보안정책 기반 침입탐지시스템에서 정보 전달을 위한 분산 통신 모델과 성능 평가

정회원 장정숙*, 전용희*, 장종수**, 손승원**

A Distributed Communication Model and Performance Evaluation for Information Transfer in a Security Policy-based Intrusion Detection System

Jung-Sook Jang*, Yong-Hee Jeon*, Jong-Soo Jang**, Seung-Won Sohn** ***Regular Members***

요 약

본 논문에서는 네트워크 차원의 종합적인 보안관리가 가능한 침입탐지시스템의 분산 통신모델을 제안하고 보안 노드와 분산 시스템 레벨에서 각각 모델링하고 시뮬레이터를 설계하고 구현한다. 노드 레벨에서는 하드웨어기반 침입탐지를 수행하는 기가비트 보안 노드의 구조분석을 기반으로 경보 메시지의 전달 성능을 평가한다. 분산 시스템 레벨에서는 보안정책을 기반으로 네트워크 수준에서 분산 침입탐지시스템의 컴포넌트 사이에 전달되는 탐지 및 경보 정보의 전달 성능을 모의실험을 통하여 성능평가를 수행한다. 제안된 모델에서 통신 메커니즘의 결정요인들을 적용하여 성능 평가를 수행하고, 시스템의 정량적인 이해를 하기 위하여 결과를 제시한다.

Key Words : Intrusion Detection System(IDS); Performance Evaluation; Distributed Communication Model, Simulation; Security Policy.

ABSTRACT

In this paper, we propose a distributed communication model of intrusion detection system(IDS) in which integrated security management at networks level is possible, model it at a security node and distributed system levels, design and implement a simulator. At the node level, we evaluate the transfer capability of alert message based on the analysis of giga-bit security node architecture which performs hardware-based intrusion detection. At the distributed system level, we perform the evaluation of transfer capability of detection and alert informations between components of distributed IDS. In the proposed model, we carry out the performance evaluation considering decision factors of communication mechanism and present the results in order to gain some quantitative understanding of the system.

Ⅰ. 서 론

인터넷의 폭발적인 발전과 함께 네트워크 상에서의 침입 시도가 증가되고 있어 불법적인 침입을 탐지하고 대응하는 침입탐지시스템에 대한 연구가 활발히 이루어지고 있다. 또한 네트워크를 통한 분산 공격의 증가로 인하여 분산 침입탐지 기술에 대하여 관심이 고조되고 있다. 현재의 상용 보안제품들은 네트워크 차원의 침입에 대한 전역적인 탐지 분석과 신속하고 적극적인 대응이 어려운 실정이다. 이에 따라 주된

* 대구가톨릭대학교 컴퓨터정보통신공학부 컴퓨터네트워크보안연구실(jsukjj, yhjeon@cu.ac.kr)
** 한국전자통신연구원 정보보호연구단(jsjang, swsohn@etri.re.kr)
논문번호 : 040174-0507, 접수일자 : 2004년 5월 1일

연구 분야는 집중 및 단일 프레임워크 기반 침입탐지 시스템에서 분산 프레임워크 기반 침입탐지시스템으로 이동하는 추세이다. 분산 침입탐지시스템은 데이터의 분석이 감시되는 호스트 수에 비례하여 다수의 위치에서 수행되며, 분석컴포넌트가 감시되는 호스트 수에 비례하고, 위치가 분산되어야 한다. 침입탐지시스템은 최근에 네트워크 보안을 위하여 아주 중요한 기술로 그 중요성이 점차 증대될 것으로 기대된다[1][2].

복잡해지고 대형화되는 네트워크 관리를 위해 정책 기반 네트워크 구조가 필요하다. 정책이란 다른 조건에서 네트워크의 행위를 제어하는 일련의 규칙을 의미한다. 침입탐지를 위한 보안정책은 보호되어야 할 정보 자산, 필요한 침입탐지시스템의 형태, 침입탐지시스템의 위치, 침입탐지시스템이 탐지할 공격의 유형, 특정 공격이 식별되었을 때 제공될 대응 혹은 경보(alert)의 형태를 정의한다. 보안정책시스템의 기본적인 컴포넌트는 정책 서버, 정책 클라이언트, 보안정책 프로토콜 그리고 데이터베이스로 구성된다[3].

분산 침입탐지시스템에서는 각 분산 노드사이 통신 메시지를 통하여 분산 시스템의 전반적인 상태를 얻을 수 있기 때문에 침입탐지 후 관리자 노드에게 보고와 대응을 위한 통신 메커니즘은 중요하다. 분산 침입탐지시스템에 대한 연구가 세계적으로 많이 진행되고 있지만, 국내에서는 아직 분산 침입탐지시스템 컴포넌트 사이의 통신 메커니즘과 일반적인 통신 모델에 대하여 발표된 연구 결과는 거의 찾아 볼 수 없다. 더구나 침입탐지시스템의 통신 모델과 성능 평가에 대한 작업은 없는 실정이다.

기존의 침입탐지시스템에서는 특정 네트워크 상에서 침입이 탐지되고 동일한 네트워크 세그먼트 상에서만 대응을 하기 때문에 네트워크 차원의 대응에 어려운 점이 있다. 즉, 같은 공격에 대하여 전체 네트워크의 다른 부분에서 인식하게 되는 정보와 전체 네트워크 차원에서 관련 데이터를 상호 결합하는 기능이 부족하고, 침입자에 대한 대응에 있어 각 도메인 간의 협력이 없는 상태이다. 체계적이고 종합적인 보안관리는 침입을 탐지하고 대응할 수 있으며 침입을 예측할 수 있게 한다. 그러므로 탐지정보의 협력으로서 전역적인 네트워크수준의 보안이 가능하려면 분산 침입탐지시스템의 컴포넌트 사이 탐지정보의 전달을 위한 통신모델에 대한 연구와 성능 평가가 선행되어야 한다.

본 논문에서는 침입탐지와 대응 그리고 침입을 예측할 수 있도록 독립적인 보안 네트워크에서의 네트워크 차원의 종합적인 보안관리를 가능하게 하기위하여 정책 프레임워크를 기반으로 체계적인 관리구조와 계층적인 침입분석기법을 적용한 통신모델을 제안하고 성능평가를 수행한다. 성능평가는 보안 노드 레벨과 분산 시스템 레벨, 두 가지 단계에서 시스템을 모델링하고 시뮬레이터를 설계 및 구현하여 다양한 입력 프로세스 모델을 적용한 모의실험과 성능평가를 수행한다. 먼저, 보안 노드 레벨에서는 네트워크의 환경이 고속화 대용량화로 변화함에 따라 침입탐지를 고속으로 수행하기위해 하드웨어기반 침입탐지를 수행하는 기가비트 보안 노드의 구조분석을 기반으로 경보 메시지의 발생에 따른 대응 능력에 대한 평가를 수행한다. 분산 시스템 레벨에서는 체계적인 구조의 정책 프레임워크를 기반으로 네트워크 수준에서 분산 침입탐지시스템의 컴포넌트 사이 전달되는 탐지정보를 이용하여 종합적인 침입탐지와 대응을 위해 계층적인 침입 분석기법을 적용한 제안된 통신 모델에서 통신 메커니즘의 결정요인들을 적용하여 성능 평가를 수행한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로서 침입탐지시스템, 보안 정책 및 표준 프로토콜, 정보 보고 및 분석의 형태, 그리고 분산 침입 탐지 시스템 통신 프레임워크에 대하여 살펴보고, 3장에서는 분산 침입탐지시스템의 구조를 분석하며, 4장에서는 구조 분석을 기반으로 모델링 및 시뮬레이터 구현, 5장에서 성능 평가, 마지막으로 6장에서 결론 및 향후 연구로 끝을 맺는다.

