2001년 한국정보처리학회 춘계 학술발표논문집 제8권 제1호

# 분산 에이전트 침입 탐지 시스템의 성능 평가

정종근*, 김용호*, 박찬호**, 이윤배*
*조선대학교 전자계산학과

# Performance Evaluation of Intrusion Detection System with Attributed Agent

Jong Geun Jeong*, Young ho Kim*, Chan Ho Park**, Yun Bae Lee*
*Dept of Computer Science Chosun University, **Chosun College of Science & Technology

**요 약**

최근 세계적으로 유수한 인터넷 사이트들의 해킹으로 인해 네트워크 보안의 중요성이 강조되고 있다. 네트워크 보안을 위해 방화벽보다는 좀 더 신뢰성이 높은 네트워크 및 시스템에 대한 보안 솔루션으로 침입 탐지 시스템(Intrusion Detection System)이 차세대 보안 솔루션으로 부각되고 있다. 본 논문에서는 기존의 IDS의 단점이었던 호스트 레벨에서 확장된 분산환경에서의 실시간 침입 탐지는 물론 이기종간의 시스템에서도 탐지가 가능한 새로운 IDS 모델을 제안· 설계하였다. 그리고, 프로토타입을 구현하여 그 타당성을 검증하였다. 이를 위해 서로 다른 이기종에서 분산 침입 탐지에 필요한 감사 파일을 자동적으로 추출하기 위해서 패턴 추출 에이전트를 이용하였다.

## 1. 서론

최근 Yahoo, Amazon, CNN 등의 유명 사이트들이 해커의 침입을 받아 서비스를 중단하는 사건이 발생하기도 하였다. 따라서, 인터넷을 통한 전자 거래에 있어서 내부 정보의 보호는 필수적이며, 새로운 시스템 보호 메카니즘이 필요하다. 현재까지는 방화벽만으로도 외부에서의 공격을 어느 정도 차단 할 수 있으나 내부적인 불법행위는 방어할 수 없다. 따라서 외부에서 침입하는 행위는 물론 내부 사용자의 불법적인 행위까지 실시간적으로 감시할 수 있는 침입 탐지 시스템에 대한 연구가 활발히 진행되고있다. 대부분의 인터넷 사이트들이나 내부 네트워크들은 단일 호스트가 아닌 분산 환경으로 되어 있기 때문에 단일 호스트에 대한 침입 탐지 방법은 효과를 거두기 어렵다.

따라서, 본 논문에서는 시스템 내에서 불법적인 행위를 하는 침입자들의 패턴을 추출하여 분석하는 에이전트를 이용하여 분산 환경에서의 다중 호스트 기반의 실시간 침입 탐지 시스템 모델을 제안한다.

## 2.침입 탐지 시스템의 기술적 분류

### 2.1 침입 탐지 시스템의 분류

침입 탐지 시스템은 외부의 침입자 뿐만 아니라 내부 사용자의 불법적인 오남용, 오용 행위등을 탐지하는데 목적이 있으며, 미국 COAST(Computer Operations Audit and Security Technology)의 분류에 따라 데이터 소스(source)를 기반으로 하는 분류 방법과 침입 모델을 기반으로 하는 분류 방법으로 나눌 수 있다. 데이터 소스를 기반으로 분류하는 방법은 단일 호스트로부터 생성되어 수집된 감사 데이터(Audit Data)를 침입 탐지에 이용하는 단일 호스트 기반(SingleOHost Based)과 여러 호스트들로부터 생성되고 수집된 감사데이터를 침입 탐지에 이용하는 다중 호스트 기반(Multi-Host Based), 그리고 네트워크 상에서 수집된 패킷 데이터들을 모아 침입 탐지에 사용하는 네트워크 기반(Network Based)로 나눌 수 있다. 침입 모델을 기반으로 하는 분류 방법은 정상적인 시스템 내에서의 사용자가 정상행위에서 벗어나 행위들을 탐지해 내는 비정상 탐지(Anomaly Detection)와 시스템의 알려진 취약점이나 버그 등을 통해 침입하는 행위를 탐지하는 오용탐지(Misuse Detection)로 구분할 수 있다[1].

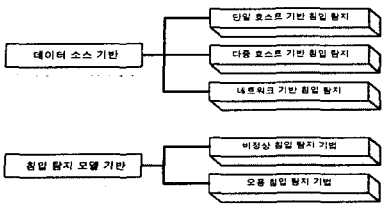


그림1. 침입 탐지 시스템의 분류

### 2.2 침입 탐지 시스템 기술 분석

침입 탐지 시스템을 구현하는 방법은 다음과 같이 크게 세 가지로 분류할 수 있다.

