혼합형 침입 탐지 시스템에서 데이터 및 정책 전달 통신 모델과 성능 평가

장 정 숙[†] · 전 용 희[††] · 장 종 수[†††] · 손 승 원[††††]

요 약

침입 탐지 시스템에 대하여 많은 연구 노력들이 진행되고 있다. 그러나 침입 탐지 시스템의 통신 모델과 성능 평가에 대한 작업은 거의 찾아 볼 수 없다. 본 논문에서는 지역적인 침입 탐지를 위한 에이전트들과 전역적인 침입 탐지를 위한 집중 데이터 분석 컴포넌트를 가지고 있는 다중 도메인 환경에서 혼합 침입 탐지를 위한 통신 프레임워크를 제안한다. 또한 전체적인 프레임워크에서 호스트 기반과 네트워크 기반 침입 탐지 시스템의 결합을 가정한다. 지역 도메인에서 경보와 로그 데이터 같은 정보 집합은 상위 레벨로 보고 된다. 계위의 루트에는 데이터 합동을 수행하는 전역 매니저가 있다. 전역 매니저는 침입 탐지 경보의 집합과 상호관련의 결과로 보안 정책을 하위 레벨로 전달하게 된다. 본 논문에서는 혼합 침입 탐지 시스템을 위한 통신 메커니즘을 모델링하고 데이터 및 정책 전달을 위한 전송 능력의 성능 평가를 위하여 OPNET 모델러를 이용한 시뮬레이터를 개발한다. 여러 가지 시나리오에 기반하여 통신 지연에 초점을 두고 모의실험 결과를 제시하고 비교한다.

Communication Models and Performance Evaluation for the Delivery of Data and Policy in a Hybrid-Type Intrusion Detection System

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

ABSTRACT

Much research efforts are being exerted for the study of intrusion detection system(IDS). However little work has been done for the communication models and performance evaluation of the IDS. Here we present a communication framework for doing hybrid intrusion detection in which agents are used for local intrusion detections with a centralized data analysis components for a global intrusion detection at multiple domains environment. We also assume the combination of host-based and network-based intrusion detection systems in the overall framework. From the local domain, a set of information such as alert, and/or log data are reported to the upper level. At the root of the hierarchy, there is a global manager where data coalescing is performed. The global manager delivers a security policy to its lower levels as the result of aggregation and correlation of intrusion detection alerts. In this paper, we model the communication mechanisms for the hybrid IDS and develop a simulator using OPNET modeller for the performance evaluation of transmission capabilities for the delivery of data and policy. We present and compare simulation results based on several scenarios focusing on communication delay.

키워드 : 침입탐지시스템(Intrusion Detection System), 통신모델(Communication Model), 성능 평가(Performance Evaluation), 시뮬레이션(Simulation)

1. 서 론

침입 탐지 시스템에 대하여 많은 연구 노력들이 진행되고 있다. 특히 네트워크를 통한 분산 공격의 증가로 인하여 분산 침입 탐지 기술에 대하여 관심이 고조되고 있다. 이에 따라 주된 연구 분야는 집중 및 단일 프레임워크 기반 침입 탐지 시스템에서 분산 시스템 기반 침입 탐지 시스템으로 이동하는 추세이다. 분산 침입 탐지 시스템은 데이터의 분석이 감시되는 호스트 수에 비례하여 다수의 위치에서 수행되며, 분석(analysis) 컴포넌트가 감시되는 호스트 수에 비례하고, 위치가 분산되어야 한다[1]. 침입 탐지 시스템은 최근에 네트워크 보안을 위하여 아주 중요한 기술로 그 중요성이 점차 증대될 것으로 기대된다[2-4].

또한 복잡해지고 대형화되는 네트워크 관리를 위해 정책 기반 네트워크의 구조가 필요하다. 정책(policy)이란 다른 조건에서 네트워크의 행위를 제어하는 일련의 규칙을 의미한다. 침입 탐지를 위한 보안정책은 보호되어야 할 정보 자산, 필요한 침입 탐지 시스템(IDS : intrusion detection system)의 형태, IDS의 위치, IDS가 탐지할 공격의 유형, 특정

† 준 회 원 : 대구가톨릭대학교 대학원 컴퓨터 · 정보통신공학부
†† 종신회원 : 대구가톨릭대학교 컴퓨터 · 정보통신공학부 교수
††† 정 회 원 : 한국전자통신연구원 정보보호연구본부 네트워크보안연구부 보안게이트웨이연구팀 팀장/책임연구원
†††† 정 회 원 : 한국전자통신연구원 정보보호연구본부 네트워크보안연구부 부장/책임연구원
논문접수 : 2003년 7월 22일, 심사완료 : 2003년 10월 10일

공격이 식별되었을 때 제공될 대응 혹은 경보의 형태를 정의한다. 보안 정책 시스템의 5가지의 기본적인 컴포넌트는 정책 서버, 정책 클라이언트, 보안 정책 프로토콜, 보안 게이트웨이 및 데이터베이스로 구성된다.

분산 침입 탐지 시스템에 대한 연구가 세계적으로 많이 진행되고 있지만, 국내에서는 아직 분산 침입 탐지 시스템 컴포넌트 사이의 통신 메커니즘과 일반적인 통신 모델에 대하여 발표된 연구 결과는 거의 찾아 볼 수 없다. 더구나 침입 탐지 시스템의 통신 모델과 성능 평가에 대한 작업은 없는 실정이다. 기존의 침입 탐지 시스템에서는 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.

본 논문에서는 다중 도메인 환경에서 지역적인 침입 탐지를 위한 에이전트들과 전역적인 침입 탐지를 위한 집중 데이터 분석 컴포넌트를 가지고 있는 혼합형 침입 탐지를 위한 프레임워크를 제안한다. 또한 전체적인 프레임워크에서 호스트 기반과 네트워크 기반 침입 탐지 시스템의 결합을 가정한다. 지역 도메인에서 경보와 로그 데이터 같은 정보 집합은 상위 레벨로 보고 된다. 계위의 루트에는 데이터의 상호 관련과 합동을 수행하는 전역 매니저가 있다. 전역 매니저는 침입 탐지 경보의 집합과 상호관련의 결과로 보안 정책을 하위 레벨로 전달하게 된다. 우리의 접근은 다른 상황에서 에이전트들이 계층적 통신 프레임워크 혹은 직접 연결을 통하여 협동하도록 사용되어지는 것을 제안한다. 특히 혼합 침입 탐지 시스템을 위한 통신 메커니즘을 모델하고 데이터 및 정책 정보의 전송 능력의 성능 평가를 위하여 OPNET 모델러를 이용한 시뮬레이터를 개발한다. 여러 가지 시나리오에 기반하여 통신 지연에 초점을 두고 모의실험 결과를 제시하고 비교한다.

논문의 나머지 구성은 다음과 같다. 제 2장에서는 관련 연구로서 침입 탐지 시스템, 보안 정책 및 침입 탐지 프로토콜, 정보 보고 및 분석의 형태에 대하여 살펴보고, 제 3장에서는 분산 침입 탐지 시스템 통신 프레임워크의 통신 메커니즘, 요구 사항 및 결정 요인에 대하여 분석하고, 제 4장에서는 혼합형 침입 탐지 시스템의 모델을 제안하고 성능 분석 결과를 제시한다. 마지막으로 제 5장에서 결론 및 향후 계획으로 끝을 맺는다.

