Fuzzy ART를 이용한 실시간 침입탐지

한광택[0] 김형천 고재영 이철원
국가보안기술연구소
kthan@etri.re.kr

Real-Time Intrusion Detection using Fuzzy Adaptive Resonance Theory

Kwangtaek Han[0], Hyoungchun Kim, Jaeyoung Koh, Cheolwon Lee
National Security Research Institute

요 약

침입 탐지 시스템의 초점이 호스트와 운영체제 탐지에서 네트워크 탐지로 옮겨가고 있고 단순한 오용 탐지 기법에서 이를 개선한 지능적인 비정상 행위 탐지 기법에 관한 연구들이 진행되고 있다. 이러한 연구들 중에는 네트워크 프로토콜의 트래픽 특성을 이용하여 비표준 포트의 사용이나 표준 포트에 대한 비표준 방법에 의한 침입을 탐지하고자 하는 노력도 있다. 본 연구에서는 실시간으로 패턴 매칭이 가능하고, 적응력이 뛰어난 신경망 알고리즘을 이용하여 네트워크 서비스들에 대한 트래픽을 수집, 특성에 따라 분석·클러스터링하고 그 결과를 바탕으로 보다 향상된 침입 탐지가 가능한 시스템을 제안한다.

1. 서 론

네트워크 기반의 침입 공격이 일반화되고 정교해짐에 따라 침입탐지의 초점은 호스트 침입탐지에서 네트워크 침입탐지로 옮겨가고 있다. 네트워크 기반의 침입탐지는 시스템 로그 정보를 대상으로 하는 호스트 기반의 탐지와는 달리 네트워크 상의 패킷 헤더 및 데이터를 분석하거나 트래픽 특성에 대한 통계를 분석하여 침입 유무를 판단한다. 네트워크 서비스 트래픽의 특성을 판단 기준으로 하는 네트워크 기반 침입탐지는 모든 표준 네트워크 서비스들이 일정한 트래픽을 가진다는 특성을 이용[1]하여 비표준 포트의 사용이나 탐지로부터 빗겨가기 위해 표준 포트를 비표준화된 방법으로 사용하는 행위를 탐지한다[2]. 이러한 침입 탐지는 서비스가 갖는 네트워크 트래픽 패턴을 찾아냄으로써 침입을 판단할 수 있다.

침입탐지 시스템에서의 기술적 관건은 컴퓨터 시스템의 침입여부를 판단하기 위한 근거를 어디에서, 얼마나 정확하게, 그리고 신속하게 찾을 수 있느냐에 달려 있다. 그리고 오류 없이 침입여부를 판단하는지의 문제도 기술적으로 해결해야 한다.

따라서 본 연구에서는 속도 면에서 매우 우수하고 적응력이 뛰어난 신경망 알고리즘의 하나인 Fuzzy ART (Adaptive Resonance Theory)를 이용한 클러스터링 방법을 이용하여 보다 능동적이고 실시간으로 침입을 탐지가능한 시스템을 제안하고자 한다.

2. 관련연구

COAST는 침입탐지를 오용탐지와 이상탐지로 분류하고 있다. 오용탐지는 알려진 취약점들을 이용하여 공격하는 행위들을 사전에 공격 특징 정보를 가지고 있다가 탐지하는 방법으로, 전문가시스템, 페트리넷, 상태전이분석 등이 있으며 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[3].

또 다른 유형인 이상탐지는 정상행위 모델을 벗어나는 경우를 침입으로 간주하는 방법으로써 통계적으로 처리된 과거의 경험 자료를 기준으로 특별한 행위 또는 유사 사건으로부터의 이탈을 탐지하는 통계적인 방법, 경험적인 침입탐지 측정 도구와 침입의 예측 및 분류 가능한 침입 도구의 집합으로 구성된 침입을 탐지하는 특징 추출 방법, 이벤트간의 상호관계와 순서를 설명하고, 각각의 이벤트에 시간을 부여하여 기존에 설정된 침입 시나리오와 비교하여 침입을 탐지하는 예측 가능한 패턴 생성을 이용한 방법 등이 있다. 이 모델은 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 기법 중에서 클러스터링 기법을 활용하고 있다.

