연관규칙 에이전트를 적용한 침입 탐지 시스템에 관한 연구

박찬호* · 정종근**

A study of Intrusion Detection System applying for association rule agent

Chan-Ho Park* · Jong-Geun Jeong**

본 논문은 2000년도 조선이공대학 광통신연구비로 수행되었음

요 약

침입 탐지 시스템이 가지고 있는 문제점중의 하나는 긍정적 결함(False Positive)이다. 이러한 결함은 침입 탐지 시스템의 성능을 저하시킬 수 있다. 긍정적 결함의 발생원인은 감사데이터 학습단계에서 충분한 학습이 이루어지지 않기 때문에 발생한다. 따라서 본 논문에서는 연관규칙을 탑재한 에이전트에 감사데이터를 학습시키는 방법으로 침입 탐지 시스템을 제안한다.

ABSTRACT

One of the Problems, which the Intrusion Detection System has, is a False Positive. This False make to low condition of the Intrusion Detection System. The cause of the False Positive is that the learning is not enough during audit data learning steps. Therefore, in this paper, I propose the method of the Intrusion Detection System that be learnt audit data to agent with association rule.

키워드

에이전트, 인터넷, 네트웍, 침입탐지, 연관규칙

Ⅰ. 서 론

기존의 침입 탐지 시스템이나 프로토 타입들은 일반적으로 단일 시스템 환경에 적합하게 설계되고 적용되고 있으므로 대규모 네트워크로의 확장에 어려움을 가지고 있다. 이는 각각의 시스템들이 지닌 독자적인 메시지 처리 방식에 기인하며 이러한 문제를 극복하기 위해서 제각기 다른 기존 시스템들을 재 사용할 수 있는 침입 탐지 시스템 프레임워크의 개발이 요구되고 있다. 따라서 전체적으로 통합된 침입 탐지 전략을 세우기 위해서는 침입 탐지 기법의 확장 및 서로 다른 방식으로 얻어지는 정보들에 대한 통합과 정제가 필요하다. 따라서, 기본적인 침입 탐지는 개별적으로 수행하되, 대규모 네트워크 사이에서의 분산적이고 협력적인 침입 형태를 탐지하기 위한 침입 탐지 시스템들간의 효율적인

*조선이공대학 정보통신과

**동강대학 전자정보과

접수일자 : 2002. 5. 3

정보 교환을 할 수 있는 에이전트에 대한 연구가 필요하다.

II. 기존 침입 탐지 시스템의 문제점

침입 탐지 시스템의 핵심 기술은 행위 판별(Behavior Classification)과 자료축소(Data Reduction) 기술이다. 행위 판별은 주어진 일련의 행위들에 대해 침입인지 아닌지를 판별하는 것이고, 자료축소는 시스템에서 발생하는 거대한 양의 각종 로그 데이터(log data)를 의미있는 데이터로 추출하여 변환하는 작업이다. 일반적으로 침입 탐지 규칙에서는규칙기반 시스템(Rule-based system)과 신경망 또는 통계적 분류 시스템을 사용한다. 기존에 사용된 규칙기반 시스템, 신경망, 통계적 분류 시스템은 많은 양의 데이터가 초기 학습을 위해 필요하며, 계속적으로 시스템을 유지하는데 많은 시간과 비용을 초래하며 새로운 공격 대응 능력이 약하다는 취약점을 가지고 있다.

규칙기반 침입 탐지 시스템의 대표적인 예로 IDES 시스템을 들 수 있다. 이 시스템은 대상 시스템의 취약성 및 보안정책 그리고 과거의 침입에 대한 지식을 데이터 베이스에 저장한 후 침입이 발생 할 때, 탐지 시스템은 침입에 대한 규칙베이스(Rule base)에 의해 현재 시스템의 침입 여부를 결정한다. 규칙기반 IDS의 경우 초기의 규칙기반을 만들기 위해 보안 분야의 높은 지식을 가진 전문가의 지식이 필요하다. 이는 오랜 시간과 막대한 개발비용을 필요로 하는 작업이다. 게다가 전문가라 할지라도 시스템의 모든 취약성에 대해 알 수 없으며, 기존의 많은 시스템들의 약점들간의 상호작용으로 생겨나는 취약성에 대해서는 발견해 낼 수 없다는 단점이 있다. 만일 시스템의 프로파일에 중요한 변화가 발생한다면, 규칙기반 시스템의 경우 새로운 침입 가능성에 대비하여 규칙기반을 새롭게 설계해야 한다.