- 실시간 침입 감시 및 분석 기술
- 실시간 패킷 수집 및 분석 기술
- 사후 감사 분석에 의한 분석 기술

실시간 침입 감시 기술은 허가 받지 않은 파일에 대한 임의적 접근이나 변경, 로그인(login) 프로그램의 변경 등을 탐지해 낸다. 실시간 침입 탐지를 위한 효과적인 방법은 네트워크를 구성하는 여러 가지 시스템과 장치에서 발생하는 불법적인 행위들을 실시간적으로 모니터링하고 조치를 취해야 한다. 대부분의 행위 모니터링은 운영체제(OS)에서 제공해주는 감사 자료(audit data)를 활용한다. 반면에 다각도에서 탐지해 내기 위해서는 Webserver, Router, Firewall, TCP/UDP port의 활성화 등에 의한 감사 자료들을 이용해야 한다.

실시간 침입 감시는 침입자가 대부분 관리자 권한을 획득하려고 하기 때문에, 이러한 행위가 감지되면 즉각적인 조치를 취하게 함으로써 시스템의 피해를 줄일 수 있다.

실시간 침입 탐지 기술은 단일 호스트 침입 탐지와 다중 호스트 침입 탐지로 나눌 수 있는데, 단일 호스트 침입 탐지는 오직 한 시스템에서만 작동하므로 오늘날과 같은 멀티 플랫폼 환경에는 적합하지 않다[2].

그리고, 다중 호스트 침입 탐지 방법은 전체 네트워크와 시스템을 에이전트로 인식하여, 분산된 환경에서 감사 자료를 수집, 분석하여 침입을 탐지한다. 이때 에이전트의 역할은 네트워크로 연결되어 있는 다중 호스트에 설치되어 감사 자료의 수집, 추출 등의 일을 담당하게 된다.

## 3. 실시간 패턴 추출 에이전트를 이용한 자동침입 탐지 시스템 설계

### 3.1 제안된 시스템의 구조

에이전트는 분산 환경하에서 네트워크나 시스템의 상태를 감시하기에 가장 적합한 시스템이다. 특히, 실시간 침입 탐지 시스템에서는 침입 정보에 대한 학습이 자동으로 이루어져야 하기 때문에 에어전트를 이용한 침입 탐지 시스템이

가장 이상적이다. (그림2)는 자동 패턴 추출 에이전트(A design of Automatic Intrusion Detection System using real-time Pattern Extracting Agent ; AIDSPEA)의 구조를 보여주고 있다. 본 논문에서는 과거의 침입 유형에 대한 학습뿐만 아니라 새로운 침입 패턴을 감지하고 학습하기 위한 자동 패턴 추출 에이전트를 제안한다. 에이전트 구조는 (그림3)에서와 같이 크게 4부분 즉, 인터페이스 에이전트, 패턴 추출 에이전트, 프로파일 수집 에이전트와 프로세스 감사 에이전트 등으로 나눌 수 있다.

인터페이스 에이전트는 침입 탐지 서버에서 만들어진

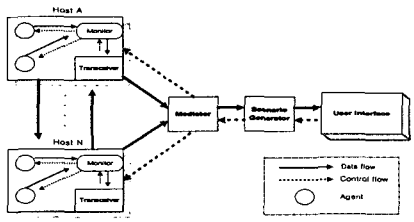


그림2. 제안된 패턴 추출 에이전트 침입 탐지 시스템 모델

탐지 시나리오등을 전송하거나, 각 대상 호스트에 맞는 환경 설정등을 할 수 있는 곳이다. 패턴 추출 에이전트는 프로파일 수집 에이전트에서 수집된 감사 자료로부터 침입 탐지서버의 시나리오에서 필요로 하는 감사 자료만을 추출하는 역할을 담당한다. 이때 수집된 감사자료는 침입 탐지 서비에게 다시 전송하게 되며, 새로운 패턴을 수집 했을 경우 패턴 데이터베이스에 저장한다. 프로파일 수집 에이전트와 프로세스 감사 에이전트는 실제 대상 호스트에서 발생하는 이벤트, 즉, CPU 사용시간, 로그인 실패 ID, 특정 포트 접근 시도 등의 감사 데이터를 커널로부터 수집하는 역할을 한다. 특히, 인터페이스 에이전트는 침입 탐지 시스템의 시나리오를 수신 받아 패턴 추출 에이전트에게 사용자에 현재 프로파일과 프로세스에 대한 정보를 수집하라는 명령을 내린다.