[4]는 사용자 행위를 클러스터링 함으로써 이를 이용하여 비정상적인 행위를 탐지하였고, [2,5]는 네트워크 서비스별 트래픽 특징에 대한 클러스터링을 이용하여 비정상행위 침입을 탐지하였다.

신경망을 이용한 침입탐지는 이론적으로 지식기반 침입탐지 방식에서 공격을 학습하고 감사 스트림에서 탐색

하는데 사용될 수 있는데 [6]은 분석된 패킷 데이터 부분에서 신경망을 적용하였고, [7]은 보다 향상된 오용탐지를 위해 신경망 알고리즘인 Back Propagation을 적용하였다.

3. Packet Filtering

네트워크 트래픽을 이용한 침입탐지를 하기 위해서는 신경망 알고리즘의 적용과 같은 학습 즉, 클러스터링이 이루어져야 한다. 이러한 학습과 침입탐지를 위해서 네트워크 트래픽으로부터 패킷의 크기(packet size), 패킷간의 지연(inter-packet delay), 패킷의 방향(direction)과 같은 정보의 수집이 선행되어야 한다[1].

보다 정확한 침입탐지를 위해서는 의미 있는 패턴 정보를 얻어야 하므로, 신경망 적용을 통한 효율적인 클러스터링을 위해 패킷으로부터 다음의 주요 판정요소 필드만을 추출함으로써 효율성을 증대시켰다.

- 근원지 주소(Source Address)
- 목적지 주소(Destination Address)
- 패킷의 크기(packet size)
- 목적지 주소 포트(Destination Port)
- 플래그 정보(Flag Set)

본 연구에서는 네트워크 서비스 중에서 TCP 프로토콜 telnet, ftp, smtp에 대한 패킷을 수집 분석하였는데 그 결과 [7]과 같은 결과를 얻을 수 있었다.

<표1> 네트워크 트래픽 수집

프로토콜	트래픽 수	에러 비율
telnet	182	3%
ftp	322	2%
smtp	874	6%

<표1>은 Tcpdump를 이용하여 수집한 감사 데이터의 통계 정보로써 감사데이터 수집을 [2]에서처럼 제한을 두었다.

4. Fuzzy ART를 이용한 트래픽 클러스터링

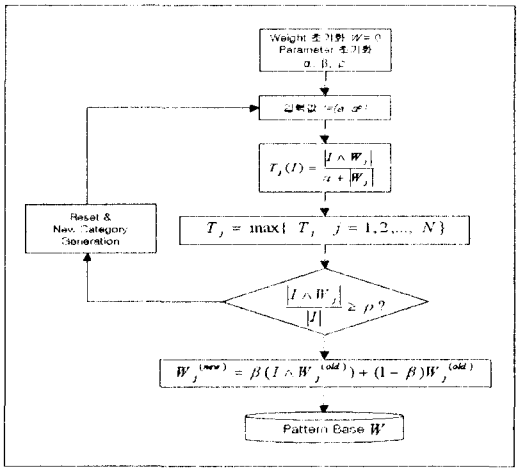
네트워크 상의 트래픽을 클러스터링 하기 위해 사용한 신경망 모델인 Fuzzy ART는 다음과 같다.

4.1 ART 신경망 모델

ART는 경쟁학습의 약점인 안정성을 보강하여 제안된 모델이다. ART 모델의 가장 큰 장점은 기존에 학습되었던 것이 새로운 학습에 의해 지워지지 않도록 새로운 지식을 자동적으로 전체 지식 베이스에 일관성 있는 방법으로 통합한다. 즉 적절하게 매칭되는 새로운 정보를 이용하여 이미 배운 내용들을 정제하며, 새로운 인식 카테고리의 학습을 위하여 새로운 유닛을 선택하고, 기억용량을 넘어서는 과다한 새로운 입력에 의해 기존에 취득한 내용이 지워지는 것을 방지한다. 따라서 끊임없이 변하는 환경에서 자신의 메모리 용량을 전부 소모할 때까지는 제한 없는 입력에 대해 실시간으로 빠르고 안정되게 배울 수 있는 구조이다.