Ⅱ. 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[4][5]. 또한, 웹 서비스와 같은 호스트에 설치되어 설치된 호스트만을 대상으로 침입

탐지를 하는 것을 호스트-기반 IDS라고 하며 일정 부분의 네트워크 전체를 대상으로 침입탐지를 하는 것을 네트워크-기반 IDS라고 한다[6][7].

보다 효과적인 IDS를 위하여 네트워크와 호스트 기반 침입 탐지를 결합하여 사용하는 것이 바람직하다. 이 경우, 어디에 각 형태를 사용하고 데이터를 어떻게 통합하는 가가 실제적이고 중요한 관심사이다. 본 논문에서는 호스트 기반 IDS와 네트워크 기반 IDS를 결합한 혼합형 IDS를 기반으로 각 IDS 시스템들에서 들어오는 정보를 종합적으로 상호 관련하여 다중 도메인 상의 네트워크에서 침입 탐지를 통합적으로 수행할 수 있는 구조를 제시하고 모델링 하여 종단 간 지연에 대한 성능 분석을 수행한다.

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[8].

2.3 표준 프로토콜

IDS의 표준 프로토콜로는 COPS, IAP/IDXP, SNMP 등이 있으며, 다음과 같은 기능 및 특성을 가지고 있다.

- COPS(Common Open Policy System): IETF의 COPS는 정책 기반 네트워크에서 정책서버(PDP)와 클라이언트(PEP) 사이의 정책정보의 전달을 위한 TCP기반의 간단한 질의/응답 프로토콜이다. 프로토콜 자체 수정 없이 확장을 통한 다양한 클라이언트 타입을 지원한다. COPS는 TCP 기반으로 상위 도메인의 정책 제공 및 통제 목적을 위한 정책 전달 프로토콜이다[9].
- IAP(Intrusion Alert Protocol): IETF의 IDWG에서 침입 경보 프로토콜(IAP)을 제안하였다. 침입 탐지 구성 요소들 사이(sensor/analyzer와 managers)에 침입 경보 데이터(Intrusion alert data)를 교환하기위한 응용 계층의 프로토콜이다. 전달되는 경보는 IDMEF(Intrusion Detection Message Exchange Format)에 명세 되어 있다. 현재 IDMEF의 메시지로는 두 가지가 정의되어 있다: Alert와 Heartbeat[10].

2.4 정보 보고 및 분석

현재 IDMEF의 메시지로는 두 가지가 정의되어 있다: Alert와 Heartbeat.

(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) Heartbeat 클래스

매니저에게 분석기의 현재 상태를 나타내기 위하여 사용된다. Heartbeat는 정기적인 기간에 전송되도록 되어있다. 분석기로부터의 Heartbeat 메시지의 정기적인 수신은 분석기가 현재 운영중임을 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.

2.5 분산 침입 탐지 시스템 통신 프레임워크

지금까지 관련 연구로 침입 탐지 시스템의 종류와 보안정책, IDS를 위한 표준 프로토콜 및 경보와 이벤

트 데이터에 대하여 살펴보았다. 본 절에서는 분산 침입 탐지 시스템의 통신 프레임워크에서 요구사항과 성능 결정 요인들에 대하여 기술한다[2].

분산 침입 탐지 시스템을 구별하는 몇 가지 특징은 다음과 같다.

- E(event)-박스의 수와 위치
- A(analyzer)-박스의 수와 위치
- 컴포넌트 사이의 조정(coordination)
- 통신 프레임워크

여기서 E-박스는 데이터 수집 장치, A-박스는 데이터 분석 장치에 각각 해당한다. 본 논문에서는 분산 침입 탐지 시스템의 통신 프레임워크 컴포넌트에 중점을 둔다. 프레임워크는 실제 통신 메커니즘과 통신 모델로 구성되어 있다. 현재 통신 메커니즘 접근으로는 TCP, UDP, SSH(Secure Shell), SNMP(Simple Network Management Protocol) 등이 사용되고 있다.

2.5.1 요구사항

IDS를 위한 통신 기법에서 바람직한 몇 가지 특징은 다음과 같다: 신뢰성(reliability), 보안(security), 인증(authentication), 무결성(integrity), 비밀성(confidentiality), 부인 봉쇄(non-repudiation), 비-복제(non-duplication), 서비스 거부(DOS) 공격에 대한 저항, 확장성(scalability), 속도(speed).

2.5.2 결정 요인

분산 침입 탐지 시스템 기능의 중요한 한 부분은 다른 컴포넌트 사이의 통신이다. 메시지를 교환함으로써 컴포넌트들은 시스템의 전체적인 상태를 알 수 있다. 통신에서의 붕괴는 시스템의 오동작을 일으키고 실패할 수 있다. 아래 요인들은 서로 배타적이지 않으며, 다른 것에 의존될 수 있다[2]: 컴포넌트의 수와 위치, 고려되는 데이터의 형태, 데이터 양, 데이터 생성빈도, 데이터 표현 방법, 데이터의 민감성.

Ⅲ. 분산 침입탐지시스템 구조 분석

네트워크 상의 통신 및 시스템을 안전하게 보호하기 위해서는 네트워크 차원의 보안관리가 필요하다. 네트워크 차원의 보안관리는 인접한 서비스 제공업자와의 보안관련 정보의 공유를 통하여 협력할 수 있어야만 가능하다. 네트워크 차원의 정보보호 서비스의 중요성이 증가하고 있어 수백 Mbps에서 기가 급까지 처리 가능한 네트워크 정보보호 제품이 등장하고 있지만 개별 시스템 단위의 보안기능의 한계가 존재한다.

이러한 문제를 해결하기위해서 네트워크 차원의 종합적인 침입탐지 분석을 수행하는 글로벌 네트워크보안관리구조의 정립이 주요한 문제로 대두되고 있다. 분산 침입탐지시스템에 체계적인 정책 프레임워크와 종합적인 계층적 분석기법을 적용하여 글로벌 네트워크보안관리가 가능하다. 본 장에서는 분산 침입탐지시스템의 보안 노드와 분산 시스템에 관한 구조를 분석한다. 분산 침입탐지시스템 구조 분석을 기반으로 보안 노드 레벨과 분산 시스템 레벨에서 성능 평가를 수행한다.

3.1 노드 구조

인터넷의 폭발적인 사용의 증가로 정보통신의 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. 기가 급 침입탐지시스템 개발을 위한 구조와 시스템 성능을 예측하기위하여 시스템 성능분석에 대한 연구가 중요하다. 시스템의 성능은 칩 상에 구현된 하드웨어 특성과 그들에서 돌아가는 소프트웨어에 의존된다. 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.

본 논문에서는 고속 네트워크 환경에서 침입탐지 및 대응을 제공하기위한 기가비트 침입탐지시스템의 보안 노드에 대한 구조를 분석한다. 네트워크 속도의 증가에 따른 침입탐지 기술도 상응하는 고속침입탐지 기술이 요구되며, 이에 따라 10G급 이상의 보안 어플라이언스 및 보안 엔진의 개발이 요구된다. 그러므로 시스템의 구조에 따른 성능분석 연구는 매우 중요하여 필수적으로 수행되어야 한다. 그림 1은 고속으로 침입탐지 및 대응기능을 제공하는 기가비트 침입탐지 시스템의 보안 노드 구조의 시스템 블록 다이어그램이다[11].

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 속도를 지원 가능하다. 또한 트래픽 모니터링뿐만 아니라 실시간 대응 기능을 지원하며 네트워크상에서 스텔스(stealth) 형태의 동작으로 자체 시스템 보

안이 용이하다. 침입분석 후 유해한 트래픽이라 판정되면 피해를 최소화 하도록 즉각적인 대응 체계를 갖는 구조이다(그림 1참조).