2. 관련 연구

2.1 침입 탐지 시스템

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 시스템은 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.

호스트-기반 IDS(HIDS : Host-based IDS)는 모니터 될 각 호스트에 상주하는 에이전트를 채택하고 있다. 에이전트는 사건, 시스템 로그, 커널(kernel) 로그, 중요한 시스템 파일과 비인가 된 변경을 조사하는 감사가 가능한 자원이나 의심스러운 활동 패턴 등을 조사한다. 정상적인 것이 아닌 것이 인지될 때, 경보(alert)나 SNMP(Simple Network Management Protocol) 트랩이 자동으로 발생된다. 전통적인 HIDS는 내부자 위협을 탐지하는데 매우 좋고 통상적으로 광범위한 손해 평가와 데이터 수사학(data forensics)을 제공한다. 이 방법의 단점은 중요 시스템 상에 에이전트를 배치해야할 필요가 있고 감사 정책에 면밀한 주의를 기울여야 한다는 필요성이다. 이것으로 인하여 전통적인 HIDS는 IDS 중에서 가장 배치하기 어렵다. 그러나 네트워크 대역폭을 작게 사용하는 특징이 있다.

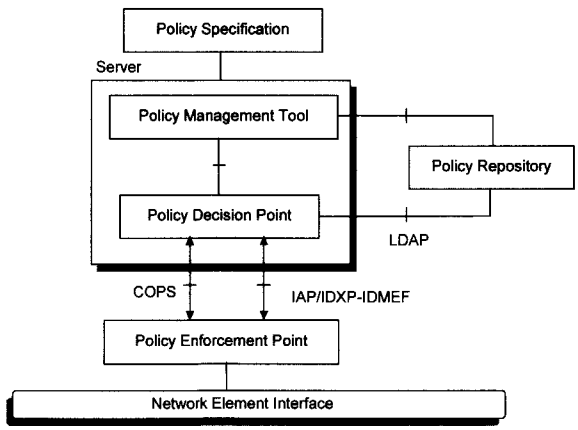
HIDS의 변형된 형태로 집중(centralized) 호스트 기반 침입 탐지가 있다. 이 방법은 분석을 위하여 감시된 파일, 로그 등을 관리자에게 보내어 집중적으로 분석을 한다. 호스트가 만일 침해되더라도 모든 필요한 정보를 관리자에게 보냄으로써 더욱 안전한 면이 있다. 그러나 정보를 전송하는데 많은 대역폭이 필요하다.

네트워크-기반 IDS(NIDS : Network-based IDS)는 네트워크 상의 패킷들을 실시간으로 감시하여 오용 패턴을 탐지한다. 패킷들을 이미 알려진 "침입 시그너처"의 데이터베이스와 대조함으로써 혹은 비정상을 탐지하기 위하여 프로토콜 복호(decode)를 수행하거나, 혹은 둘 다를 수행함으로써 이루어진다. 이 흔적(signature) 데이터베이스는 새로운 공격이 발견될 때마다 정기적으로 갱신된다. 의심스러운 행위가 인지되면, NIDS는 경보를 발생하거나 공격하는 연결을 즉시 종료할 수 있다. 또한 방화벽과 연동하여 공격자를 차단하도록 하기 위한 새로운 규칙을 자동으로 정의할 수 있다.

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 시스템은 중요한 정보와 다른 자원들이 특정한 시스템에서 관리되어 분산되는 방법을 규제하는 법 혹은 규칙을 설정한다. 보안 정책 시스템(SPS : Security Policy System)은 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, 로긴, 경고 혹은 통과 허용 같은 조치를 명시하기 위한 지시와 같은 qualifier를 사용하여 보안 정책을 자동으로 시행하도록 해준다.



(그림 1) 정책 기반 보안 시스템의 컴포넌트

네트워크 운용상의 정책이란 현재 가지고 있는 자원에 대한 모든 정보를 가지고 어떻게 활용할 것인가에 대한 원칙과 계획을 말한다. 분산 네트워크 환경에서 보안 관리를 가능하게 하고 자신의 네트워크에 있는 특정 트래픽에 영향을 미치게 하는 정책기반의 네트워크 관리(PBNM : policy-based network management) 기술 개발이 필요하다. IETF에서의 정책 기반 관리 구조는 정책 관리를 위한 정책관리 도구(PMT : Policy Management Tool), 정책 저장소(Policy Repository), 정책 결정을 위한 Policy Consumer(Policy Decision Point), 정책 적용을 위한 Policy Target(Policy Enforcement Point) 등의 기능적 컴포넌트들을 포함한다((그림 1) 참조).

정책 관리부는 망 운용자 서버의 목적 및 사업자의 목표에 따라 결정된 망운용 규칙을 일관성 있는 정책 데이터로 변환하기 위해서 PFDL(Policy Framework Definition Language)을 이용한다. 망 관리 정책은 정책 저장소에 저장되며, 망 내의 분산되어 있는 정책 결정부(PDP)에 의해 실시간으로 검색되고, 정책 저장소에 수용되는 데이터는 정책을 결정하기 위한 정책 결정조건과 결정된 정책에 따라 적용되어야하는 정책 동작으로 구성된다. 저장된 정책을 조회하거나 생성된 신규 정책을 저장하기 위한 프로토콜로 디렉토리 서비스에 널리 이용되고 있는 Lightweight Directory Access Protocol(LDAP)가 이용된다[5].

보안 정책의 예로는 다음과 같은 것이 있다.

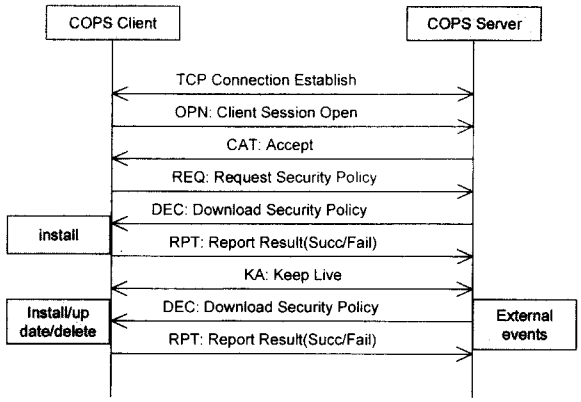
- Detection Policy : 분석기 모듈에서 패킷을 분석하여 침입을 탐지하는 정책
- BlockPoint Policy : 차단 모듈에서 특정패킷을 허용하거나 차단하는 정책
- Sensing Policy : Sensor 모듈에서 특정 패킷만을 센싱하는 정책
- AlertControl Policy : 에이전트 모듈에서 경보메시지의 축약, 결합을 위해 제어하는 정책
- IPsecPolicy : IPsec 설정을 위한 정책

2.3 표준 프로토콜

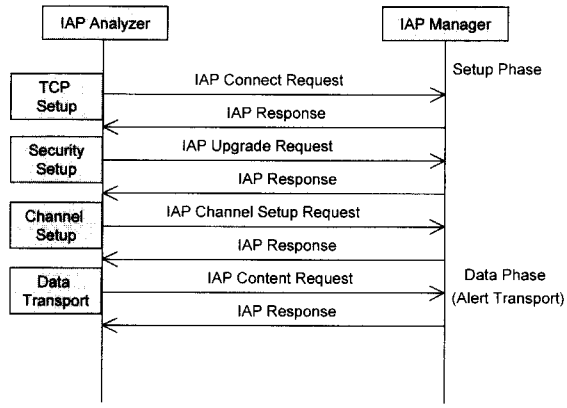
IDS의 표준 프로토콜로는 COPS, IAP/IDXP, SNMP 등이 있으며, 다음과 같은 기능 및 특성을 가지고 있다.

