신경망 기반의 협동적 침입탐지

김형천, 강철오, 박중길
국가보안기술연구소
(khche, cyberkan, jgpark)@etri.re.kr

Collaborative Intrusion Detection based on Neural Network

Hyoung-Chun Kim, Chul-Oh Kang, Jung-Gil Park
National Security Research Institute

요 약

최근 네트워크 환경이 고속화 됨에 따라 네트워크 상의 침입 공격이나 인터넷 웜의 활동이 급속도로 증가하고 있다. 이러한 네트워크 상의 침입이나 바이러스를 방어하기 위한 기술적 관건은 침입여부를 판단하기 위한 근거를 어디에서, 얼마나 정확하게, 그리고 신속하게 찾을 수 있느냐에 달려있다. 본 논문에서는 속도 면에서 매우 우수하고 적응력이 뛰어난 신경망 알고리즘인 Fuzzy ART 엔진을 탑재한 침입탐지 에이전트를 구성하여 분산된 네트워크 환경에서 협동적인 실시간 침입 탐지와 조기 경보가 가능한 시스템을 제안하고자 한다.

1. 서 론

침입탐지 시스템(intrusion detection system)은 컴퓨터 시스템 또는 네트워크 자원의 무결성(integrity), 기밀성(confidentiality), 가용성(availability)을 저해하는 악의적인 행위를 실시간으로 탐지하는 시스템을 말한다. 침입탐지 시스템은 이러한 침입에 대한 탐지를 통해 시스템 자원의 고의적인 파괴 또는 부정 사용하려는 행위를 사전에 예방할 수 있으며, 이는 정보보호의 가장 중요한 분야 중 하나이다.

최근 1.25 인터넷 대란과 같이 조기 경보체계가 제대로 갖추어지지 않은 상황에서 웜의 활동으로 인한 피해는 기하급수적으로 퍼져 나갔다. 네트워크 환경이 고속화 됨에 따라 그 피해의 규모는 커져가고 있는 상황이다. 또한 인터넷의 발전과 더불어 대규모 네트워크에서의 시스템 간 상호협력이 중시되고 있으며, 이는 침입탐지 시스템의 새로운 환경에 많은 영향을 미치게 되었다. 기존의 침입 탐지 시스템들은 갈수록 다양해지는 침입에 대해 능동적으로 대처하는데 어려움이 많았으며, 대규모 네트워크 환경에서의 효율적인 탐지에 적합하지 않은 구조를 지니고 있다. 따라서 이를 고려한 새로운 형태의 침입 탐지 시스템 구조가 제시되고 있다. 이러한 대한 필요성에 의해 최근의 침입탐지 시스템의 경향은 대규모 네트워크 상에서의 상호 협력을 추구하고 있으며, 이를 통해서 탐지할 수 있는 침입 유형에 대한 기초 연구가 이루어지고 있다.

본 논문에서 제안하는 협동적(collaborative) 침입탐지 시스템은 속도 면에서 매우 우수하고, 점증적 클러스터링이 가능한 신경망 알고리즘인 Fuzzy ART(Adaptive Resonance Theory) 엔진을 탑재한 침입탐지 에이전트를 구성함으로써, 분산된 네트워크 환경에서 협동적으로 실시간 침입 탐지가 가능한 시스템을 제안하고자 한다. 이는 기존의 단일 영역의 침입탐지 시스템의 한계를 극복하는 것으로써 대규모 네트워크 환경에서 각 침입탐지 에이전트들은 서로에게 Fuzzy ART 엔진에 의해 생성된 소량의 침입정보 벡터 및 네트워크 이상 경보를 전송함으로써, 기존의 로컬 침입 탐지 시스템들이 탐지해낼 수 없었던 침입 공격까지 탐지해낼 수 있는 침입탐지 시스템의 프레임워크이다.

2. 관련연구

COAST 는 침입탐지를 오용탐지(Misuse Detection)와 이상탐지(Anomaly Detection)로 분류하고 있다. 오용탐지는 알려진 취약점들을 이용하여 공격하는 행위들을 사전에 공격 특징 정보를 가지고 있다가 탐지하는 방법으로, False-positive 오류가 매우 적고 상대적으로 구현비용이 저렴하다는 장점이 있는 반면 공격에 대한 정보를 계속 수집하는 데에 어려움이 있고 알려진 공격에 대해서만 탐지할 수 있다는 한계가 있다.