보안 노드에서는 하드웨어기반으로 고속의 침입탐지를 수행하지만 침입분석에 대한 대응정책 수립에 있어 소프트웨어기반의 처리를 수행하기 때문에 성능 저하가 예상된다.

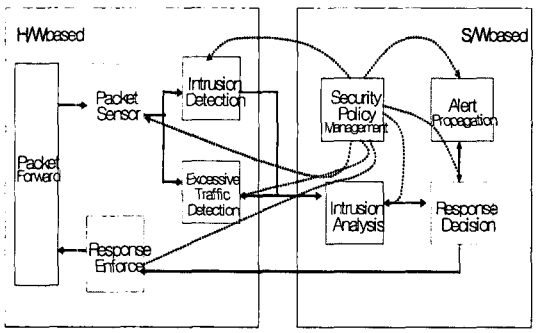


그림 1. 보안 노드의 블록 다이어그램

3.2 시스템 구조

네트워크 차원의 정보보호서비스를 제공하기위해 보안 노드를 광역 네트워크 전역에 조직적으로 분산시켜 이를 중앙에서 통합 관리함으로서 기존의 단일 환경의 정보보호서비스가 가지는 제약적인 문제점을 해결할 수 있다. 즉, 트래픽의 과다한 증가와 다양한 공격 유형에 보다 효율적으로 대응하기 위해서는 현재의 지역적 보안 환경을 광역적 보안 환경으로 확장하여 시스템 상호간의 조직적이고 유기적인 연동을 가능하게 하는 정책기반 프레임워크를 이용하여 네트워크를 보안관리 할 수 있다. 또한 다양한 정보를 수집하고 통합 분석하여 조기에 대응하기위해서는 계층적 통합 분석기법을 적용할 수 있다.

그러므로 정책기반 프레임워크에서 침입탐지 및 대응기능을 계층적으로 분리하고 광역 네트워크 전역에 조직적으로 분산시켜 이를 최상위의 정책서버에서 통합 관리함으로서 기존의 단면적이고 단일 환경의 제약적인 문제점을 해결 할 수 있고 계층적 분석을 통한 침입예측 및 환경에 적합한 대응정책의 결정과 인가가 가능할 것이며 글로벌 네트워크 보안 제어관리가 가능하다.

분산 침입탐지시스템 구조에서는 글로벌 네트워크 보안제어 프레임워크를 위해서 체계적인 보안관리가 가능한 정책기반 관리구조와 종합적인 보안 상황에 대한 판단과 수단을 제공하는 계층적인 침입분석기법을 분석한다[12][13].

3.2.1 글로벌 프레임워크

글로벌 네트워크보안관리 기술이란 지역망의 보안관리방법을 보완하기위한 네트워크 차원의 보안관리로서 망 인입점에서 유해 트래픽을 분석 및 차단하여 네트워크의 성능 저하를 사전에 방지하고 네트워크의 자원 및 주요 통신 장비의 보호기능을 수행하는 것을 목표로 한다.

그림 2는 글로벌 보안관리 네트워크 개념도를 나타낸다. 글로벌 보안관리 네트워크는 보안 오버레이 망(Security Overlay Network)의 구조를 가지며 인접 도메인과의 보안관련 정보의 교환 및 상호협력을 통하여 사용자가 사용하는 광역망에서 동일한 보안 서비스 품질을 유지할 수 있을 것이며 코어망의 보안성을 강화하고 사용자의 서비스 트래픽을 안정적으로 제공할 수 있다.

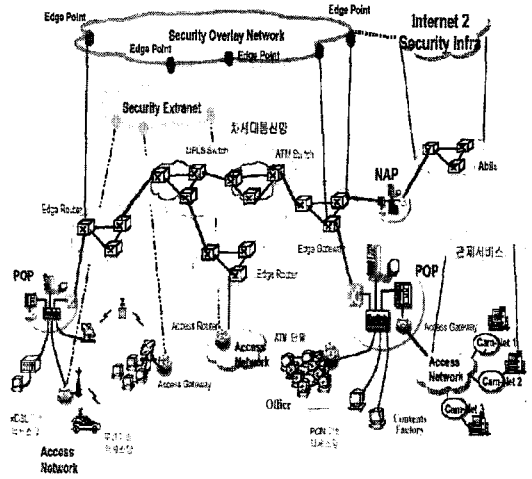


그림 2. 글로벌 보안관리 네트워크 개념도

3.2.2 보안정책기반 관리구조

구조적이고 체계적인 관리와 통합적인 관리를 제공할 수 있도록 IETF 정책기반 프레임워크를 적용하여 네트워크를 보안관리 할 수 있다. 정책기반 네트워크 보안관리 프레임워크는 네트워크 자원에 대한 운용 및 보안관리를 공통된 정책에 따라 일관성 있게 제어할 수 있는 기능을 제공한다. 그림 3은 보안정책 관리 프레임워크의 구조를 보여준다.

그림 3에서 보안정책기반의 보안관리 프레임워크는 보안정책시스템(SPS)의 보안정책서버와 보안정책서버의 관리를 받는 다수개의 정책대상시스템(STS)으로 구성된 중앙 집중화된 관리구조를 갖는다. 여기서 보

안정책 서버가 일관성 있는 정책으로 관리하는 영역을 도메인이라 하며 이 도메인에서 발생하는 모든 보안관련 상황은 해당 도메인의 보안정책서버로 전달되어 체계적이고 종합적으로 관리되며 필요시 인접 도메인으로 전파할 수 있다.

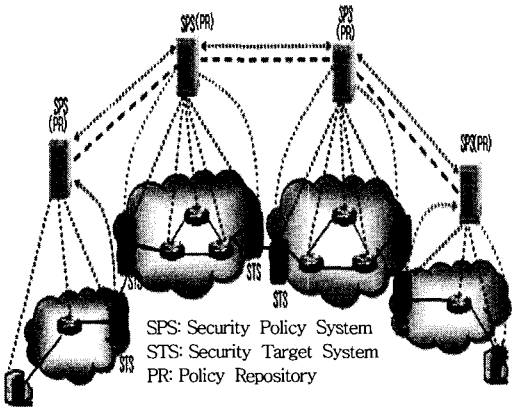


그림 3. 보안정책 관리구조

이 정책 프레임워크에서는 보안정책시스템은 정책서버, 정책저장소로 구성되고 그리고 보안대상시스템은 정책대상의 기능 구성요소를 가진다. 정책서버는 크게 정책관리도구 및 정책 결정기능으로 구성되며 정책저장소는 정책서버와 독립적인 시스템으로 존재할 수도 있다. 또한 정책대상은 정책을 실행하는 네트워크 시스템으로 자원관리관점에서는 경계라우터가 이에 해당된다.

3.2.3 계층적인 침입분석기법

보안에 관한 분석 장비들의 개별관리와 이들 간의 연동이 불가능함으로 네트워크 관리자들은 통합 관리의 어려움을 가지게 되고 보안시스템의 운용에 한계를 보이게 된다. 개별 보안 장비들은 단일 시스템 수준에서의 단면적인 침입분석을 수행하므로 네트워크 차원의 종합적인 침입분석과 예측을 수행할 수 없는 문제점을 가지게 된다.

이러한 문제를 해결하기위해서 보안장비의 분석과 이의 이벤트 정보와 경보정보를 기반으로 하여 네트워크 전반에 걸친 분석을 수행하도록 단순분석과 통계적 분석으로 이루어진 계층적인 분석기법을 사용한다. 계층적인 침입분석은 정책 도메인 내에서 발생하는 모든 보안 이벤트정보를 수집하고 체계적인 관리를 통하여 전체 정책 도메인에 따른 보안상황의 분석을 수행함으로 종합적인 네트워크보안관리 프레임워크를 구축할 수 있다.