Kumar와 Spaffod에 의해 제안된 패턴 매칭 기법에 기반한 접근법은 시스템상에 요구되는 유연성의 향상에 초점이 맞추어져 있지만 학습능력을 갖추지 못하였다는 단점을 가지고 있다[6][7][22]. 이들은 시스템상에 나타나는 현상들에 근거하여 침입을 어떻게 분류하는 지를 보여주고 있다. 여기서의 각 패턴들은 시스템 상태들간의 의존도를 인코딩하고 있는 것이다. 이러한 접근법은 침입을 탐지하는 강력한 방법이나 사전에 만들어진 패턴들에 의존적이라는 단점 또한 가지고 있다. 즉, 패턴 자체가 완전하지 못할 경우 시스템의 방어에 커다란 헛점(Hole)이 나타나게 되는 것이다. 그리고 보안 정책이나 시스템 운영상에 변화가 있을 경우 패턴들을 다시 만들어야 한다는 문제점이 있다.

현재까지 제시된 침입탐지 시스템들은 몇 가지 문제점들을 공통적으로 가지고 있는데 이 중 가장 두드러진 문제점은 변형된 공격패턴이 발생할 경우 이를 탐지해 내지 못한다는 것이다. 따라서, 본 논문에서는 독립적인 에이전트에 연관규칙을 적용하여 감사데이터를 학습시킴으로 변형된 형태의 침입기법을 탐지할 수 있는 방법을 제안하고자 한다.

III. 에이전트기반 침입 탐지 시스템

침입 탐지 시스템에서는 각 모듈에이전트들이 분산되어 있는 호스트들에 대한 모니터링을 하게되며, 비정상적인 행동이라고 의심이 갈 경우 이 사실을 관리자에게 즉각 통보한다. 그리고, 새로운 침입 패턴을 항상 학습하게 된다. 에이전트 학습을 위해서 연관규칙 알고리즘을 적용한다[2]. 데이터 마이닝 알고리즘은 과거에서 현재까지의 행동 패턴을 수집하여 분류하는 알고리즘으로 전자상거래 등에서 고객의 구매 패턴을 예측하는데 주로 이용하는 기술이다. 에이전트들은 상호 독립적으로 태스크를 수행하며 사용자들이 로그아웃(log out) 할 때까지 모니터링하여 로그 데이터를 수집한다.

수집된 로그 데이터는 침입탐지 메인 호스트에 있는 학습 모듈로 전송되어 각각의 사용자들에 대한 행동패턴을 다양한 각도에서 분류한다. 이렇게 분류된 각 사용자들의 행동패턴은 침입패턴 데이터베이스(Intrusion Pattern DB)에 저장된 다음 지속적으로 에이전트와 통신하면서 패턴데이터를 교환한다. 그림1은 에이전트 모듈의 내부구조를 나타낸 것이다.

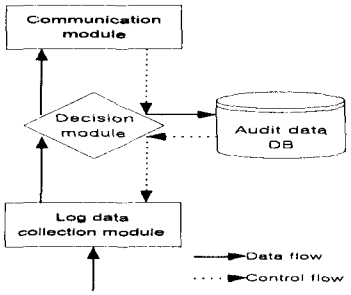


그림 2. 에이전트모듈 내부 구조
Fig 1. Internal structure of agent module

IV. 에이전트 학습

기계학습(machine learning)은 동일한 성격의 작업을 더욱 효과적으로 수행 할 수 있도록 시스템을 적응적으로 변화시키는 것이라고 할 수 있다[35]. 가장 기초적인 기계학습 방법은 계산 결과를 단순히 기억하거나 지시자(instructor)로부터 주어진 정보를 지식베이스에 저장하여 다음 작업에 효율적으로 이용하는 방법이다. 보다 복잡한 형태의 기계학습은 과거 문제해결 경험으로부터 새로운 기술을 습득하거나 현재의 지식을 새롭게 구조화하는 것이다. 이러한 기계학습에 기반으로 한 방법은 최소한의 배경지식으로 사용자의 행위(behavior)를 학습함으로써 사용자를 돕는 데 필요한 지식을 얻는 방법이다.

사용자 행위의 관찰을 통한 학습(learning by observing the user)방법은 에이전트가 사용자의 행위를 지속적으로 관찰하여 필요한 지식을 습득하고 학습하는 방식이다. 에이전트는 오랜 기간 동안 사용자의 행위를 모니터링(monitoring)하고 반복되는 행위의 패턴을 자동적으로 습득한다.