- COPS : IETF의 COPS는 정책 기반 네트워크에서 정책서버(PDP)와 클라이언트(PEP) 사이의 정책정보의 전달을 위한 TCP기반의 간단한 질의/응답 프로토콜이다[6]. 프로토콜 자체 수정 없이 확장을 통한 다양한 클라이언트 타입을 지원한다. COPS는 TCP 기반으로 상위 도메인의 정책 제공 및 통제 목적을 위한 정책 전달 프로토콜이다. COPS는 평균 64KB의 메시지 크기를 채택함으로서 전역적인 보안관리를 위한 적합한 프로토콜이라 할 수 있다.
- IAP(Intrusion Alert Protocol) : IETF의 IDWG에서 침입경보 프로토콜(IAP)을 제안하였다[7]. 침입 탐지 구성 요소들 사이(sensor/analyzer와 managers)에 침입 경보 데이터(Intrusion alert data)를 교환하기 위한 응용 계층의 프로토콜이다. 전달되는 경보는 IDMEF(Intrusion Detection Message Exchange Format)에 명세 되어 있다. 현재 IDMEF의 메시지로는 두 가지가 정의되어 있다 : Alert와 Heartbeat.

(그림 2)는 보안 정책 정보 전달 프로토콜과 경보 전달프로토콜의 동작 시나리오를 보여준다.



(a) 보안 정책 정보 전달 프로토콜



(b) 경보 전달 프로토콜

(그림 2) 보안 정책 및 경보 전달 프로토콜

2.4 정보 보고 및 분석

현재 IDMEF의 메시지로는 두 가지가 정의되어 있다. Alert와 Heartbeat[7].

2.4.1 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.

2.4.2 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.

2.4.3 이벤트 정보

이벤트 스트림의 종류로는 운영 체제 감사 레코드, 네트워크 트래픽, 응용 로그, 시스템 콜 등과 같은 여러 가지 형태가 있다.

현재의 보안 시스템은 시스템간의 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[8].

3. 분산 침입 탐지 시스템 통신 프레임워크

2장에서는 침입 탐지 시스템의 종류와 보안정책, IDS를 위한 표준 프로토콜 및 경보와 이벤트 데이터에 대하여 살펴보았다. 본장에서는 분산 침입 탐지 시스템의 통신 프레임워크에서 요구사항과 성능 결정 요인들에 대하여 기술한다.

분산 침입 탐지 시스템을 구별하는 몇 가지 특징은 다음과 같다[2] :

- 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].

3.1 요구 사항

IDS를 위한 통신 기법에서 바람직한 몇 가지 특징은 다음과 같다[2].

- 신뢰성(reliability) : 잘못된 긍정(false positive)과 잘못된 부정(false negative)을 야기 할 수 있기 때문에 통신 기

법은 신뢰성이 요구된다.

- 보안(security) : IDS 자체가 공격 대상이 될 수 있으므로 통신 메커니즘에 엄격한 보안 특징들을 반영하여야 한다.
- 인증(authentication) : 메시지의 송수신자는 서로의 신원에 대하여 자신감을 가지는 것이 중요하므로 엔티티들 사이에 상호 인증을 필요로 한다.
- 무결성(integrity) : IDS 컴포넌트 사이에서 메시지의 악의 있는 변경을 방지하기 위하여 필요하다.
- 비밀성(confidentiality) : IDS 컴포넌트 사이에 교환되는 메시지는 패스워드, 시스템의 보안 상태 등과 같은 극도로 민감한 정보를 포함하므로 암호 기술을 사용하여 비밀성을 유지하는 것이 중요하다. 이 때 비밀성과 성능 사이의 타협이 이루어져야 한다.
- 부인 봉쇄(non-repudiation) : 통신 프로토콜은 신뢰할 수 있는 방법으로 메시지를 근원지로 태그할 수 있는 메커니즘을 제공해야 한다.
- 비-복제(non-duplication) : 메시지의 추가 및 변경이외에 메시지의 복사도 막아야 한다. 그러므로 이러한 복제 메시지의 탐지는 통신 메커니즘의 바람직한 특성이다.
- 서비스 거부(DOS) 공격에 대한 저항 : IDS에 대한 서비스 거부 공격으로 메시지의 전달을 어렵게 하거나 불가능하게 만들 수 있다.
- 확장성(scalability) : 통신 메커니즘의 확장성은 대규모 네트워크 상에 분산된 IDS의 측면에서 중요하다. IDS 컴포넌트 사이의 통신은 호스트와 네트워크에서의 오버헤드를 심각하게 증가해서는 안 되며, 성능에 최소한의 영향을 미쳐야 한다.
- 속도(speed) : IDS가 실시간(혹은 거의 실시간) 전달을 만족하기 위하여 하부의 통신 메커니즘은 좋은 전송 시간뿐만 아니라 고속의 효율적인 알고리즘을 양단에서 사용하는 것이 요구된다.

3.2 결정 요인

분산 침입 탐지 시스템의 다른 컴포넌트 사이의 통신이 시스템 기능의 중요한 부분이다. 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].

