

# 에이전트기반의 IDS

이상훈<sup>0</sup> 송상훈 노용덕  
세종대학교 컴퓨터공학과  
taebaik<sup>0</sup>@gce.sejong.ac.kr

## A IDS system of Agent Based

Lee sang hun<sup>0</sup>, Song sang hur, Noh Yong Deok  
Dept. of Computer, Sejong Computer Science

### 요 약

컴퓨터망의 확대 및 컴퓨터 이용의 증가에 따른 부작용으로 컴퓨터 보안 문제가 중요하게 대두되고 있다. 이에 따라 침입자들로부터 침입을 줄이기 위한 침입탐지 시스템에 관한 연구가 활발히 논의 되고 있다. 본 논문에서 IDS 모델들의 소개와 새로운 IDS의 모델을 제시하고 단위 침입 행동별로 학습된 모니터링 프로세스에서 전송되는 사용자 위협 메시지에 대한 처리를 담당하는 조정자 에이전트 시스템을 설계하고자 한다. 본 논문에 제안된 조정자는 안정화된 메시지 처리 문제 뿐 아니라 기존 모델의 에이전트간 협력 작업에 의해 처리되었던 침입판단 기능 및 모니터링 프로세스들의 관리 기능 또한 수행하도록 한다. 그리고 시스템의 유연성 및 확장성 향상을 하도록 하였다.

### 1. 서 론

네트워크 상에서의 침입시도는 날이 갈수록 점점 더 증가하고 있으며 또한 여러 가지 형태로 침입하고 있다. 해커들의 악의적이고 독창적인 침입방식으로 인하여 침입탐지 프로그램의 개발은 점점 더 어려워지고 있다. 또한 인터넷의 발전과 더불어 네트워크상에서 시스템간에 협력이 증시되고 있다. 기존의 침입탐지 시스템은 다양한 침입에 대처하기가 어렵기 때문에 새로운 형태의 침입탐지 시스템이 필요하다

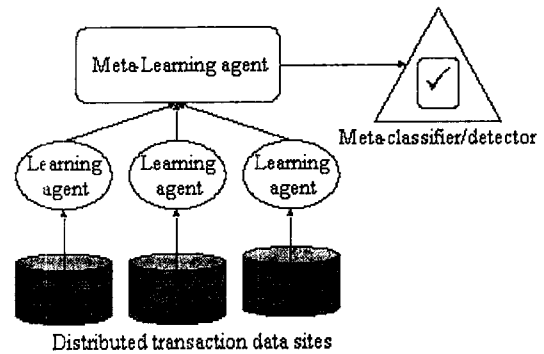
### 2. 모델에 관한 연구

대부분이 침입탐지 시스템들은 하나의 통합된 시스템 구조를 가지고 있다. 커널과 같은 시스템의 운영 체제 위에 놓여져 커널로 들어오는 처리 요구에 대해 모니터링을 수행한다. 그러나 이러한 시스템 모델들은 전체 시스템에 걸리는 부하문제 및 탐지 모듈의 파괴에 따른 안정성문제와 시스템의 확장에 따른 성능 보장 등과 같은 많은 문제점을 지니게 되었다.

따라서 네트워크환경에서의 감시 및 탐지, 침입여부에 대한 판정과 더불어 각 시스템이 제공하는 침입탐지 정보의 통합 분석을 통하여 광범위한 분석을 가능하게 하는 계층적 구조의 침입탐지 시스템개발이 필요하다. 이에 모델 살펴보고자 한다.

JAM(Java agent for Meta-Learning over Distributed)은 데이터 마이닝 프로그램을 평가하는데

어 일반적인 접근 방법인 Meta-Learning을 활용하여 분산환경에서의 이식성과 확장성을 제공하는 에이전트 기반의 데이터 마이닝 시스템이다.



<그림 1> JAM 학습 구조

<그림-1>에서 볼 수 있듯이 JAM의 수행 구조는 먼저 원격 데이터 사이트로 학습에이전트가 수행되며 데이터 사이트의 지역 분류자를 계산하여 데이터 사이트로 보내고 지역 메타 학습 에이전트에서 결합시킨다. 이러한 행위는 모든 데이터 사이트에서 동시에 실행된다.

이것은 거짓과 침입 패턴의 연속적인 학습을 위한 보안 에이전트의 하부구조를 지원한다. 그리고 에이전트에서 전달된 분류자를 조합하여 원격으로 Meta-Learning을 할 수 있다. 또한 개인의 데이터를 보여주지 않고 사

이트의 데이터를 공유하는 것이 가능하다. 따라서 거짓과 침입 패턴에 대한 빠른 분배학습이 가능하며 네트워크 정보 시스템에 면역성을 주는 행위 모델이 되었다.