그림 4는 제안된 계층적 침입분석 및 대응구조를 나타낸다. 망의 인입점에 위치하는 보안 노드는 시그너처 기반의 침입탐지를 수행하는 비교분석과 트래픽 변화 유형을 모니터하는 관측분석을 통한 하위계층 침입분석을 수행한다 하위계층 침입분석의 결과를 기반으로 보안 노드에서 실시간 대응을 하거나 상위계층의 보안정책서버로 경보 정보를 전달함으로써 상위계층 침입 예측을 가능하게 한다.

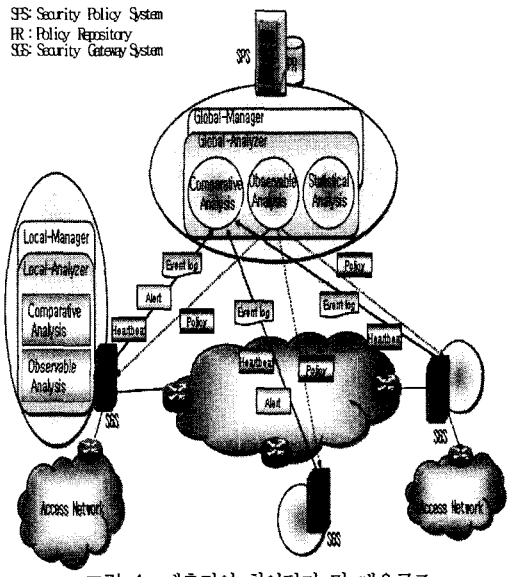


그림 4. 계층적인 침입탐지 및 대응구조

네트워크 전체의 보안관련 정보를 수집하고 관리하는 보안정책서버는 통계적 데이터를 기반으로 유사성 분석, 잠재성 분석과 침입 가능성 분석을 통하여 상위계층에서 침입 예측을 수행한다. 이를 토대로 네트워크 내에 적용한 대응정책을 결정하거나 침입의 징후에 대한 정보를 인접 도메인과의 통신을 통해 공유하므로 글로벌 네트워크 차원의 침입에 대한 대응을 협력할 수 있는 체계를 구축할 수 있다.

네트워크 보안에서 현재 가장 심각한 문제를 유발하는 것이 DDoS(Distributed Denial of Service) 공격이다. 그것은 DDoS가 사전에 예측하기가 힘들고 정상적인 트래픽과 식별하기가 어려우며 그 피해규모가 네트워크 전역에 걸쳐 매우 크기 때문이다. 또한 과다한 트래픽을 네트워크에 유입시켜 네트워크 자원을 고갈시켜 대역폭을 소모시키는 공격형태로 발전되고 있어 네트워크 보안 측면과 관리 측면에서 매우 심각한 문제를 유발시키고 있다. 계층적인 침입탐지와 종합적인 분석은 하위의 정책대상(SGS)과 상위의 정책

서버 간 계층적이고 상호연동적인 통합분석 기법을 제공한다. 그러므로 현실적으로 DDoS 공격을 완전히 예측하고 대응할 수는 없어도 네트워크 인입점에서 유입되는 트래픽의 상태 변화를 자동으로 감지하여 조기에 대응함으로서 피해를 최소화 할 수 있는 구조라고 판단된다.

Ⅳ. 모델링 및 시뮬레이터 구현

보안 노드와 분산 시스템에 대한 분석을 기반으로 본 장에서는 성능 평가를 수행하기위해 시스템을 모델링하고 시뮬레이터를 구현한다.

4.1 보안 노드

보안 노드의 성능을 평가하기위해서 기가비트 침입탐지시스템인 보안 노드의 성능을 저하시킬 수 있는 요소를 분석할 필요가 있다. 보안 노드는 하드웨어 기반의 시그너처 탐지를 고속으로 수행하여 경보를 생성하지만 생성한 경보들의 신속한 대응에 관한 소프트웨어적인 처리로 인하여 기가급만큼 침입탐지시스템의 성능을 향상시키지 못하여 하드에어와 소프트웨어의 인터페이스 부분이 병목점으로 작용할 것으로 예상된다. 따라서 본 논문에서는 보안 노드에 관한 분석을 토대로 성능을 평가하기위해서 시스템을 모델링하고 시뮬레이터를 구현한다.

4.1.1 모델링

보안 노드는 하드웨어기반에서 고속으로 모든 이벤트를 탐지하여 생성하는 경보를 대응능력에 따라 성능을 평가하도록 모델링 하였다. 그림 5는 5개의 보안엔진에서 경보를 생성하여 주 프로세스의 대응능력에 따라 처리하는 평가 모델을 보여준다.

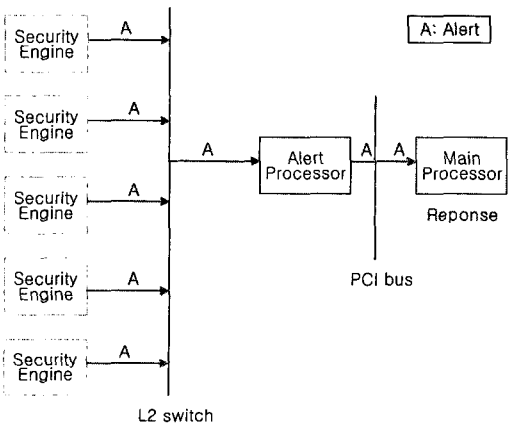


그림 5. 경보 평가 모델

4.1.2 경보 도착 프로세스 모델링

경보 도착 프로세스 모델링을 위해 포아송 프로세스의 이산 모델인 랜덤 프로세스 모델을 이용하였다. 랜덤 프로세스는 베르눌리(Bernoulli) 프로세스에 의해 표현된다. 또한 버스티니스(burstiness)의 영향을 분석하기위해서 IPP(Interrupted Poisson Process)의 이산 모델인 IBP(Interrupted Bernoulli Process) 모델을 사용하였다[14].

(1) 랜덤 프로세스

베르눌리 프로세스에서 각 슬롯에서의 도착확률은 각 슬롯 사이가 독립적으로 p이다. 그림 6에서는 랜덤 프로세스 모델에서의 시간 슬롯(time slot)을 보여주고 있다.

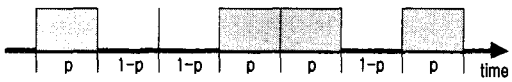


그림 6. 랜덤 프로세스 모델에서의 시간 슬롯

(2) 버스티 프로세스

지수분포를 가지는 ON(active period) 상태와 또 하나의 다른 독립적인 지수분포를 가지는 OFF(silent period) 상태가 교대로 나타나는 포와송 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 7은 버스티 프로세스 모델에서의 시간 슬롯을 보여준다. 본 논문에서는 α값을 1로 가정하였다.

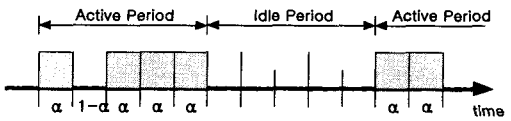


그림 7. 버스티 프로세스 모델에서의 시간 슬롯

IBP 프로세스의 전이 확률(transition probability)

행렬은 식(1)과 같이 주어진다.

$$\rho = \frac{1-q}{2-p-q} \quad (1)$$

πA, πI를 각각 활동 및 휴지 상태의 정상 상태(Steady State)확률로 정의하면 정상상태 방정식 πP = π로부터 다음과 같은 식 (2)을 구할 수 있다.

$$\pi_A = \frac{1-q}{2-p-q}, \quad \pi_I = \frac{1-p}{2-p-q} \quad (2)$$

πA 는 평균 대역폭 혹은 평균 도착률(λ)이다.

d를 연속적인 경보들간의 도착간 시간이라 하고, d1을 휴지 슬롯의 어느 슬롯에서 다음 도착 시간까지의 시간 간격이라 한다면 도착간 시간의 제곱 변화계수(squared coefficient of variation of interarrival times) C2를 식 (3)과 같이 구할 수 있다.

