealSecure Gigabit Network Sensor. http://www.iss.net/products_serivces/enterprise_protection/rsnetwork/gigabitsensor.php, Setember, 2002.

[13] CISCO. CISCO Intrusion Detection System. Technical Information, November, 2001.

[14] M. Roesch. "Snort-Lightweight Intrusion Detection for Networks". In Proceedings of the USENIX LISA '99 Conference, November, 1999.

[15] 한국전자통신연구원 기술문서 v1.0, 2003년 7월.

[16] Frederic Cuppens, Alexander Mierge, "Alert Correlation in a Cooperative Intrusion Detection Framework", IEEE Symposium on Security and Privacy 2002.

[17] H. Debar and A. Wespi, "Aggregation and Correlation of Intrusion Detection Alerts", RAID 2001, LNCS 2212, pp.85-103, 2001.

[18] Ichiro Ide, "Superposition of Interrupted Poisson Process and its application to packetized voice multiplexer", in *ITC*-12, pp.1399-1405, Turin, 1988.

전 용 희

e-mail : yhjeon@cu.ac.kr

1978년 고려대학교 전기공학과(학사)

1989년 North Carolina State University Elec. and Comp. Eng.(석사)

1992년 North Carolina State University Elec. and Comp. Eng.(박사)

1989년 노스캐롤라이나주립대 Dept of Elec. and Comp. Eng. TA

1989년~1992년 노스캐롤라이나주립대 부설 CCSP(Center For Comm. & Signal Processing) RA

1992년~1994년 한국전자통신연구원 광대역통신망연구부 선임연구원

1994년~현재 대구가톨릭대학교 컴퓨터·정보통신공학부 교수

2001년~2003년 대구가톨릭대학교 공과대학장 역임

2004년~2005년 한국전자통신연구원 정보보호연구단 초빙연구원

관심분야 : 네트워크 보안, BcN QoS & Security, 통신망 성능분석

장 정 숙

e-mail : jsukjj@cu.ac.kr

1989년~1991년 경일대학교 공과대학 컴퓨터공학과(학사)

1992년~1995년 대구가톨릭대학교 교육대학원 전자계산교육전공(석사)

1998년~2004년 대구가톨릭대학교 대학원 컴퓨터·정보통신공학 전공 이학박사

2004년~현재 대구가톨릭대학교 컴퓨터정보통신공학부 IT교수

관심분야 : 임베디드 네트워크 보안, BcN & QoS 보안, 홈네트워크 보안, 통신망 성능분석,

장 종 수

e-mail : jsjang@etri.re.kr

1984년 경북대학교 전자공학과(학사)

1986년 경북대학교 전자공학과(석사)

2000년 충북대학교 컴퓨터공학과(공학박사)

1989년~현재 한국전자통신연구원 정보보호연구단 네트워크보안그룹 그룹장

관심분야 : 네트워크보안, 웹서비스보안, Secure OS, IDS/IPS, Traffic Management