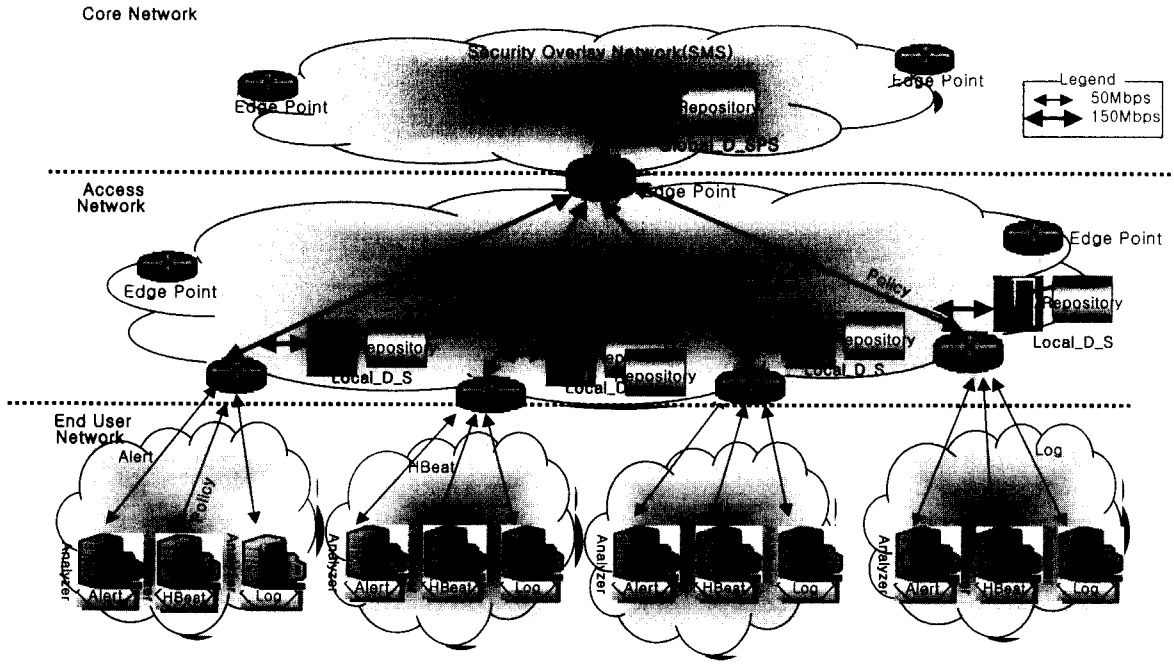
- 컴포넌트의 수 : 컴포넌트의 수에 따라 통신 오버헤드가 증가하는 중요한 요인이 된다.
- 컴포넌트의 위치 : 호스트 내 통신과 호스트 간 통신으로 컴포넌트 사이 통신의 형태가 컴포넌트의 위치에 따라 의존한다.
- 고려되는 데이터의 형태 : 데이터는 원시 감사 트레일, 원시 네트워크 트래픽, 다른 컴포넌트로부터의 축약된 혹은 압축된 감사 혹은 경보(alert)일 수 있다.
- 데이터 양 : 고려되는 데이터의 양이 많다면 수집 컴포넌트 가까이 분석기 컴포넌트를 위치시키는 것이 효율적이다.
- 데이터 생성빈도 : 데이터의 발생빈도가 높으면 비 연결형 메커니즘보다는 연결형 통신 메커니즘을 사용하는 것이 효율적이다. 반면에, 경보와 같이 발생 빈도가 상대적으로 낮은 경우에는, 비 연결형 통신 메커니즘을 사용하는 것이 효율적이다.
- 데이터 표현 방법 : 데이터 표현 방법은 데이터의 크기에 영향을 주며, 이것은 다시 통신 메커니즘의 선택에 영향을 미친다. CIDF와 IDWG는 침입 탐지 시스템들이 정보와 자원을 공유할 수 있도록 데이터 형식과 프로토콜을 표준화하기 위한 노력을 하고 있다. 현재 고려되고 있는 데이터 형식으로는 UML(Unified Modeling Language)과 XML(eXtensible Markup Language)이 있다.
- 데이터의 민감성 : 침입 탐지 시스템의 컴포넌트는 모니터 되고 있는 호스트에 대한 가장 민감한 데이터에 대한 접근을 가진다. 컴포넌트 사이에 그러한 데이터를 교환하기 위하여 사용되는 통신 메커니즘은 안전해야 한다. 통신 메커니즘은 비밀성과 인증을 보증할 필요가 있으며 이것은 시스템의 성능에 영향을 미친다.

4. 혼합형 IDS 통신 모델과 성능평가

4.1 혼합형 IDS 통신 모델

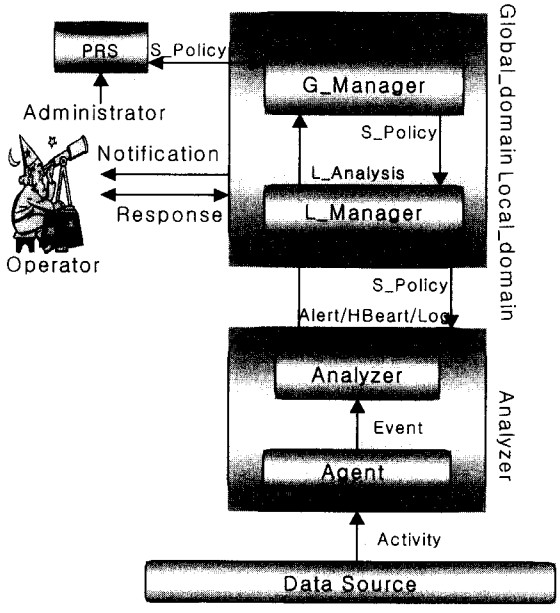
(그림 3)은 호스트 기반과 네트워크 기반 그리고 분산 IDS와 중앙 집중 형태의 IDS 관리 구조를 보여주는 전역적인 네트워크 보안 관리 프레임워크이다.

혼합형 IDS 평가를 위한 모델에서는 전역적인 침입 탐지를 수행하기 위해서 IETF 정책 프레임워크를 기반으로 분석기(analyzer), 지역적인 도메인(local_domain) 그리고 보안 정책 서버(SPS : security policy server)로 구성되는 전역적인 도메인(global_domain)과 같이 계층적인 구조를 가지고 있다. 가장 하위의 분석기는 각 도메인에서 다양한 형태의 침입을 탐지하는 에이전트들로 구성되어 있고 각 에이전트들은 그들의 특정한 탐지 정보를 상위의 지역적인 도메인 매니저에게 보고한다. 에이전트들로 구성된 분석기에서는 수립 된 보안 정책을 기반으로 침입을 분석한다. 분석기에는 다양한 침입을 탐지하는 에이전트들이 있다. 네트워크 기반 침입을 분석하여 경보(alert)를 발행하는 에이전트, 분석기의 현재 상태 정보(heartbeat)를 정기적으로 상위의 매니저에게 보고하는 에이전트 그리고 호스트 기반 로그를 바탕으로 정보를 전달하는 에이전트들이 있다. 각 분석기는 경보와 로그에 관한 메시지를 비동기적으로 그리고 분석기의 상태 정보는 정기적으로 상위의 매니저에게 보고 하도



(그림 3) 다중 도메인 환경에서 혼합형 IDS 평가 모델

록 하였다. 상위의 매니저는 보고받은 침입 탐지 정보들을 분석하고 최상위의 전역적인 도메인으로 보고한 후 그들의 정보를 저장소에 기록한다. 최상위의 전역적인 도메인 매니저는 보고 받은 탐지 정보를 기반으로 보안 정책 서버를 통한 전역적인 보안정책을 수립 한 후 보안 정책을 하위의 노드들에게 하달한다. (그림 4)는 혼합형 IDS 모델의 통신 프로세스를 보여준다.

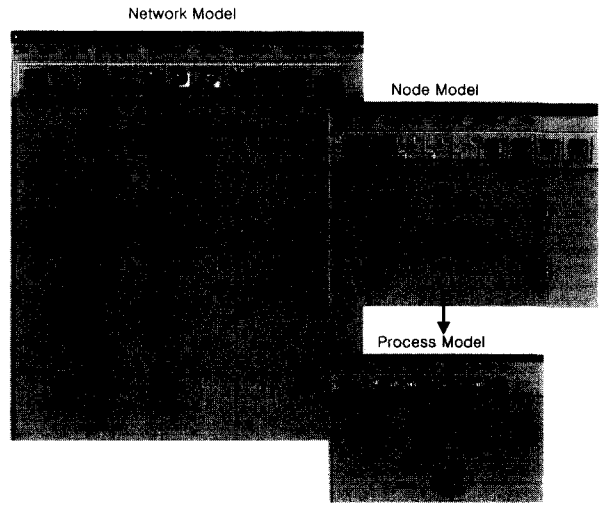


(그림 4) 혼합형 IDS 모델의 통신 프로세스

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

4.2 시뮬레이터 설계와 모델 구현

혼합형 IDS 모델 구현과 성능평가를 위해서 시뮬레이터 설계와 구현에는 OPNET Modeler를 사용하였다. (그림 5)는 구현된 시뮬레이터의 네트워크 모델과 하나의 노드 모델과 프로세스 모델의 예를 보여준다.