또 다른 유형인 이상탐지는 정상행위 모델을 벗어나는 경우를 침입으로 간주하는 방법으로써 정상 행위에 대한 대량의 데이터를 분석해야 하므로 구현 비용이 큰 단점이 있지만 알려지지 않은 새로운 공격도 탐지할 수 있고 False-negative 오류를 줄일 수 있어서 날로 다양해지는 침입기법에 대응하기 위한 방안으로 연구가 활발한 상태이다. 이러한 비정상행위의 판단 근거로는 내부 시스템 자원 사용량에 따른 변화, 사용된 프로그램 및 명령어의

변화, 그리고 네트워크의 사용에 따른 변화 등이 있는데 네트워크 사용에 따른 변화는 사용된 서비스 트래픽 특성에 따른 클러스터링 등을 이용할 수 있다.

최근 침입탐지 방안으로 네트워크 트래픽의 특성을 이용한 방안이 제시되고 있고 이러한 방대한 데이터 분석을 좀더 지능적이고 자동적으로 수행하기 위해 데이터 마이닝(Data Mining) 기법 중에서 클러스터링 기법을 활용하고 있다. 사용자의 행위를 클러스터링 함으로써 이를 이용하여 비정상적인 행위를 탐지하는 방법과 네트워크 서비스별 트래픽 특징에 대한 클러스터링을 이용하여 비정상행위 침입을 탐지하였다[1][2][3].

신경망을 이용한 침입탐지는 이론적으로 지식기반 침입탐지 방식에서 공격을 학습하고 감사 스트링에서 탐색하는데 사용될 수 있는데, 보다 향상된 오용 탐지를 위해 신경망 알고리즘인 Back Propagation 을 적용한 연구[2]와 오용탐지 방법과 이상탐지 방법이 결합된 데이터 마이닝 알고리즘을 이용하여 실시간 침입탐지가 가능한 시스템에 관한 연구도 이루어졌다[1].

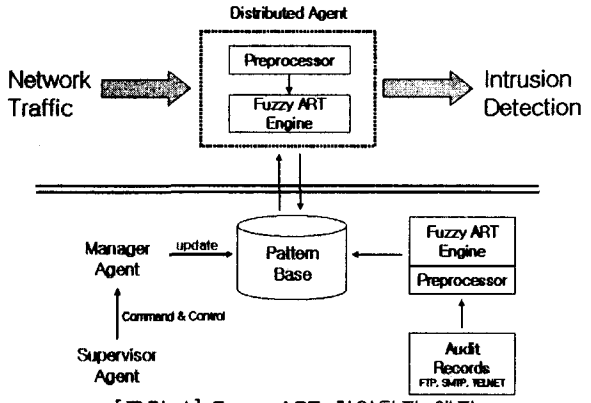
대규모의 하부구조를 지닌 네트워크에 대한 침입은 다양하고 포괄적인 형태를 지니며, 이러한 형태의 침입은 단일 시스템에서 탐지하기가 쉽지 않다. 따라서 지역 네트워크의 탐지 정보를 전역 네트워크에서 수집하고 해석하여 대규모 네트워크를 대상으로 한 침입을 탐지할 수 있도록 계층구조로 침입탐지 모듈을 연결하는 프레임워크에 관한 연구들이 이루어지고 있다. 다음 [표 1]은 DARPA 에 의해 수행된 계층적 구조를 갖는 침입탐지 시스템들의 특징을 나타낸 것이다.

[표 1] 계층적 네트워크 침입탐지 시스템

JAM	Columbia U.	Meta-Learning 지원
JiNao	MCNC	IDS 상호간 안전한 연결 프로토콜
AAFID	Purdue U.	분산 에이전트 기반
EMERALD	SRI Int.	오용, 이상 통합 탐지 및 계층화
NETSTAT	Santa Babara U.	호스트/네트워크 침입탐지 시스템 배치 및 공격 시나리오 표현
GrIDS	U.C. Davis	각 호스트의 행위 관계에 대한 그래프 생성