본 논문에서는 이러한 에이전트 시스템의 특성에 기존의 기계 학습 방법 대신 연관규칙을 적용한 학습 방법을 제안한다. 연관규칙 학습 방법과 기계학습은 과거의 경험을 바탕으로 학습한다는 점은 동일하지만 다양한 패턴으로의 변화와 새로운 패턴의 추측 면에서는 이 방법이 훨씬 뛰어나다. 따라서 기능은 기존의 에이전트 시스템과 동일하지만 학습 방법에서는 연관규칙 을 채택하였다. 비정상 탐지를 위한 기계학습 방법의 어려움은 알려져 있지 않은 패턴과 알려진 패턴의 한계를 정하는 것이다. 학습 데이터에 있어서 비정상 패턴에 대한 별다른 예를 가지고 있지 않은 상태에서는 기계 학습 알고리즘은 훈련 데이터에 있는 알려진 패턴에 대한 한계를 구분할 수 없다. 일반적으로 비정상과 오용 탐지를 구분하기란 쉬운 일이 아니다. 비정상 탐지는 전형적으로 비통제된 학습 방법을 사용하는 반면에 오용 탐지에서는 통제된 분류 방법을 사용한다. 변형된 새로운 유형의 공격이 발생할 경우, 이 공격 패턴을 즉시 학습시킴으로써 새로운 공격에 대응하고자 한다. 이를 위해 새로운 공격 패턴이 발생할 경우 이미 분류되어 있는 침입 패턴 집합에 계속적으로 추가시킨다.

```
if (H1(x)=normal) ∨ (H1(x)=anomaly) then
  if H2(x)=normal
    then output ← H1(x)(normal or anomaly)
    else output ← new_intrusion
else output ← H1(x)
```

그림 2. 학습데이터 분류
Fig 2. Classification of learning data

그림2의 알고리즘에서와 같이 H_2는 새로운 침입 패턴과 정상 데이터로부터 학습된 추가된 분류자이다. 알고리즘에서 결정 규칙은 출력을 위해서 평가된다. H_1은 존재하는 침입 탐지 시스템 모델이고 H_2는 최근에 발견된 새로운 침입 패턴을 위해 훈련된 새로운 모델이다. H_1에서는 정상과 비정상 패턴만을 확인하고 새로운 침입을 확인할 수 없기 때문에 대부분의 패턴들은 비정상과 오용으로 분류한다. 그러나 H_2는 새로운 침입과 정상 데이터로 분류한다. 이때 새로운 침입 패턴의 양이 적기 때문에 H_2는 다른 데이터로부터 침입 패턴을 쉽게 분류할 수 있다.

V. 시스템 설계 및 구성

전체적인 시스템 모듈은 크게 에이전트(agent)와 침입탐지서버(IDS server)에 포함된 로그 프로세서 모듈, 연관규칙학습모듈, 침입 상태 보고 모듈 그리고 콘솔(console) 등으로 구성되는데 그림3과 같다. 에이전트 모듈은 각 시스템에 존재하여 시나리오 모듈에서의 시나리오에 해당하는 이벤트를 수집하고 침입을 탐지하는 역할을 한다. 침입탐지 서버는 에이전트로부터 전송된 감사 데이터를 분석하여 분산 공격 여부를 판단하는 탐지엔진 역할을 하고, 침입으로 판정되면 서버는 에이전트에게 대응 명령을 내린다. 그리고 에이전트로부터 전송된 감사 데이터를 기록하고 콘솔로 응답하게 된다. 서버의 또 다른 기능중의 하나는 새로운 탐지 규칙과 운영에 관한 각종 설정을 네트워크로 연결되어 있는 에이전트에게 분배함으로 업데이트(update)가 가능하다. 서버에 포함된 시나리오 모듈은 침입 유형 분석을 통해 발견된 침입 패턴과 시스템 공격 유형에 대한 정보 등이 탑재되어 에이전트의 작업에 필요한 명령을 지시한다.

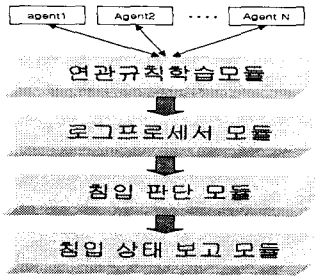


그림 3. 시스템 구성도
Fig 3. Structure of System

로그 프로세서는 에이전트를 통해 수집된 이벤트의 로그정보를 표준화된 단일 형태로 변환한다. 연관규칙 학습 모듈은 기존의 침입 패턴을 분류·학습하여 침입 패턴을 다각적으로 분석한다. 침입 판단 모듈은 에이전트에서 수집한 로그 정보와 감사데이터를 비교하여 침입의 유무를 판단하여 침입 상태모듈에 전송하며, 침입 상태 모듈에서는 침입 보고와 사용자에대한 강제 접속 종료등의 업무를 담당한다. 콘솔(consle)은 침입탐지시스템을 운영하기 위한 인태페이스로써 IDS서버나 에이전트에 대한 운용과 관련된 설정 기능과 접속자들의 로그(log) 조회기능, 침입과 관련된 보고 기능 등을 수행한다.