(그림 5) 시뮬레이터 구현에서 각 레벨의 모델 예

<표 1>은 본 IDS 평가 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 1〉 이벤트별 데이터 크기

(단위 : 바이트)

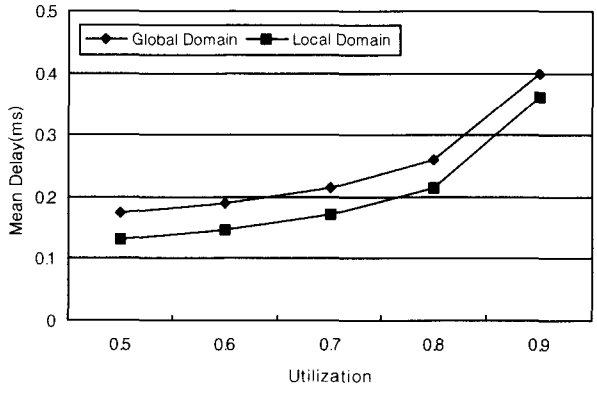
이벤트 종류	Alert	HeartBeat	Log 데이터
크 기	512	512	440

4.3 모의실험 및 성능분석

모의실험과 성능분석에서는 혼합형 IDS 평가모델을 대상으로 개발된 시뮬레이터를 이용하여 성능 모의실험을 통한 결과를 제시하고 분석한다. 에이전트가 탐지한 정보의 보고 및 보안 정책 서버의 보안 정책 하달은 독립적인 네트워크로 가정하여 모의 실험하였으며 성능분석은 두 단계에서 진행하였다. 첫 단계는 침입을 탐지한 분석기에서 최 상위의 전역적인 도메인 보안 정책 서버까지 네트워크 수준에서 정보 전달에 따른 성능 분석이며 두 번째는 보안 정책 서버에서 분석기까지 보안 정책의 하달 성능을 분석한다. 성능 분석 파라미터로는 지연(delay)만을 사용하였다. 본 성능 분석에서 사용한 파라미터는 3.2절에서 기술된 성능 결정 요인들과 일반적인 네트워크 성능 분석 파라미터들을 고려하여 결정하였으며, 데이터의 표현 방법과 민감성에 대한 성능 분석은 수행하지 않았다.

4.3.1 네트워크 이용률의 영향

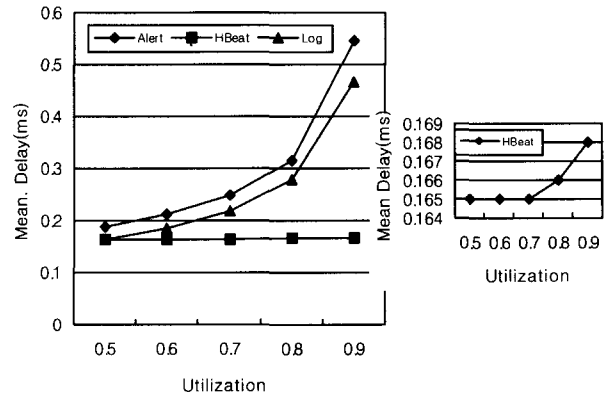
(그림 6)과 (그림 7)은 침입 탐지 정보들을 전역적인 도메인 내 보안 정책 서버에게 보고 할 때의 각기 이벤트의 평균 지연 성능을 나타낸다. (그림 6)은 전역적인 도메인과 지역적인 도메인에서 입력 부하의 크기(즉 네트워크 이용률)의 변화에 따른 전송 패킷의 평균 지연을 보여준다. 지연은 이용률 0.7 이상에서는 지수적으로 크게 증가하는 것을 볼 수 있다.



(그림 6) 네트워크 이용률에 따른 지연

4.3.2 이벤트 데이터 형태와 크기의 영향

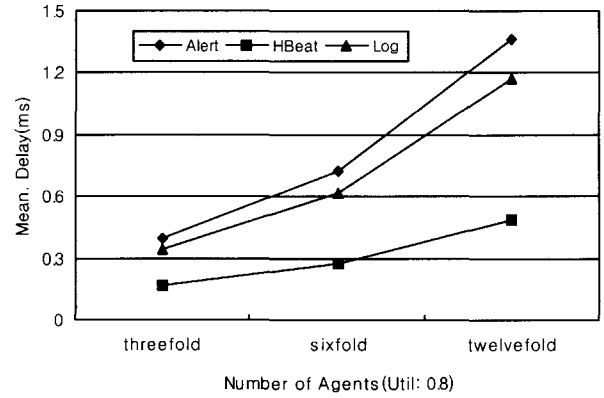
(그림 7)은 각 이벤트 종류에 따른 지연 성능을 나타낸다. 경보와 로그 이벤트는 지연이 이용률에 따라 증가하는 추이를 확연히 보이며 분석기 상태 정보(HeartBeat)는 네트워크의 상태 변화에서도 정기적인 보고가 이루어지므로 가시적인 지연 성능은 이용률에 따라 다른 이벤트 데이터에 비하여 상대적으로 지연 변화가 작은 것으로 분석된다. 그러나 (그림 8)에서 상태정보를 좀 더 상세하게 분석하여 보면 지연이 미세하게 이용률에 따라 증가함을 보여준다.



(그림 7) 이벤트 종류에 따른 지연

4.3.3 에이전트 수의 영향

전역적인 보안을 위한 분산 침입 탐지 시스템에서 계위를 통한 통신 메커니즘을 결정하는 요인 중의 하나가 침입을 탐지하는 컴포넌트 수, 즉 에이전트 수이다. (그림 8)은 에이전트 수가 증가함에 따라 지연이 증가함을 보여준다. 에이전트 수를 3배, 6배, 12배로 증가시켰을 때 네트워크의 지연 성능이 크게 증가함을 보여준다.

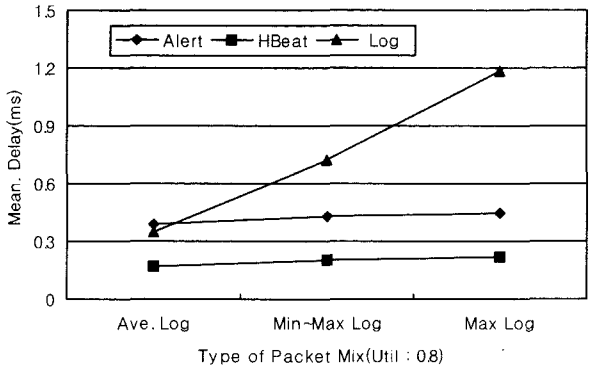


(그림 8) 에이전트 수에 따른 지연

4.3.4 로그 패킷의 영향

(그림 9)는 호스트 기반의 보안 운영 체제 또는 보안 소프트웨어에서 기록한 로그 파일의 특성에 따른 지연을 나타내고 있다. 로그 파일의 특성은 로그 파일의 패킷 크기로 설정하였으며 평균(Ave) 로그 패킷은 440byte, 최소-최대

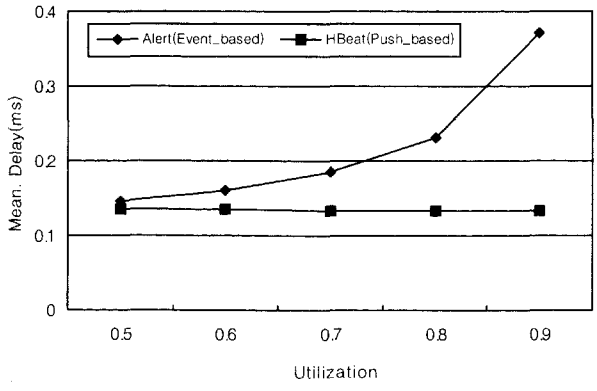
(Min-Max) 로그 패킷의 크기는 각각 64byte와 1518byte로 하고, 균일 분포를 이용하였다. (그림 9)에서 최대(Max)로그 패킷 크기를 사용하여 보고할 때 지연이 가장 크게 나타나고, Min-Max 사이의 균일 분포의 혼합 패킷을 사용하였을 때는 중간, 그리고 단일 평균 크기의 패킷을 사용하였을 때 가장 낮은 지연을 보여준다. 현재 모든 호스트 기반과 네트워크 기반의 도구들은 침입 분석에 대하여 로그 파일을 생성한다. 따라서 네트워크 상의 전송 지연을 감소시키고, 전역 매니저의 처리 부담을 줄이기 위하여 네트워크를 통한 전역적인 보안 관리를 위한 긴요한 로그 정보들에 대한 효율적인 선별과 데이터 감축(data reduction)이 필요한 것으로 사료된다.