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

본 논문에서는 파라미터 C2를 군집성(burstiness)의 척도로 사용한다.

4.1.3 경보 도착 프로세스 구현

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

(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.

(2) 버스티 프로세스 모델

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

4.2 분산 침입탐지시스템

그림 8은 호스트 기반과 네트워크 기반 그리고 분산 침입탐지시스템과 중앙 집중 형태의 침입탐지시스템 관리 구조를 보여주는 전역적인 네트워크 보안관리 프레임워크이다.

4.2.1 제안된 모델

혼합형 침입탐지시스템을 위한 제안된 모델에서는 전역적인 침입탐지를 수행하기 위해서 IETF 정책 프레임워크를 기반으로 분석기, 지역적인 도메인 그리고 보안정책 서버로 구성되는 전역적인 도메인의 계층적인 구조를 가지고 있다. 가장 하위의 분석기는 각 도메인에서 다양한 형태의 침입을 탐지하는 에이전트들로 구성되어 있고 각 에이전트들은 그들의 특정한 탐지정보를 상위의 지역적인 도메인 매니저에게 보고한다. 에이전트들로 구성된 분석기에서는 수립된 보안정책을 기반으로 침입을 분석한다[15][16].

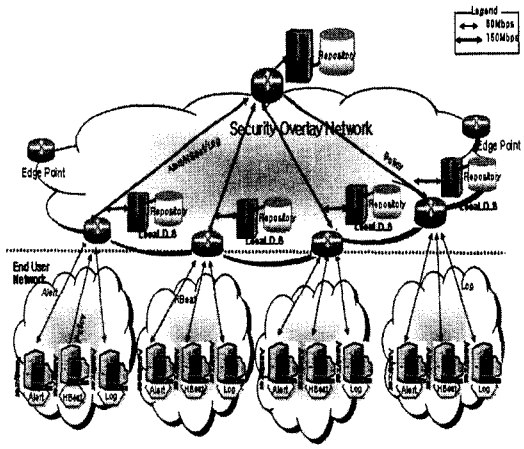


그림 8. 다중 도메인 환경에서 제안된 혼합형 IDS 모델

분석기에는 다양한 침입을 탐지하는 에이전트들이 있다. 네트워크 기반 침입을 분석하여 경보를 발행하는 에이전트, 분석기의 현재 상태정보를 정기적으로 상위의 매니저에게 보고하는 에이전트 그리고 호스트 기반 로그를 바탕으로 정보를 전달하는 에이전트들이 있다. 각 분석기는 경보와 로그에 관한 메시지를 비동기적으로 그리고 분석기의 상태정보는 정기적으로 상위의 매니저에게 보고 하도록 하였다. 상위의 매니저는 보고받은 침입 탐지정보들을 분석하고 최상위의 전역적인 도메인으로 보고한 후 그들의 정보를 저장

소에 기록한다. 최상위의 전역적인 도메인 매니저는 보고 받은 탐지정보를 기반으로 보안정책 서버를 통한 전역적인 보안정책을 수립 한 후 보안정책을 하위의 노드들에게 하달한다.

본 논문에서 제안한 통신 모델은 각 에이전트에서 독립적인 침입 탐지를 수행한다는 측면에서 분산 침입탐지라 할 수 있으며, 지역 도메인으로부터 경보나 다른 중요한 이벤트 데이터를 상위의 전역 매니저로 전송하여, 대규모 분산 시스템에서의 침입탐지시스템 사이의 정보 교환을 허용하는 구조를 취하고 있다는 것이 특징이다.

V. 성능 평가

5.1 보안 노드

본 장에서는 네트워크 차원의 종합적인 보안관리를 가능하게 하기위하여 보안 노드 레벨과 분산 시스템 레벨, 두 가지 단계에서 성능평가를 수행한다. 먼저 보안 노드 레벨에서는 고속 보안 노드인 기가비트 침입탐지시스템의 구조 분석을 토대로 성능 평가를 수행한다.

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 기가 급으로 생성하는 경보에 대하여 정책을 기반으로 신속한 대응을 결정하고 처리하여야한다. 본 절에서는 고속 보안 엔진에서 생성하는 경보의 대응 능력에 관하여 성능 평가를 수행하고자 한다.

5.1.1 성능평가 시나리오

성능평가의 파라미터는 대응에 대한 처리 속도, 경보 정보 전달 율, 버퍼 크기 등을 기준으로 정보 전달 지연과 손실을 평가하였다. 보안 노드의 구조에서 적용할 시나리오는 표 1과 같다.

표 1. 보안 노드 성능평가 시나리오

시나리오	성능 평가 항목
1	경보정보 전송 구조: 기가비트 스위치
2	경보정보 전송 구조: PCI 버스
3	버퍼 크기
4	버스티 크기

성능 평가 모델에서는 5개의 보안 엔진에서 경보를 발생하며 경보 대응능력을 파라미터로 적용하여 평가하였다. 대응능력의 파라미터로는 100Mbps에서 300Mbps까지 적용하였으며, 버퍼의 크기는 1000에서 4000개로 설정하였다.

5.1.2 성능 평가

(1) 기가비트 전송 평가

그림 9는 평가모델의 5개의 보안엔진에서 생성하는 경보의 전체 부하량이 50%에서 90%까지에 대한 기가 비트 스위치를 이용한 전송 성능을 평가한 것이다. 보안 엔진에서 기가 비트 스위치를 이용하여 생성한 경보를 주 프로세서의 대응 능력에 따른 지연 성능을 나타낸다. 경보의 량이 증가할수록 대응 유닛 100Mbps 처리 속도에서 지연이 크게 증가됨을 보여준다.

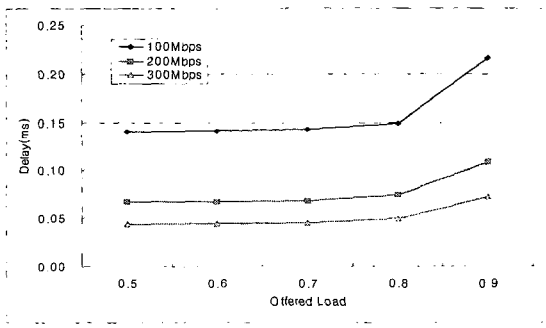


그림 9. 기가비트 스위치를 이용한 경보 지연

(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 전송 결과와 거의 동일한 결과를 도출하였다. 따라서 본 논문에서는 결과를 별도로 제시하지 않았다. 위의 결과들을 분석하여 보면, 경보 정보의 지연 성능은 대응 처리 속도와 가장 밀접하게 연관된 것으로 생각되며, 따라서 대응 프로세싱 속도를 향상시킬 수 있는 방안 연구가 필요하다고 하겠다. 예를 들어, 대응 프로세싱 속도가 Gbps급까지 처리가능하다면 지연과 손실은 거의 발생하지 않는 것으로 모의실험 결과 분석되었다.

(3) 버퍼 크기에 따른 평가

그림 10과 그림 11은 평가모델이 보안엔진에서 생성하는 경보의 전체 부하량이 50%에서 150%까지에 대하여 대응 유닛의 처리 능력 300Mbps에서 기가비

트 스위치를 이용한 전송 시 버퍼 수에 따른 지연과 손실을 나타낸다. 예측된 데로 버퍼의 수가 클수록 지연은 증가하고 손실은 감소하는 일반적인 경향을 보인다. 그러나 그림 9의 지연 특성과 비슷하게, 손실 성능은 버퍼의 영향 보다는 대응 처리 속도에 더욱 의존되는 것을 알 수 있었다. 그러므로 지나친 버퍼 수의 증가는 오히려 네트워크의 성능을 저하시키는 요인으로 작용할 수 있음을 알 수 있다.