3. Fuzzy ART(Adaptive Resonance Theory) 엔진

Fuzzy ART 는 빠른 속도 이외에도 다음과 같이 장점이 있다. 첫째, 비교사 학습(unsupervised learning)에 의해 입력 패턴을 클러스터링 함으로 사전에 학습 데이터를 통한 훈련 없이 새로운 입력 패턴을 학습할 수 있다. 둘째, ART 는 기존 신경망들의 딜레마인 Stability-Plasticity 문제를 해결할 수 있다. 입력 패턴과 학습된 클러스터간의 비교를 통해, 이미 학습된 클러스터에 영향을 미치지 않으면서 학습을 수행할 수 있는 Reset 매커니즘을 사용하여 이 딜레마를 해결할 수 있다. 셋째, 경계변수(vigilance parameter) 값에 따라 클러스터링의 분류 결과를 조정할 수 있다. 즉, 경계 변수의 값을 크게 주면, 좀 더 세분화되고 구체적인 클러스터들을 얻을 수 있다[6][7].



[그림 1] Fuzzy ART 침입탐지 엔진

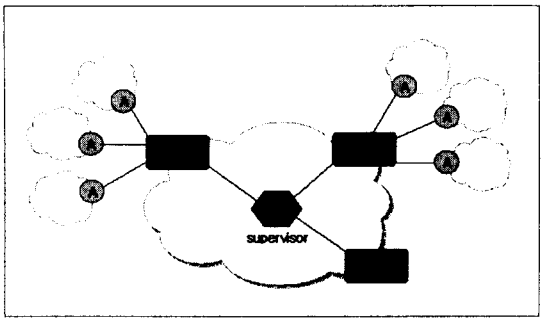
[그림 1]은 본 논문에서 사용한 Fuzzy ART 침입탐지엔진이다. 이러한 Fuzzy ART 의 능력은 네트워크상의 트래픽 패턴을 모델링하는데 매우 적합하다고 할 수 있다. 대량의 데이터가 생성되는 네트워크 트래픽의 특성상 패턴 모델링 과정에서의 빠른 학습 능력은 필수적인 요소라고 할 수 있다. 또한 이전에 학습된 패턴을 일관되게 처리할 수 있는 능력은 정확한 패턴 분류와 점증적 갱신을 위한 필수 요소라 할 수 있으며, 새로운 클러스터의 생성을 새로운 침입 유형의 발견으로 보기 때문에 알려지지 않은 침입 유형에 유연하게 대처할 수 있으며 조기 침입탐지가 가능하다.

4. 협동적 침입탐지 시스템

본 논문에서 제안하는 침입탐지 시스템은 대규모 네트워크에서 서로 분산된 침입 탐지 에이전트들이 해당 지역에 대한 침입탐지를 책임지고, 각 에이전트들은 서로 정보를 교환함으로써 새로운 침입에 대한 협동적 탐지가 가능할 뿐만 아니라 조기 경보 체계를 이룰 수가 있다. 다음 [그림 2]는 이러한 협동적 침입탐지 프레임워크를 나타낸다. 각 침입탐지 에이전트는 supervisor 에이전트로부터 받은 침입 패턴 베이스를 바탕으로 침입을 탐지한다. supervisor 는 새로운 침입에 대한 패턴이 생성되면 각 지역네트워크 manager 에이전트에게 전송하여 각 에이전트들의 침입패턴 베이스를 갱신한다.

Fuzzy ART 엔진은 소량의 패턴 벡터 값만 전송하면 되므로 기존의 시스템들에서처럼 대량의 데이터를 전송할 필요도 없을 뿐만 아니라 각 에이전트가 패턴베이스를 저장하기 위해 별도의 DB 또는 파일 시스템을 유지할 필요가 없다. 그러므로 에이전트가 가볍게 운용될 수

있으며 침입탐지 또한 실시간으로 처리할 수 있다.



[그림 2] 협동적 침입탐지 프레임워크

이렇게 정제된 데이터를 바탕으로 Fuzzy ART 엔진은 침입패턴을 생성하고 이 패턴 베이스를 바탕으로 실시간 침입탐지를 수행한다. 침입 탐지에 사용되는 패턴 베이스는 Fuzzy ART 의 weight 에 해당하는 소량의 턴 벡터 값이므로 각 에이전트들은 메모리에 올려놓고 침입탐지를 수행할 수 있다. 또한 각 에이전트들은 새로운 침입에 대한 정보를 manager 에게 전달하고 manager 는 이를 종합하여 supervisor 에이전트에게 전달함으로써, 기존에 알려지지 않은 침입 정보를 갱신할 수 있다. 또한 각 에이전트는 침입 징후를 발견하면 조기 경보를 발령함으로써 모든 에이전트들이 침입에 대처하여 DDOS 와 같은 공격 및 인터넷웜의 피해를 예방 할 수 있다.