(그림 9) 로그 패킷에 따른 지연

4.3.5 푸시 시스템과의 비교

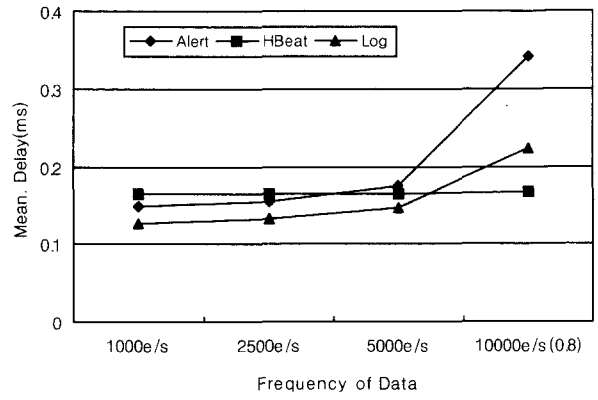
성능분석을 위해서 구현한 시뮬레이터의 가장 하위의 분석기에는 다수의 에이전트들이 있다. 에이전트들이 탐지한 정보를 기반으로 분석기는 경보를 발생시키며 경보는 이벤트가 발생할 때마다 비동기적으로 상위의 도메인(local domain)으로 보고 된다. 현재 분석기의 상태 정보(heartbeat)는 정기적으로 상위의 도메인으로 푸시(push) 된다. (그림 10)은 이벤트 기반과 푸시기반의 따른 성능을 나타낸다. 푸시기반은 이벤트 발생이 증가할수록 상대적으로 지연 증가가 둔화됨을 보여준다.



(그림 10) 푸시 시스템과의 비교

4.3.6 데이터 생성빈도의 영향

이벤트의 발생 빈도가 증가하여 과다한 이벤트의 생성빈도를 가질 때 네트워크 성능에 미치는 영향을 분석하였다. (그림 11)은 데이터 생성빈도에 따른 지연 성능을 나타내며 종단 간 지연을 증가시켜 네트워크 성능에 영향을 미치는 것으로 분석된다. 분산 서비스 거부 공격 같은 공격이 발생하면 다른 도메인에 존재하는 여러 에이전트들로부터 공격 발생으로 인한 이벤트의 빈도수가 과다하게 생성 될 수 있고 네트워크 성능에 심대한 영향을 미칠 수 있음을 알 수 있다. 반면에 정기적인 Heartbeat의 전달 성능은 상대적으로 영향이 작음을 볼 수 있다.



(그림 11) 데이터 생성빈도에 따른 지연

4.3.7 정책 서버의 처리 부하 분석

본 논문에서 모델링한 혼합형 IDS 성능 분석 시뮬레이터는 독립적인 분석 기능을 가진 에이전트들로 구성된 분산 IDS와 중앙 집중 형태의 정책 서버로 구성된 전역적인 네트워크 IDS 보안 관리 구조를 가지고 있다. 분산 IDS의 수가 증가하면 할수록 최상위의 전역적인 도메인의 매니저인 서버의 처리 부하(processing load)가 가중된다. 따라서 지역 도메인의 서버와 최상위 전역 도메인의 정책 서버의 처리 부하를 분석하였다. <표 2>는 지역 도메인과 전역 도메인의 각 서버에서 처리하는 이벤트 수이며 <표 3>은 각 분산 IDS 에이전트들이 분석한 데이터 형태별 이벤트 수를 보여준다.

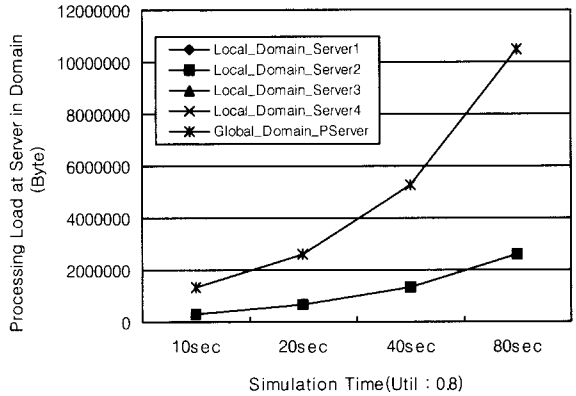
〈표 2〉 혼합형 IDS의 각 서버의 처리 이벤트 수

Domain_Server	10sec	20sec	40sec	80sec
Local_Domain_Server1	328958	658004	1315465	2628211
Local_Domain_Server2	328536	657845	1313659	2627027
Local_Domain_Server3	328903	657060	1312984	2625704
Local_Domain_Server4	328501	656157	1312782	2624628
Global_Domain_PServer	1314898	2629066	5254890	10505570

〈표 3〉 혼합형 IDS의 데이터 형태별 이벤트 수

Event Type	10sec	20sec	40sec	80sec
Alert	415675	831300	1662312	3322491
HBeat	415035	830072	1660152	3320307
Log	484188	967694	1932426	3862772

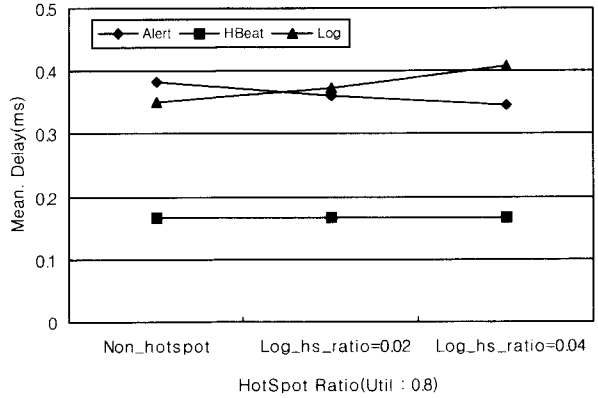
(그림 12)는 <표 2>를 그래프로 표시한 것으로, 보안 정책 서버의 처리 부하의 성능을 보여준다. 각 지역적인 도메인에서 처리하는 부하는 거의 유사한 것으로 나타나며 최상위의 전역적인 도메인 내 정책 서버의 처리 부하는 확연히 증가함을 보여준다.