이때 대상 시스템이 이종간일 경우 감사 파일의 포맷(format)에 문제가 생긴다. 본 논문에서는 이러한 문제를 해결하기 위해 추출된 감사 파일의 표준화 방식을 채택하였다. 패턴 추출 에이전트로 이동한 감사 파일들은 로그생성기

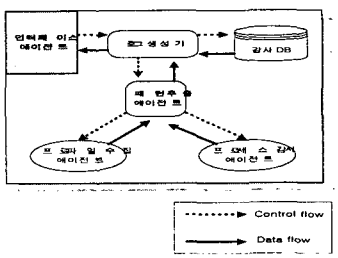


그림3. 자동 패턴 추출 에이전트 구조

(Log Generator)에서 표준화된 포맷으로 재생성된다.

### 3.2 로그 감사 데이터 표준화

이전까지 연구되어온 침입 탐지 시스템의 감사 데이터 기법은 시스템 의존적인 특성을 지니고 있어 이종의 환경을 지원하기에 적합하지 않았다. 따라서 본 연구에서는 로그 데이터 분석기에서 각각의 시나리오에서 수집되어 분석된 로그 자료는 로그필터(log filter)를 이용해서 감사 자료를 표준화하여 일관된 로그 감사 자료 구조를 유지하게 하였다. 각 운영체제의 로그 분석기에서 필요한 로그 정보를 수집한 다음, 로그 필터를 통해 로그 프로세서에서 필요로 하는 로그 필드만을 추출 한다음 로그프로세서에 의해 표준 형식으로 변환된다. 이때 로그프로세서는 침입 탐지 시스템에서 필요로 하는 감사 자료를 표준화된 구조대로 생성하는 역할을 한다.

본 논문에서 제안한 감사 자료 표준화를 위해 각기 다른 OS인 SUN 기종과 AIX 기종의 OS에서 생성되는 로그파일을 표준화하였다.

(그림4)는 로그 프로세서를 통해 변환된 표준화된 감사 데이터의 구조를 보여주고 있다. 이때 표준화된 양식을 작성하기 위해서는 시나리오 생성기를 통해 생성되는 시나리오의 항목들이 필요하다.

```
struct std_audit_data {
        unsigned long       tseq;
        char                hostname[32];
        char                remotehost[32];
        char                ttyname[16];
        char                cmd[18];
        char                jobname[16];
        char                dellog;
        char                errlogin;
        time_t              time;
        long                syscall;
        long                errno;
        char                dellog;
        long                pid;
```

그림4. 감사 자료 표준 형식

### 3.3 시나리오 생성기

Anomaly detection과 Misuse detection에서 기본적으로 분석할 자료가 시스템 로그인이다. 로그기록은 시스템 관리자에게 시스템 보안과 관련된 주요한 정보를 제공한다. 이러한 도구에 대한 연구의 결과로 Swatch와 같은 도구가 개발되었다. 그러나 Swatch는 시스템의 로그 파일 중 사용자가 미리 지정한 패턴이 발견되면 즉각적으로 통보해주는 기능이 있는 반면, 로그 기록을 통합적으로 분석해 주는 기능은 약하다. 본 논문에서 제안한 시나리오 생성기의 특징은 기본적인 로그 분석뿐만 아니라 종합적인 문제 분석까지 가능하게 했다는 것이다. 본 연구에서는 여러 개의 시나리오를 통해서 종합적인 분석 기능을 향상시켰다. 시나리오 생성기에서 생성된 탐지 패턴은 (그림4)와 같은 감사 자료 표준 형식에 따라 수집된다.

```
Class Scenario_Generator {
Rcv_scen();
//침입 탐지 엔진으로부터 시나리오 생성에 필요한 항목 수신
Generate_scen(); //시나리오 생성
send_scenario();
//시나리오의 내용을 에이전트에게 전송
update_scen();
//시나리오의 내용을 업데이트
```

그림5. 시나리오 생성기 함수 구조

(그림5)에서는 시나리오 생성기 클래스의 구조를 보이고 있다. User Interface를 통해 침입 탐지 엔진으로부터 탐지에 필요한 시나리오 작성을 위해 시나리오 생성기에 필요 항목(field)을 전송한다. 시나리오 생성기는 전송되어온 항목대로 시나리오를 구성하고 각 대상 호스트에 탑재되어 있는 에이전트에게 시나리오의 항목들을 전송한다. 이때 새로운 시나리오 항목이 침입 탐지 엔진으로부터 전송되면 새로운 시나리오로 업데이트(update) 된다.

### 3.4 침입 판단 엔진

침입 판단 엔진에서는 침입 탐지 시스템의 핵심 부분으로서 침입을 판단하고 이에 대응하는 보고를 하는 역할을 한다. 대상 호스트에 분산되어 있는 에이전트로부터 로그 자료를 수집하여 표준화된 감사 자료로 변환 다음 탐지 규칙에 의해 침입 여부를 결정한다. 본 논문에서 적용한 침입 결정 방법은 시나리오에서 적용한 패턴과 에이전트에서 추출된 패턴의 비교율의 임계값이 80%에 해당되면 침입으로 결정한다.