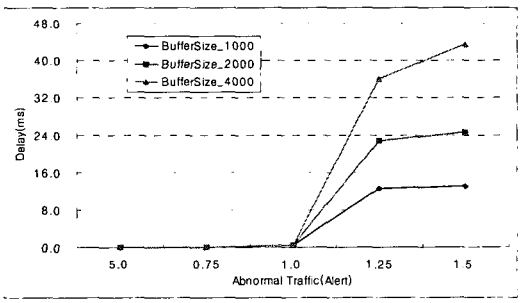


그림 10. 버퍼 크기에 따른 경보 지연

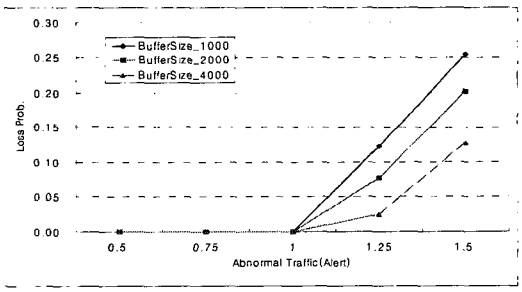


그림 11. 버퍼 크기에 따른 경보 손실

(4) 버스티니스 정도에 따른 전송 평가

그림 12와 13은 평가모델의 보안엔진에서 생성하는 경보의 전체 부하량이 네트워크 용량의 50%에서 90%까지에 대하여 버스티니스(C^2)의 값을 1에서 50까지의 범위에서 기가비트 스위치를 이용한 경보 전송 지연과 손실을 평가한 것이다.

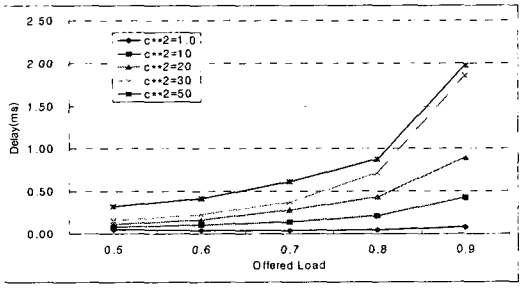


그림 12. 버스티니스 정도에 따른 경보 전송 지연

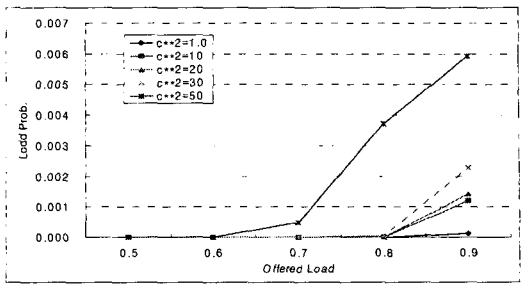


그림 13. 버스티니스 정도에 따른 경보 전송 손실

그림 12와 그림 13은 버스트니스(C^2) 정도에 따라 네트워크 전송에 미치는 영향을 평가한 것으로서 그림 12는 버스티니스가 증가함에 따라 경보 전송 지연이 크게 증가함을 보여준다. 그림 13은 과다한 경보의 생성으로 인한 버퍼의 손실을 나타내며 버스트니스(C^2)의 크기에 따라 손실률이 다르게 증가함을 나타낸다. 특히 버스티니스(C^2)의 정도가 클수록, 경보의 부하가 높아질수록 지연 및 손실이 급격히 증가함을 볼 수 있다.

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

5.1.3 소 결론

본 논문에서는 고속 보안 노드로서 기가비트 침입탐지시스템인 보안 게이트웨이의 개발 시스템을 모델링하여 성능을 평가하였다. 차세대 침입탐지시스템에서의 요구 안은 정확성, 탐지 뿐 만아니라 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 평가를 통해서 도출 되었다.

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

5.2 분산 침입탐지시스템

분산 시스템의 성능 평가에서는 혼합형 IDS의 제안된 모델을 대상으로 개발된 시뮬레이터를 이용하여 성능 모의실험을 통한 결과를 제시하고 분석한다. 에이전트가 탐지한 정보의 보고 및 보안정책 서버의 보안정책 하달은 독립적인 네트워크로 가정하여 모의실험하였다. 평가는 침입을 탐지한 분석기에서 최상위의 전역적인 도메인 보안정책 서버까지 네트워크 차원에서 정보 전달에 따른 성능 분석이다. 성능 분석 파라미터로는 지연(delay)만을 사용하였다. 본 성능 분석에서 사용한 파라미터는 2.5.2절에서 기술된 성능 결정 요인들을 고려하여 결정하였으며, 데이터의 표현 방법과 민감성에 대한 성능 분석은 수행하지 않았다.

5.2.1 성능평가 매개변수

표 2는 본 혼합형 IDS 모델에서 적용한 이벤트별 데이터 크기이다. 시뮬레이터 구현에는 각 노드 이벤트 전송 율은 분석기와 지역적인 도메인 연결은 50Mbps, 전역적인 도메인과의 연결은 150Mbps를 통하여 연결하였으며 각 분석기와 정책 서버에서는 데이터의 스케줄링과 처리를 위하여 유한버퍼를 사용하였다.

표 2. 이벤트별 데이터 크기(단위: 바이트)

이벤트 종류	Alert	HeartBeat	Log 데이터
크기	512	512	440

매개변수별 성능 평가 착안점은 다음과 같다.

표 3. 매개 변수에 따른 성능평가 항목

성능 평가 항목
네트워크 이용률의 영향
이벤트 데이터 형태와 크기의 영향
에이전트 수의 영향
데이터 생성빈도의 영향

5.2.2 성능 평가

(1) 네트워크 이용률의 영향

그림 14와 그림 15는 침입 탐지정보들을 전역적인 도메인 내 보안정책 서버에게 보고 할 때의 각 이벤트의 평균 지연 성능을 나타낸다. 그림 14는 전역적인 도메인과 지역적인 도메인에서 입력 부하의 크기(즉 네트워크 이용률)의 변화에 따른 전송 패킷의 평균 지연을 보여준다. 지연은 이용률 0.7이상에서는 지수적으로 크게 증가하는 것을 볼 수 있다.

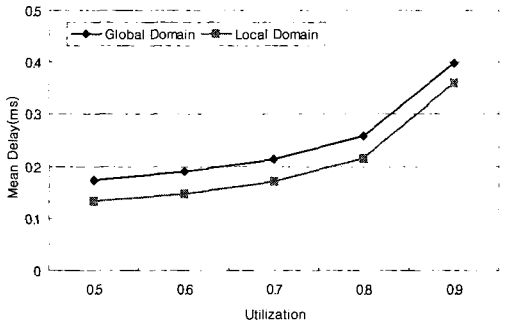


그림 14. 네트워크 이용률에 따른 지연

(2) 이벤트 데이터 형태와 크기의 영향

그림 15는 각 이벤트 종류에 따른 지연 성능을 나타낸다.