VI. 성능 평가

침입 탐지 시스템의 핵심이 탐지의 정확도와 높은 탐지율이라면 가장 큰 문제점은 탐지 오판율을 최소화시키는 일이다. 침입 탐지 오판의 대부분은 긍정적 결함(false positive)과 부정적 결함(false negative)으로써, 이와 같은 결함들을 최소화시키는 것이 오판율을 줄이는 것이다. 본 논문에서는 긍정적 결함을 최소화하는 것에 초점을 두었다. 긍정적 결함의 발생원인은 침입 패턴을 감사 데이터화 하는 과정에서 침입 패턴에 대한 감사 데이터 범위를 결정하는 과정에서 발생한다. 이를 해결하기 위해서 본 논문에서는 감사 데이터를 학습하는 과정에서 연관규칙기법을 적용하여 하나의 침입 패턴에서 발생할 수 있는 여러 가지 변형 형태에 대한 예측 학습이 가능하도록 하여 긍정적 결함의 발생을 최소화하였다. 다음 그림은 임계값(threshold)이 증가함에 따라 긍정적 결함이 감소하는 실험 결과를 보여주고 있다.

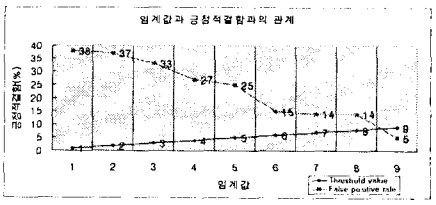


그림 4. 임계값과 긍정적 결함과의 관계
Fig 4. Relationship of threshold and false positive

VI. 결 론

본 논문에서는 연관규칙 알고리즘의 분류 알고리즘으로 정상과 비정상 패턴을 분류하여 탐색할 로그 데이터의 양을 줄였고 비정상 패턴중에 변형

된 비정상 패턴을 추측하여 침입을 탐지해내도록 하였다. 분산된 환경에서 여러 호스트를 탐지해내기 위해 독립적으로 동작할 수 있는 에이전트를 사용하였다. 에이전트의 학습에 연관규칙을 적용하여 긍정적 결함의 비율을 현저하게 줄일 수 있었다. 향후 연구과제로는 실시간 침입 탐지를 위한 학습의 최적화 방안을 모색하고, 네트워크상의 비정상 탐지를 위한 방안에 대한 연구가 지속적으로 필요하다. 또한 새롭게 나타나고 있는 해킹 패턴에 대응할 수 있는 다각적인 시각에서의 대처 방안이 연구되어야 한다.

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.

[7] Crosbie M, Spafford E, "Defending a Computer System using Autonomous Agents," Technical Report, Purdue University, Department of Computer Science, 1996.

[8] 은유진, 박정호, "침입 탐지 기술 분류 및 기술적 구성요소", 정보보호센터 정보보호 뉴스 1998.7 통권 13호.

[9] "정보시스템 침해사고 방지기술 개발에 관한 연구", 정보보호센터,1999.1

[10] 정종근 외 4인, "데이터 마이닝 기법을 적용한 최적 침입 탐지 모듈 설계", 1999 춘계 정보과학회 논문집

저 자 소 개

박찬호(Chan-Ho Park)

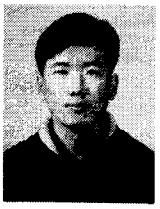
1977년 광운대학교 무선통신공학과 (공학사)

1988년 조선대학교 전자공학과 (공학석사)

2000년 원광대학교 전자공학과(공학박사)

1978년~2002년 현재 조선이공대학 정보통신과 교수

※관심분야 : 이동통신, 정보보안, 데이터통신, 디지털신호 및 전송



정종근(Jong-Geun Jeong)

1995년 조선대학교 전자계산학과 졸업(이학사)

1997년 조선대학교 대학원 전 자계산학과졸업(이학석사)

2002년 2월 조선대학교 대학원 전자계산학과 대학원 박사수료

1999년 3월~2002년 현재 서린정보시스템 팀장

1999년 3월~2002년 현재 동강대학 전자정보과 겸임교수

※관심분야 : 인공지능, 전문가 시스템, 멀티미디어, 정보보안, 네트워크, 전자상거래, 바이러스