### 3. 침입탐지 시스템의 설계

기존에 제안된 대부분의 침입탐지시스템들은 하나의 통합된 단일시스템구조를 가지고 있다. 커널과 같은 대상 시스템의 운영 체제위에 놓여져 커널로 들어오는 모든 처리 요구에 대해 모니터링을 수행한다

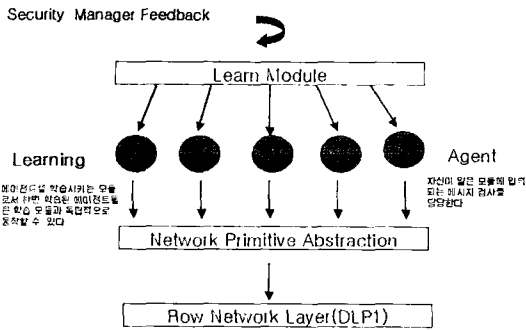


그림 2 에이전트를 이용한 침입탐지 시스템구조도

그러나 이러한 시스템 모델들은 전체시스템에 걸리는 부하문제 및 탐지 모듈의 파괴에 따른 안전성의 문제, 시스템의 확장에 따른 성능보장과 같은 문제점을 가지고 있다. 그러나 이러한 시스템 모델들은 전체시스템에 걸리는 부하문제 및 탐지 모듈의 파괴에 따른 안전성의 문제, 시스템의 확장에 따른 성능보장과 같은 문제점을 가지고 있다. 이러한 성능상의 문제 해결을 위한 방법으로 대상 시스템을 지역적 또는 기능적으로 분할하는 방식이 있다. 이는 다수의 프로세서들로 하여금 독립적인 동작으로 분할된 시스템 자원을 모니터링 하는 것이다. 전체 시스템에 대한 침입 발생 시 이들 프로세서간의 협력을 통해 탐지하도록 시스템을 구성해야 한다. 이러한 구조는 기존의 시스템에 대한 부하문제 및 탐지모듈의 파괴에 따른 전체 기능의 마비 및 시스템의 확장에 따른 탐지 시스템의 확장성 보장등의 문제들을 해결 할 수 있다.

#### 3.1 Learning Module

에이전트를 학습시키는 모듈로서 한번 학습된 에이전트들은 학습모듈과 독립적으로 동작할 수 있으며 에이전트들이 동작하는 동안 모든 기록은 다음 학습으로 입력

된다. 판단한다. 검사단계에서 침입 추정값이 특정 임계치를 지나면 이를 침입으로 간주한다.

#### 3.3 DCL1

Sun의 DCL1 은 인터페이스로 응용 프로그램이 실제 데이터를 링크 계층의 패킷을 전송하고 받을 수 있게 해주는 인터페이스이다.

#### 3.3 Network Primitive Abstraction

DCL1은 인터페이스로부터 실제 네트워크 패킷을 받아 에이전트들이 그 패킷을 다룰 수 있도록 패킷의 구조를 바꾸어주는 레벨이다.

### 4. 에이전트 기반의 침입탐지 시스템

본 논문에서 제안하고있는 시스템에서는 각 모듈 프로세서들이 시스템 자원들에 대한 행동패턴을 관찰하여 비정상적인 행동이라고 생각될 경우 이를 알릴 수 있도록 학습되어진 에이전트의 형태를 가진다.

학습을 위해서는 유전자 알고리즘을 사용하여 의심스러운 행위패턴에 대해 분별할 수 있도록 학습시킨후 각 모니터링 대상이 되는 리소스를 올려놓는다.

시스템 사용자들에 의한 행동은 일련의 시스템자원에 대한 접근 및 서비스 요구로 이루어짐으로서 각각의 대상 시스템에서 사용자의 형태가 모니터링 된다. 상호 독립적으로 증속하는 에이전트들은 모니터링 중 비정상 행위가 발생하였을 경우 주변의 에이전트들에게 알리고 의심스러운 특정사용자의 행위에 대해서는 계속적으로 모니터링 하게 된다. 만약 그 행동이 시스템 전체에서 허용하는 특정수위의 한 계치를 넘을 경우 이를 비정상적인 행동으로 보고 이에 대한 대응 및 보고를 한다.

#### 4.1 조정자 에이전트

새로운 침입탐지 모델은 Audit data를 통한 해석을 이용하여 침입판단 및 탐지모듈과 시스템의 전반적인 조정을 하는 조정자 에이전트를 가진다. 또한 그 하부에 활동적인 에이전트를 기반으로 두 단계의 에이전트의 구조를 가지고 있다. 상부의 에이전트는 Genetic를 이용한 내부사용자의 비정상적인 사용과 오용행위패턴을 지식 데이터 베이스로 구축하며 Coordinator Agent와 Autonomous Agent 간에는 black board 시스템을 이용한다. 이는 시스템상의 여러 에이전트들이 협조하여 침입을 감시하고 새로운 형태의 침입에 대한 반응속도를 높여 실 시간적인 침입탐지 시스템을 구축하기 위함이다.