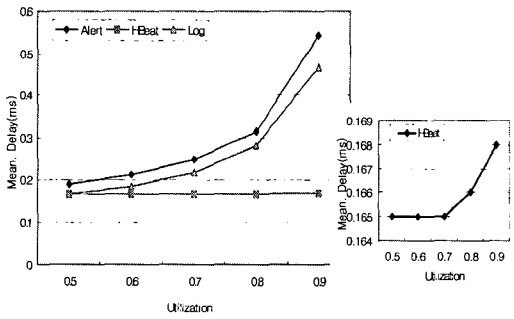


그림 15. 이벤트 종류에 따른 지연

경보와 로그 이벤트는 지연이 이용률에 따라 증가하는 추이를 확연히 보이며 분석기 상태정보는 네트워크의 상태 변화에서도 정기적인 보고가 이루어지므로 가시적인 지연 성능은 이용률에 따라 다른 이벤트 데이터에 비하여 상대적으로 지연 변화가 작은 것으로 분석된다. 그러나 그림 15에서 상태정보를 좀 더 상세하게 분석하여 보면 지연이 미세하게 이용률에 따라 증가함을 보여준다.

(3) 에이전트 수의 영향

전역적인 보안을 위한 분산 침입탐지시스템에서 계위를 통한 통신 메커니즘을 결정하는 요인 중의 하나가 침입을 탐지하는 컴포넌트 수, 즉 에이전트 수이다. 그림 16은 에이전트 수가 증가함에 따라 지연이 증가함을 보여준다. 에이전트 수를 3배, 6배, 12배로 증가시켰을 때 네트워크의 지연 성능이 크게 증가함

을 보여준다.

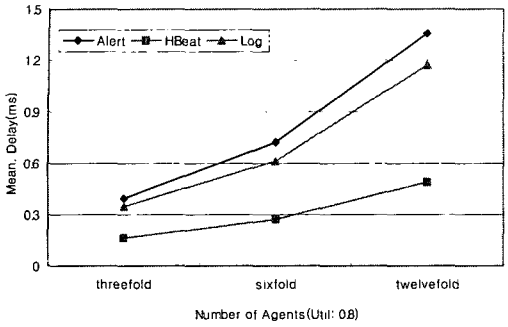


그림 16. 에이전트 수에 따른 지연

(4) 데이터 생성빈도의 영향

이벤트의 발생 빈도가 증가하여 과다한 이벤트의 생성빈도를 가질 때 네트워크 성능에 미치는 영향을 분석하였다. 그림 17은 데이터 생성빈도에 따른 지연 성능을 나타낸다.

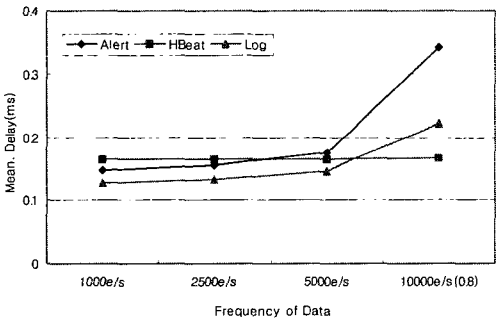


그림 17. 데이터 생성빈도에 따른 지연

분산 서비스 거부 공격 같은 공격이 발생하면 다른 도메인에 존재하는 여러 에이전트들로부터 공격 발생으로 인한 이벤트의 빈도수가 과다하게 생성 될 수 있고 이것은 또한 네트워크 성능에 심대한 영향을 미칠 수 있음을 알 수 있다. 반면에 정기적인 상태정보의 전달 성능은 상대적으로 영향이 작음을 볼 수 있다.

5.2.3 소 결론

개별 시스템 단위의 과대한 트래픽 분석과 다양한 침입 유형에 보다 능동적으로 대응하기 위하여 지역적 보안환경에서 광역적인 보안환경으로 적용하기 위한 글로벌 네트워크 보안제어 프레임워크 기술이 대두되고 있다. 글로벌 네트워크 보안제어 프레임워크에서는 각 지역 망의 출력 트래픽들의 종합 분석과 망의 구성과 상태정보, 관리정보 및 통계정보를 다단계 분석으로 침입을 예측하고, 환경에 적합한 대응정책의 결정이 가능하게 된다. 이를 위하여 고속화 침입탐지 엔진, 전달 정보를 축약하기 위한 기법 및 전달 프로토콜의 개발, 정보를 공유하기 위한 협력 메커니즘의 수립 그리고 종합적인 침입 대응 시나리오 등이 필요하다.

이러한 글로벌 프레임워크에서 컴포넌트 사이의 통신은 전체 시스템 기능성의 한 중요한 부분이다. 컴포넌트들은 통신 메시지를 통하여 시스템의 전반적인 상태를 얻을 수 있기 때문에, 통신의 붕괴는 전체 시스템의 오동작을 유발하거나 실패하게 만들 수 있다. 따라서 네트워크 수준의 혼합형 분산 침입 탐지를 위한 계층적인 통신 모델을 제안하고 제안한 통신 모델을 대상으로 모델링 및 시뮬레이터를 구현하였다. 성능 평가를 위해서 글로벌 프레임워크의 통신 메커니즘을 결정하는 주요 요인인 침입을 탐지하는 컴포넌트의 수, 네트워크 이용률, 이벤트 데이터 형태와 크기 그리고 데이터 생성빈도 등에 대하여 모의실험을 통한 결과를 제시하였다. 따라서 본 논문은 종합적인 네트워크 보안관리를 위한 시스템 설계에 적용 할 수 있을 것으로 사료된다.

VI. 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. 현재의 상용보안제품들은 단면적인 침입탐지를 수행하고 있어 계속적으로 그 형태가 지능화되고 있는 네트워크 차원의 침입에 대한 탐지분석과 신속하고 적극적인 대응은 어려운 실정이다. 또한 기존의 분산 침입탐지시스템인 DIDS, AAFID, EMERALD, 그리고 GrIDS는 단순한 계층적 혹은 중앙 통제 형태로 침입을 분석한다. 따라서 네트워크 수준의 계층적인 분석 문제, 데이터의 정련 문제, 계층의 모든 단계에서 부피가 큰 모듈 보유 및 정적인 상호 작용 등의 단점을 가지고 있다.

이러한 문제들을 해결하기위해서, 본 논문에서는

다중 도메인 환경에서 지역적인 침입탐지를 위한 에이전트들과 전역적인 침입탐지를 위한 집중 데이터 분석 컴포넌트를 가지고 있는 분산 침입탐지를 위한 모델을 제안하였다. 제안한 프레임워크는 각 에이전트에서 독립적인 침입탐지를 수행한다는 측면에서 분산 침입탐지라 말할 수 있으며, 현재의 보안 시스템이 시스템 간의 상호 운용성의 부족으로 대규모 망에서 효과적인 침입탐지를 수행하는데 어려움이 있으므로, 이를 해결하기 위하여 지역 도메인으로부터 경보나 다른 중요한 이벤트 정보를 상위의 전역 매니저로 전송하여, 대규모 분산시스템에서의 침입탐지시스템 사이의 정보 교환을 허용하는 구조를 취하고 있다는 것이 기존 시스템과 다른 점이라 할 수 있다. 또한 보안 관리 프레임워크 구조에 의해 정책 도메인 내에서 발생하는 모든 보안 이벤트 정보를 수집하고 이를 체계적으로 관리하여 정책 도메인에 따른 보안상황을 분석하므로 종합적인 네트워크 보안관리가 가능한 구조를 가지고 있다.

제안된 모델의 성능평가를 수행하기 위하여 보안 노드 레벨과 분산 시스템 레벨에서 각각 시스템을 모델링하고 시뮬레이터를 설계 및 구현하여 모의실험을 수행하였다. 성능 평가에서는 크게 두 가지 수준에서 수행하였다. 먼저 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 메시지 도착 프로세스는 이산적인 트래픽 모델로 일반적인 포와송 모델과 버스티 트래픽 모델인 IPP를 사용하였으며, 이산 모델로는 랜덤 프로세스, 버스티 트래픽 모델인 IBP를 사용하였다. 본 논문에서는 이산 모델에 대한 결과만을 제시하였다. 시뮬레이터 구현에는 OPNET을 이용하였으며 통신시스템의 기능성을 검정할 수 있는 여러 가지 인수들을 사용하여 성능 평가 매개 변수로 이용하였다. 시스템 레벨에서는 제안된 계층적 분산 침입탐지시스템에 대하여 제시된 통신 메커니즘의 결정요인들을 적용하여 성능평가를 수행하였다. 성능 분석 파라미터로는 지연 및 손실 등을 사용하였다.