4.2 Fuzzy ART 구조 및 알고리즘(Algorithm)

Fuzzy ART 모델[8]은 ART1 모델이 이진(binary)값만을 처리하는 특성을 발전시켜 아날로그 값을 처리할 수 있게 만든 것으로 서로 매우 유사한 형태를 가지고 있다. ART1에서 사용되는 논리곱 연산자 ∩을 퍼지 집합이론의 최소화 연산자 ∧으로 대체하여 사용함으로써 퍼지 연산자가 갖는 특성인 0과 1사이의 값을 처리할 수 있도록 하였다. (그림1)은 본 논문에서 사용한 Fuzzy ART 알고리즘이다.



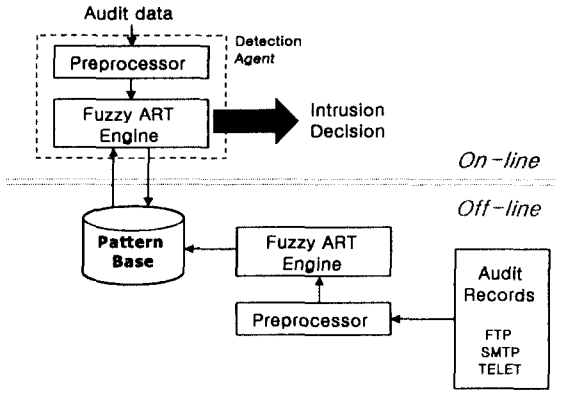
(그림1) Fuzzy ART 알고리즘

Fuzzy ART는 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, ART는 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. 이러한 Fuzzy ART의 능력은 네트워크상의 트래픽 패턴을 모델링하는데 매우 적합하다고 할 수 있다. 대량의 데이터가 생성되는 네트워크 트래픽의 특성상 마이닝 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 있다.

5. 실험 및 성능 평가

본 연구에서 제안하는 시스템은 크게 두 부분으로 나눌 수 있다. 먼저 telnet, ftp, smtp에 관련된 방대한 양의 트래픽 데이터를 수집하여, 전처리 과정을 거친 후

Fuzzy ART를 이용하여 트래픽 패턴베이스를 생성하는 오프라인(off-line) 부분과, 실시간으로 네트워크의 트래픽을 관찰하여 구해진 패턴 베이스와 매칭함으로써, 침입자를 판별해 내는 온라인(on-line) 부분으로 구성된다. 전체 시스템 구성은 (그림2)와 같다.



(그림2) Fuzzy ART를 이용한 침입탐지 시스템 구성

제안된 시스템의 패턴 모델링 성능을 평가하기 위해, 3장에서 제시한 방법을 통해 패킷을 필터링 하였는데 의미 있는 클러스터링을 위해 프로토콜별로 패킷 크기, 패킷간의 간격, 패킷 방향을 나타내는 정보만을 추출하였다. 그 이유는 클러스터링에 영향을 주지 못하는 데이터는 오히려 전처리 과정에서의 계산량 증가뿐만 아니라, 의미 있는 클러스터링 과정에 악영향을 미칠 수 있기 때문이다. 필터링 된 데이터는 Fuzzy ART에서 이용할 수 있는 형태로 바꾸어주어야 하는데 이는 전처리 모듈에서 이루어진다. 전처리 모듈을 거친 네트워크 트래픽은 4차원 벡터의 형태로 처리되어 Fuzzy ART 엔진을 통해 클러스터링이 수행된다. 각 프로토콜별로 Fuzzy ART의 경계값을 조정하며 클러스터링 된 결과를 나타내면 다음 <표 3, 4, 5>와 같다. 선택 매개변수 α=0.001, 학습률 β=0.9로 초기화하였다.