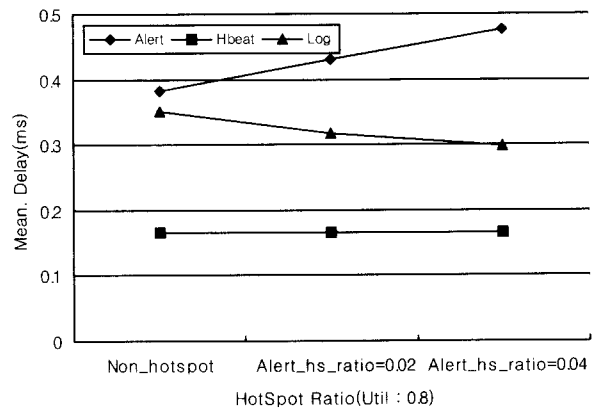
(그림 12) 지역과 전역 매니저의 처리 부하 증가 비교

4.3.8 핫 스폿의 영향 분석

핫 스폿(Hot Spot)이란 특정한 데이터 형태의 이벤트가 집중적으로 발생하는 현상으로 핫 스폿을 이용하여 특정 부분의 네트워크에 미치는 성능을 분석 할 수 있다. (그림 13)과 (그림 14) 각각 로그 데이터와 경보 데이터의 핫 스폿 영향을 보여준다. 전체 네트워크 이용률을 일정하게 유지하고 로그 데이터의 핫 스폿 율이 증가할 할수록, 비 핫 스폿(non-hot spot)인 경보 데이터의 지연은 감소함을 보여준다.



(그림 13) 로그 데이터의 핫 스폿 영향

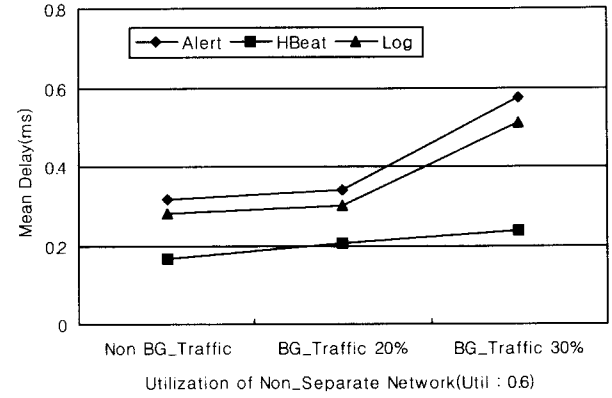


(그림 14) 경보 데이터의 핫 스폿 영향

(그림 14)에서는 경보 데이터의 핫 스폿이 증가할수록 경보 데이터의 지연은 증가하는 반면, 비 핫스폿 데이터인 로그 데이터의 지연 성능은 낮아짐을 또한 나타낸다. 상태 정보 에이전트는 정기적인 이벤트 발생으로 인하여 지연의 변화는 거의 없음을 보여준다.

4.3.9 백그라운드 트래픽의 허용에 따른 영향

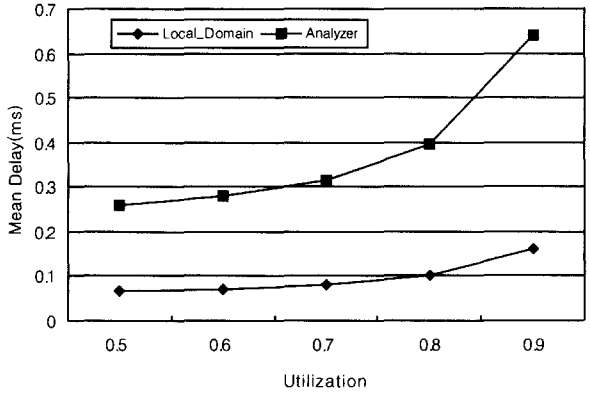
혼합형 IDS의 평가 모델의 성능은 모두 독립적인 네트워크(separate-network)라는 가정 하에 분석하였다. 비 독립 네트워크(non-separate network)는 기존의 네트워크에서 사용하고 있는 트래픽이 있음을 의미하는 것으로 백그라운드 트래픽(background traffic)을 얼마나 사용하고 있느냐에 따른 영향을 분석한 것이다. (그림 15)는 백그라운드 트래픽을 사용하고 있을 경우에 대한 네트워크의 성능을 보여준다. 백그라운드 트래픽율이 증가할수록 상태 정보 데이터를 포함하여 모든 유형의 데이터에 대한 네트워크의 지연이 크게 증가함을 보여준다. IDS 정보를 일반 네트워크 트래픽과 같이 전송할 경우 암호화를 위한 지연도 추가되는 것을 고려하면, 보안 정보 전달을 위한 독립적인 네트워크의 사용이 장점이 많을 것으로 분석된다.



(그림 15) 백그라운드 트래픽의 영향

4.3.10 정책 전달에 따른 영향

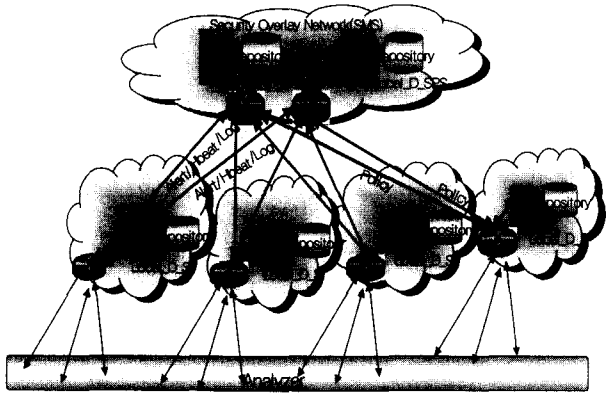
(그림 16)은 전역적인 도메인 내 보안 정책 서버의 정책을 이용률에 따라 지역적인 도메인 내 분석기까지 하달하는 지연 성능을 보여준다. 지역적인 도메인과 분석기 사이 네트워크 수준의 지연 성능이 차이를 나타낸다. 보안 정책 전달을 위한 데이터 크기는 일반적인 크기의 512B를 적용하였다. 이 그림에서 분석기까지의 지연은 이용률 0.7 이상에서 지수적으로 증가함을 알 수 있다.



(그림 16) 정책 전달 지연 성능

4.3.11 결점 감내 구조와 분석

본 논문에서 제시한 혼합형 IDS의 평가 모델은 분산 IDS에서 중앙 집중형태의 보안 정책 서버까지 계층적으로 구성되어 전역적인 보안 관리를 하는 구조이다. 전역적인 도메인 내 정책서버는 단일화로 구성되어있다. 최상위 매니저인 정책 서버의 실패는 곧 모든 보안 정책의 실행이 불가능함을 의미하다. 그러므로 (그림 17)에서처럼 보안 정책 서버의 이원화를 통하여 결점에 적응하는 구조를 설계하고 구현하여 성능을 분석하였다. 각 지연 도메인 분석기에서 보고 받은 탐지 정보들을 지역 도메인 서버에서는 이원화 구조로 이루어진 전역 보안 정책 서버에게 보고하도록 되어있다.



(그림 17) 보안 정책 서버의 이원화 구조

(그림 17)과 같은 결점 감내 구조에서는 각기 다른 연결(link)을 통하여 이원화된 보안 정책 서버에게 정보를 보고한다. 근원지의 분석기 정보들은 주(primary) 보안 정책서버에 보고하고 지역적인 도메인 내 서버에서 복사된 패킷은 백업 보안 정책 서버에게 보고 된다. 주 보안 정책 서버에 도달한 지연 성능은 단일 보안 정책 서버 시스템과 비교했을 때 네트워크의 성능에는 거의 차이가 없음이 분석되었다. 다만 보안 정책 서버의 이원화와 링크 추가에 따른 비용이 추가적으로 필요할 것이다.