보안 노드에서 하드웨어 기반의 고속 침입 탐지부에서는 고속의 침입 탐지를 수행하지만 이 탐지 정보를 기반으로 하는 대응 정책 결정부는 소프트웨어 기반의 처리가 이루어지기 때문에 전체적인 보안 노드의 성능이 대응 장치의 대응 처리 능력에 의하여 의존된다는 것이 분석되었다. 시스템의 성능평가에서 먼저 네트워크 이용률에 따른 지연을 분석하였다. 시스템은 60% 부하 수준까지는 좋은 성능을 나타내었고 70% 이상의 부하에서는 지연이 지수적으로 크게 증가하였다. 다음에 이벤트 데이터의 형태와 크기에 대한 영향을 분석하였다. 경보와 로그 이벤트는 지연이 이용률에 따라 확실히 증가하였고, 반면에 정기적인 보고가 이루어지는 상태정보는 상대적으로 지연변화가 작은 것으로 분석되었다. 전역적인 보안을 위한 분산 침입탐지시스템에서 계층을 통한 통신 메커니즘을 결정하는 요인 중의 하나는 침입을 탐지하는 컴포넌트의 수, 즉 에이전트의 수이다. 이에 따라 에이전트 수가 네트워크상의 미치는 영향에 대한 분석을 수행하였으며, 지나친 에이전트 수는 네트워크 성능에 영향을 미치는 것으로 분석되었다. 다음에 이벤트의 발생 빈도에 따른 네트워크의 성능을 분석하였다. 경보와 로그 데이터의 생성 빈도수가 증가함에 따라 과다한 트래픽이 생성되어 네트워크 성능에 심대한 영향을 미칠 수 있음이 분석되었다.

본 논문에서 제시된 분산 시스템은 정책 기반의 계층적인 분석기법을 통해 종합적인 침입탐지와 신속한 대응이 가능하여 네트워크차원의 보안관리와 분산 시스템 설계에 이용 될 수 있을 것이다. 이를 위하여 네트워크 간의 유기적인 협력을 통한 글로벌 대응 체계의 구축과, 네트워크 간 교환 되는 정보보호 관련 정보의 표준화 및 교환 의무화를 위한 방안이 필요하다. 성능 분석 결과는 종합적인 네트워크 보안관리 시스템을 설계하는데 이용될 수 있을 것으로 생각되며, 향후 연구 계획으로는 침입탐지 엔진과 연계하여 침입탐지 성능과 시스템 성능의 통합적인 분석이 있다.

참고 문헌

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

[3] "Introduction to Policy Based Networking & QoS", White Paper, http://www.iphighway.com/

[4] T. Lunt, H. Javitz, and A. Valdes, et al. "A Real-Time Intrusion Detection Expert system(IDES)", SPI Project 6784, *SRI* International Technical Report, February 1992.

[5] The Computer Misuse Detection System. http://www.cmds.net/, 1998

[6] Thomas E. Daniels, Eugene H. Spafford, "Identification of host audit data to detect attacks on low-level IP vulnerabilities", *Journal of Computer Security*, 7(1), pp.3-35, 1999.

[7] Chris Herringshaw, "Detecting Attack on Network", *IEEE Computer Magazine*, pages 16-17, December 1997.

[8] Madalina Baltatu, Antonio Lioy, and Daniele Mazzocchi, "Security Policy System: status and perspective", pp. 278-284. 1999.

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

[10] 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.

[11] 김병구, 김익균, 이종국, 장종수, "고속 침입 탐지 및 대응을 위한 기가비트 침입탐지시스템의 구현", *제8회 COMSW 학술대회 논문집*, pp. 51-55, 2003. 7월.

[12] 장종수, 김기영, 류걸우, "안전한 정보보호 인프라 제공을 위한 글로벌 네트워크 보안제어 프레임워크", *한국통신학회지*, 제19권 8호, pp.1146-1156, 2002년 8월.

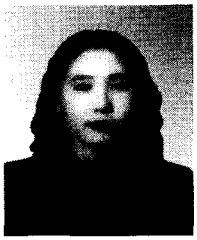
[13] M. Stevens, Policy Framework Internet Draft, draft-ietf-policy-framework-05.txt, Sep. 1999.

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

[15] IP Security Policy, http://www.ietf.org/html.charters/ipsp-charter.html

[16] Diego Martin Zamboni, "Using Internal Sensors for Computer Intrusion Detection", Ph. D. dissertation, Purdue University, *CERIAS* TR 2001-42, August 2001.

장 정 숙 (Jung-Sook Jang)



1989. 3~1991. 2 경일대학교 공과대학 컴퓨터공학과 (공학사)
1992. 8 ~1995. 2 대구가톨릭대학교 교육대학원 전자계산교육전공(석사)
1998.3~2004. 2 현재 대구가톨릭대학교 대학원 컴퓨터·정보통신공학 전공 (이학박사)
2004년 3월~현재 대구가톨릭대학교 컴퓨터정보통신공학부 IT교수
<주관심분야> 네트워크 보안, Active Network, 통신망 성능분석, 고속 통신망 응용 서비스

전 용 희 (Yong-Hee Jeon)

1978년 고려대학교 전기공학과 졸업(공학사)
1985~1987년 미국 플로리다공대 대학원 컴퓨터공학과
1989년 미국 노스캐롤라이나주립대 대학원 Elec. and Comp. Eng. 졸업(공학석사)
1992년 미국 노스캐롤라이나주립대 대학원 Elec. and Comp. Eng. 졸업(공학박사)
1978~1978년 삼성중공업(주) 근무
1978~1985년 한국전력기술(주) 근무
1989~1989년 미국 노스캐롤라이나주립대 Dept of Elec. and Comp. Eng. TA
1989~1992년 미국 노스캐롤라이나주립대 부설 CCSP(Center For Comm. & Signal Processing) RA
1992~1994년 한국전자통신연구원 광대역통신망연구부 선임 연구원
1994~현재 대구가톨릭대학교 컴퓨터·정보통신공학부 교수
2001.3~2003.2 동 공과대학장 역임
2001. 3~현재 한국통신학회 학회지 편집 위원
2004. 2~현재 한국전자통신연구원 정보보호연구단 초빙연구원
<주관심분야> 네트워크 보안, 통신망 성능분석, BcN 보안 및 QoS 보장 기술

장 종 수 (Jong-Soo Jang)

1984년 경북대학교 전자공학과 졸업(공학사),
1986년 경북대학교 대학원 전자공학과 졸업 (공학석사),
2000년 충북대학교 대학원 컴퓨터공학과 (공학박사)
1989년 7월~현재 한국전자통신연구원 정보보호연구단 네트워크보안그룹장/책임연구원
<주관심분야> Network Security, Active Network, Biometry

손 승 원 (Seung-Won Sohn)

1984년 경북대학교 전자공학과 졸업 (공학사),
1994년 연세대학교 대학원 전자공학과 졸업 (공학석사),
1999년 충북대학교 대학원 컴퓨터공학과 졸업 (공학박사),
1983년~1986년 삼성전자 연구원
1986년~1991년 LG 전자(주) 중앙연구소 H18mm 캠코더 팀장
1991년~현재 한국전자통신연구원 정보보호연구단 단장/책임연구원
<주관심분야> 네트워크보안, 차세대인터넷, Active Internet