5. 실험 및 성능 평가

Fuzzy ART 엔진에 대한 성능 평가는 DARPA 에 의해 수집된 KDD CUP 99 데이터를 이용하였다[5]. 이 데이터는 1998 년 MIT Lincoln Labs.에 의해 DARPA Intrusion Detection Evaluation Program 의 하나로 미국 군사 네트워크상에서 시뮬레이션을 통한 TCP dump 데이터 이다. 테스트용 데이터는 7 개의 symbolic 속성과 34 개의 numeric 속성으로 구성되어있다. 데이터는 크게 4 개의 공격 유형으로 구분되며, 세부적인 공격 유형은 총 37 가지 종류의 공격 방법으로 구성되어 있다.

본 논문에 사용된 침입탐지 알고리즘을 평가하기 위해 탐지율과 False-Positive 오판율, False-Negative 오판율을 테스트 하였다.

탐지율=올바르게 판정된 침입 수/전체 침입 행위 수
False-Positive 오판율= 오판 수/정상행위 수
False-Negative 오판율=탐지 못한 수/침입행위 수

Fuzzy ART 의 선택 변수 α =0.001, β =0.9 로 초기화 하였으며, 경계값 매개변수(vigilance parameter) ρ 값을 조정해 가면서 탐지율과 오판율을 측정하여 [표 2],[표 3]과 같은 결과를 얻었다.

[표 2] 탐지 성능 평가 결과

ρ =0.92	탐지율	F-P 오판율	F-N 오판율
	92.02%	22.71%	5.31%

[표 3] 공격 유형에 따른 탐지율

공격유형	탐지율
DoS	91.2%
R2L	61.4%
U2R	57.2%
Probing	90.7%

결과에서처럼 경계값 매개변수의 값이 0.92 일 때 가장 높은 탐지율을 나타내었다. False-Positive 오판율은 비교적 높게 나타났고 False-Negative 오판율은 낮게 나타났는데 이것은 침입탐지 정책에 맞게 경계값을 조절하면서 선택하는 것이 바람직하다. 각 공격 유형 별 탐지율은 DoS 공격과 Probing 공격의 경우가 탐지율이 좋게 나타났다.

6. 결론

최근의 고속화된 네트워크 환경에서는 오히려 침입이나 바이러스 유포가 이루어지는 최적의 환경을 제공하고 있다. 침입의 형태가 분산화되고 다양화됨에 따라 침입탐지는 날로 어려워 지고 있는 상황에서 실시간으로 네트워크 침입탐지가 가능한 시스템은 절실히 요구되고 있다. 따라서 본 논문에서 제시한 침입 탐지 시스템은 실시간 패턴 매칭이 가능한 Fuzzy ART 알고리즘을 사용함으로써 이러한 요구에 적합하다 할 수 있다. 또한 대규모 네트워크에서 침입 탐지 시스템의 분산화 및 계층화는 침입탐지 시스템이 앞으로 나아갈 방향이라 할 수 있다. 향후 연구과제로는 보다 정확한 탐지를 위해 침입 판정 요소에 대한 구체적인 연구가 필요하며, 서로 다른 형태의 네트워크 환경에서의 침입 탐지를 위한 표준에 관한 연구도 수행되어야 할 것이다.

7. 참고문헌

[1] Wenke Lee, et al., "Real Time Data Mining - based Intrusion Detection", IEEE, 2001.

[2] J. Cannady, "Artificial Neural Networks for Misuse Detection," NISSC, October 1998.

[3] Dunigan T, Ostrouchov. G, "Flow Characterization for Intrusion Detection", ORNL, TM-2000.

[4] G. A. Carpenter, et al., " Fuzzy-ART : Fast stable learning and categorization of analog patterns by an adaptive resonance system", Neural Networks, 1991.

[5] Results of the KDD '99 Classifier Learning Contest, http://www-cse.ucsd.edu/users/elkan/clresults.html