<표3> TELNET에 대한 클러스터링 결과

vigilance parameter(ρ)	0.85	0.90	0.92	0.95	0.97	0.98
클러스터 수	3	5	5	6	7	10

<표 4> FTP에 대한 클러스터링 결과

vigilance parameter(ρ)	0.85	0.90	0.92	0.95	0.97	0.98
클러스터 수	7	8	10	10	13	17

<표 5> SMTP에 대한 클러스터링 결과

vigilance parameter(ρ)	0.85	0.90	0.92	0.95	0.97	0.98
클러스터 수	5	7	8	10	13	16

결과에서처럼 네트워크 상에서 telnet, ftp, smtp 서비스를 이용하는 패턴은 그 유사도에 따라서 수 개의 클러스터로 나뉜다. Fuzzy ART의 경계값을 높게 할수록 클러스터의 수가 증가하는 것을 볼 수 있다. 이는 보다 세분화되고 구체적인 클러스터들이 생성됨을 나타낸다. 따라서 관리자의 결정에 따라 클러스터링 결과를 조정할 수 있는 장점을 갖고 있다. 이렇게 생성된 패턴 베이스를 기반으로, 탐지 에이전트는 감시된 트래픽을 이용해 전처리 과정을 거친 후, Fuzzy ART의 학습 부분을 제외한 패턴 매칭 알고리즘을 이용하여 침입자를 판별한다. 또한 판별된 침입에 대해 경로 차단뿐만 아니라 공격패턴에 대한 리포팅이 수행되어야 한다.

5. 결론 및 향후 연구과제

최근 실시간 네트워크 침입탐지 연구가 진행 중에 있다. 이에 대한 탐지 방안으로 네트워크 트래픽의 특성을 이용한 방안이 제시되고 있고 이러한 방대한 데이터 분석을 좀더 지능적이고 자동적으로 수행하기 위해 데이터 마이닝 기법 중에서 클러스터링 기법을 활용하고 있다. 이러한 트래픽의 클러스터링은 시간이 지남에 따라 클러스터링이 매우 유동적으로 변경될 수 있다. 이에 본 연구에서는 Fuzzy ART 신경망 알고리즘을 적용함으로써 트래픽 클러스터링의 실시간적인 변동을 통해 보다 정확한 탐지를 고려하였다. 향후 연구 과제로는 새로운 공격에 대한 탐지능력을 높이기 위해 판정요소에 대한 더 구체적인 연구가 필요하며, 다양한 공격을 탐지하기 위해 모델의 특성에 따른 탐지영역을 구체화 할 수 있는 연구가 이루어져야 할 것이다.

[참고문헌]

[1] Thompson. K, Miller. G. J, Wilder. R, "Wide-Area Internet Traffic Patterns and Characteristics," IEEE Network , Volume 11, Issue 6 , pp. 10-23, Nov./Dec. 1997.

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

[3] 주운기 "정보보안을 위한 침입탐지 기술," 한국경영학회/대한산업공학회 춘계공동학술대회, 27-28, 2001.

[4] 오상현 "사용자 행위 클러스터링을 활용한 비정상 행위 탐지," 한국정보처리학회 논문지, 제7권, 2000.

[5] 박보석, 장희진, 김홍철, 송병욱, 박인성, 김상욱, " 네트워크 흐름 클러스터링에 의한 침입탐지," 학술발표회 논문집, 한국통신정보보호학회영남지부, 2001

[6] Bonifacio. J. M. Jr, Cansian. A.M , De Carvalho. A. C. P. L. F, Moreira. E. S, "Neural Networks Applied in Intrusion Detection System," In Proc. of the 1998 IEEE World Congress on Computational Intelligence, pp. 205 -210, 1998.

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

[8] G. A. Carpenter, S. Grossberg and D. B. Rosen, "Fuzzy-ART: Fast stable learning and categorization of analog patterns by an adaptive resonance system", Neural Networks, vol.4, pp.759-771, 1991.