## 4. 제안된 시스템의 성능평가

본 논문에서는 실험을 위해 시나리오 생성기에서 생성된 시나리오와 연관된 명령어들을 실험 자료로 이용하였다. 이 자료들은 UNIX에서 사용하는 명령어나 파일, 디렉토리에 해당하며, 침입 판단을 위해 임계값을 주었다. 이때 임계값을 너무 높게 주게되면 침입 판정의 정확도는 높게 되지만 전체적인 탐지율은 낮아지고 침입을 정상적인 사용으로 인정해버리는 치명적인 에러가 생길 수 있고, 임계값을 낮게 주면 탐지의 정확도는 낮아지지만 탐지율은 높아진다. 따라서, 본 논문에서의 임계값의 조정은 침입 판단 엔진에서 할수 있게 하였다.

에이전트는 시나리오대로 사용자의 로그파일을 수집해서 침입을 판정에 이용하게 된다. 임계값의 조정은 시스템 관리자에 의해 사용자의 수나 시스템 처리 능력에 따라 변화시킬 수 있게 하였다. (그림6)은 침입 판정을 위해 임계값을 조정했을 때의 탐지율을 그래프로 보이고 있다.

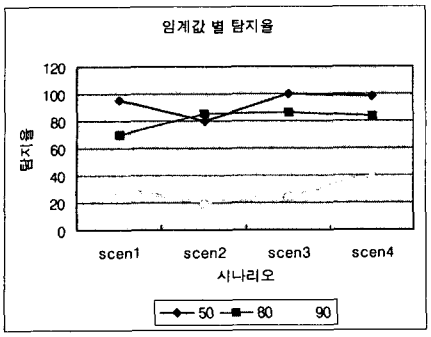


그림11. 임계값 별 침입 탐지율 변화

Fig11. Intrusion detection ratio variation following by critical value

(그림6)에서 알 수 있듯이 임계값을 낮게 줄수록 침입 탐지율은 높아지고 소요시간은 짧아지며, 임계값을 높일수록 탐지율이 낮아지는 반면에 정확도는 올라가고, 탐지 시간이 길어지는것을 볼 수 있다.

본 시스템의 특징은 에이전트 단계에서 침입 탐지에 필요한 감사자료를 추출하여 표준화된 포맷으로 변형시킴으로써 침입 탐지 호스트에서의 작업 부하를 최소화 시켰고, 탐지에 적합한 임계값을 조정하게 할 수 있게 함으로써 시스템의 상황에 적절히 대처할 수 있게 하였다[14].

## 5. 결론

본 논문에서 제안한 패턴 추출 에이전트 침입 탐지 시스템은 실시간적으로 분산된 호스트에 대해 에이전트에서 침입 탐지에 필요한 데이터를 수집하며, 특히 감사 파일의 표준화 단계를 거침으로써 이 기종간의 침입 탐지의 효율성을 극대화하였다. 에이전트에서 침입 탐지에 필요한 자료를 수집하도록 하기 위해 시나리오생성기에서 침입 시나리오를 작성하여 에이전트에게 전송함으로써 에이전트는 즉각적으로 반응하고 필요한 자료만을 수집하게 된다. 감사파일 표준화 단계에서는 다중의 호스트에서 다중침입이 발생할 경우 침입 탐지 시스템에서는 큰 부하가 발생하여 전체적인 시스템 속도를 저하 시킨다.따라서, 표준 감사 파일 포맷을 만들어 이 기종에서 수집되는 감사 데이터를 하나의 포맷으로 작성하여 침입 판정에 있어서의 시스템 부하를 최소화하였다.

## 참 고 문 헌

[1] S.Kumar and E.Spafford, "A pattern matching model for misuse intrusion detection." Seventeenth National Computer Security Conference, Baltimore, MD, October 1994, 11-21.

[2] S.Stolfo, A.Prodromidis, S. Tselepis, W. Lee, "Java Agents for Meta learning over Distributed Databases", in AAAI97 workshop on AI Methods in Fraud and Risk Management 1996.

[3] Neil Crowe and Sandra Schiavo, "An Intelligent Tutor for Intrusion Detection on Computer System", code Cs/rp, Department of Computer Science, Naval postgraduate school monterey, 1997

[4] Sandeep Kumar, gene Spafford. "A Pattern Matching Model for Misuse Intrusion Detection", Proceedings of the 17th National Computer Security Conference, October 1994.

[5] T. lane and C. E. Brodley. "Detecting the abnormal: Machine learning in computer security", Technical Report TR-ECE 97-1, Prudue University, West Lafayette, IN, 1997.

[6] Jai Sundar B. Spafford E, "Software Agents for Intrusion Detection," Technical Report, Purdue University, Department of Computer Science, 1997.