4.4 소결론

개별 시스템 단위의 과대한 트래픽 분석과 다양한 침입 유형에 보다 능동적으로 대응하기 위하여 지역적 보안환경에서 광역적인 보안환경으로 적용하기 위한 글로벌 네트워크 보안 제어 프레임워크 기술이 대두되고 있다. 글로벌 네트워크 보안 제어 프레임워크에서는 각 지역 망의 출력 트래픽들의 종합 분석과 망의 구성과 상태정보, 관리정보 및 통계정보를 다단계 분석으로 침입을 예측하고, 환경에 적합한 대응 정책의 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. 본 절에서는 글로벌 프레임워크의 통신 메커니즘을 결정하는 주요 요인인 침입을 탐지하는 컴포넌트의 수, 네트워크 이용률, 이벤트 데이터 형태와 크기 등에 대하여 보안 정책 서버를 포함한 시스템 성능에 대하여 모의실험을 통한 결과를 제시하였다.

5. 결론 및 향후 연구

기존의 분산 침입 탐지 시스템인 DIDS[9], AAFID[1], EMERALD[10], 그리고 GrIDS[11]는 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 가진다. [2]에서는 집중 분석 컴포넌트가 존재하지 않는 분산 침입 탐지를 위한 프레임워크를 제안하였다. 개별 분산된 에이전트에서만 데이터 분석을 수행하고, 에이전트 간 통신은 관심(interest)의 전달을 통하여 이루어진다.

본 논문에서는 다중 도메인 환경에서 지역적인 침입 탐지를 위한 에이전트들과 전역적인 침입 탐지를 위한 집중

데이터 분석 컴포넌트를 가지고 있는 혼합형 침입 탐지를 위한 프레임워크를 제안하였다. 본 논문에서 제안한 프레임워크는 각 에이전트에서 독립적인 침입 탐지를 수행한다는 측면에서 분산 침입 탐지라 말 할 수 있으며, 현재의 보안 시스템이 시스템 간의 상호 운용성의 부족으로 대규모 망에서 효과적인 침입 탐지를 수행하는데 어려움이 있으므로, 이를 해결하기 위하여 지역 도메인으로부터 경보나 다른 중요한 이벤트 정보를 상위의 전역 매니저로 전송하여, 대규모 분산 시스템에서의 침입 탐지 시스템 사이의 정보 교환을 허용하는 구조를 취하고 있다는 것이 지금까지 제안된 구조와 다른 점이라 할 수 있다. 본 논문에서 제시한 계층형 혼합 침입 탐지 시스템은 보안 관리 프레임워크 구조에 의해 정책 도메인 내에서 발생하는 모든 보안 이벤트 정보를 수집하고 이를 체계적으로 관리하여 정책 도메인에 따른 보안 상황을 분석하므로 종합적인 네트워크 보안관리가 가능한 구조이다.

특히 본 논문에서는 제안된 혼합 침입 탐지 시스템을 위한 통신 메커니즘을 모델하고 전송 능력의 성능 평가를 위하여 OPNET 모델러를 이용하여 시뮬레이터를 개발하였다. 다양한 시나리오에 기반하여 통신 지연에 초점을 두고 여러 가지 성능 파라미터를 사용하여 모의실험을 수행하고 성능 분석 결과를 제시하였다. 본 논문에서의 성능 분석 결과는 종합적인 네트워크 보안 관리 시스템을 설계하는데 이용될 수 있을 것으로 생각되며, 향후 침입 탐지 엔진과 연계하여 침입 탐지 성능과 시스템 성능의 통합적인 분석을 수행할 예정이다.

참 고 문 헌

[1] Eugene H. Spafford and Diego Zamboni, "Intrusion detection using autonomous agents," Computer Networks, 34 (4), pp.547-570, October, 2000.

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

[3] http://www.ietf.org/html.charters/ipsp-charter.html.

[4] http://www.ietf.org/html.charters/idwg-charter.html, "Internet Draft".

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

[6] http://www.ietf.org RFC 2748(COPS).

[7] http://www.ietf.org/internet-drafts/draft-ietf-idwg-idmef-xml-10.txt.

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

[9] S. Snapp, J. Brentano and G. Dias et al., "DIDS (Distributed Intrusion Detection System) : motivation, architecture, and an early prototype," In Proceedings of the 14th National Computer Security Conference, October, 1991.

[10] Phillip A. Porras and Peter G. Neumann. "EMERALD : event monitoring enabling responses to anomalous live disturbances," In 1997 National Information Systems Security Conference, Oct., 1997.

[11] S. Staniford-Chen, S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, K. Levitt, C. Wee, R. Yip and D. Zerkle, "GrIDS-a graph based intrusion detection system for large networks," In Proceedings of the 19th National Information Systems Security Conference, September, 1996.

장 정 숙

e-mail : jsukjj@cu.ac.kr

1991년 경일대학교 공과대학 컴퓨터공학과 (학사)

1992년~1995년 대구가톨릭대학교 교육대학원 전자계산교육전공(석사)

1998년~현재 대구가톨릭대학교 대학원 컴퓨터·정보통신공학 전공 박사 수료

관심분야 : 네트워크 보안, Active Network, 통신망 성능분석, 고속 통신망 응용 서비스

전 용 희

e-mail : yhjeon@cu.ac.kr

1978년 고려대학교 전기공학과(공학사)

1985년~1987년 미국 플로리다공대 대학원 컴퓨터공학과

1989년 미국 노스캐롤라이나주립대 대학원 Elec. and Comp. Eng.(공학석사)

1992년 미국 노스캐롤라이나주립대 대학원 Elec. and Comp. Eng.(공학박사)

1978년~1978년 삼성중공업(주) 근무

1978년~1985년 한국전력기술(주) 근무

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

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

1992년~1994년 한국전자통신연구원 광대역통신망연구부 선임연구원

2001년~2003년 대구가톨릭대학교 공과대학장 역임

1994년~현재 대구가톨릭대학교 컴퓨터·정보통신공학부 교수

관심분야 : 네트워크 보안, Active Network, 통신망 성능분석, QoS 보장 기술

장 종 수

e-mail : jsjang@etri.re.kr

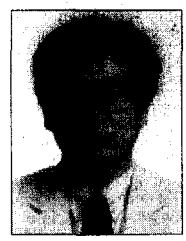
1984년 경북대학교 전자공학과 학사,

1986년 경북대학교 대학원 전자공학과 석사

2000년 충북대학교 대학원 컴퓨터공학과 박사

1989년~현재 한국전자통신연구원 정보보호연구본부 네트워크보안연구부 보안게이트웨이연구팀 팀장/책임연구원

관심분야 : Network Security, Active Network, Biometry



손 승 원

e-mail : swsohn@etri.re.kr

1984년 경북대학교 전자공학과(공학사)

1994년 연세대학교 전자공학과(공학석사)

1999년 충북대학교 컴퓨터공학과(공학박사)

1983년~1986년 삼성전자 연구원

1986년~1991년 LG 전자(주)·중앙연구소 H18mm 캠코더 팀장

1991년~현재 한국전자통신연구원 정보보호연구본부 네트워크보안연구부 부장/책임연구원

관심분야 : 네트워크보안, 차세대인터넷, Active Internet