초록

본 논문에서는 서비스 거부 공격 탐지 NIDS 개발에서 ANN의 중요성을 제안한다. 제안된 ANN 기반 NIDS는 첫 번째 단계에서 입력 패킷을 DoS, U2R, R2L, PROBING의 4개 범주로 분류한다. 두 번째 단계에서 NIDS 시스템은 DoS 공격을 Smruf, Teardrop, Neptune, Land, Pod, Back으로 탐지하도록 향상될 수 있다. 이렇게 개발된 NIDS는 인공 신경망 구성 시 은닉층의 수를 증가시킴으로써 오진과 미탐지율을 최소화할 수 있다.

1. 침입탐지 시스템이란?

IDS(침입 탐지 시스템)는 악의적인 활동이나 정책 위반에 대해 네트워크 및 시스템 활동을 모니터링하고 관리 스테이션에 보고서를 생성하는 장치 또는 소프트웨어 응용 프로그램이다.

IDS의 목적

컴퓨터 시스템이 공격에 대처하는 방법에 대해 도움을 주는 것이며, IDS는 컴퓨터 시스템과 네트워크 내의 여러 다른 소스로부터 정보를 수집하고 공격 또는 취약점이 있는지 여부에 대해 기존의 차별 패턴과 이 정보를 비교한다. 기존 IDS는 데이터를 일반 데이터 또는 공격 데이터로 분류할 수 있는 반면 현대 IDS는 들어오는 공격을 다음의 주요 4가지로 분류할 수 있다.

1. DOS: 서비스 거부
2. R2L: 원격 시스템에서 무단 액세스
3. U2R: 로컬 슈퍼 사용자(루트) 권한에 대한 무단 액세스
4. PROBING: 감시 및 기타 조사

새로운 기술 사용의 필요성

공격자와 침입자는 매우 지능적이며 조직 인트라넷에 침투하기 위한 새롭고 정교한 기술을 개발한다. 따라서 우리의 방어 시스템은 새로운 공격 패턴과 취약점을 탐지하기 위해 새로운 방법론을 사용해야 한다.

인공 신경망(Artificial Neural Network), Support Vector Machine, 데이터 마이닝 또는 기계 학습 알고리즘 중 하나를 기반으로 IDS를 설계하고 구현해야 한다. 본 논문에서는 인공 신경망을 사용하여 NIDS를 개발할 것을 제안한다.

2. 조사

IDS의 분류

연구자들은 행동, 사용 및 탐지 기술에 따라 다양한 유형의 침입 탐지 시스템을 제안하고 있다.

1. 오용 탐지 기반 또는 서명 기반 IDS
2. 이상 탐지 기반 또는 휴리스틱 또는 동작 기반 IDS
3. 호스트 기반 시스템
4. 네트워크 기반 또는 NIDS
5. 패시브 시스템 IDS
6. 반응형 시스템 IDS
7. 오프라인 IDS
8. 온라인 IDS

다양한 AI 유형
NIDS 설계에는 유전 알고리즘(Genetic algorithm), 퍼지 논리(Fuzzy logic), 확률론적 추론(Probabilistic reasoning), 인공신경망(Artificial Neural Network), Support Vector Machine, Decision Tree 등 다양한 기술이 활용되어 왔다. 이러한 기술들을 조합하여 사용하는 것도 가능하다.

- 유전 알고리즘은 최적의 해를 찾기 위해 세트의 값을 무작위화하고 계속해서 혼합하고 구별하여 반복적으로 최적의 해를 찾는다.
- 확률론적 추론 기반 IDS는 Bayesian 네트워크를 사용하여 침입 가능성을 평가하며, 다중 에이전트 시스템을 통해 서로 다른 침입을 탐지하고 효율성을 높인다.
- SVM 기반 IDS는 지도 학습 방법으로 데이터를 이진 형식으로 분류하여 공격 데이터를 특정 범주로 분류한다.

표 1 AI 기술 비교 분석

번호	기술	데이터 세트	장점	단점
1	Decision Tree	KDD99	1. 간단한 사용법 2. 여러 데이터베이스와 함께 작동 3. 낮은 오분류율	1. 패턴 찾기 프로세스는 시간이 많이 소요
2	Genetic Algorithm	KDD99	1. 분류 규칙은 네트워크 감사 데이터에서 파생 2. 기술은 데이터 세트에서 독립적	1. 알 수 없는 공격에 대한 탐지율이 낮음
3	SVM	KDD99	1. 41개의 기능이 29개로 감소 2. 중요하지 않은 기능이 제거	1. 전체 교육 데이터 세트를 처리할 수 없음 2. 특정 범주로 분류할 수 없음

표 1은 IDS 구현에 사용되는 서로 다른 기술의 긍정적인 측면과 부정적인 측면을 각각 보여준다.

ANN 장점
1. 자체 학습 기능이 있습니다.
2. 신경망의 요소가 실패해도 병렬 특성으로 인해 문제 없이 계속할 수 있다.
3. 신경망은 학습하므로 다시 프로그래밍할 필요가 없다.
4. 공격을 감지하는 동안 빠르고, 유연한다.
5. 유사한 기능을 공유하는 패턴을 클러스터링할 수 있으므로 ANN을 Dos 공격 탐지에 사용한다.
6. ANN을 이용하여 공격 문제의 분류를 풀 수 있다.

3. 인공 신경망

ANN을 사용하여 네트워크의 패킷을 정상 또는 공격으로 분류하려면 다음 단계가 사용된다.
1. 신경망의 입력 노드의 개수를 제시한다.
2. 특정 입력에 대해 생성된 실제 출력이 원하는 출력과 얼마나 근접하게 일치하는지 확인한다.
3. 출력에 더 근접하도록 신경망 매개변수를 변경한다.

공격을 특정 DoS 공격으로 분류하기 위해 따라야 할 단계는 다음과 같다.
1. NIDS를 위한 입력 및 출력이 적은 간단한 ANN 설계
2. 합성 입력으로 ANN 기반 NIDS 학습
3. 합성 입력을 사용하여 대표적인 DoS 공격에 대해 ANN 기반 NIDS를 테스트
4. 다른 DoS 공격에 대한 NIDS 확장
5. Feature Extraction 알고리즘 개발 및 NIDS와 통합
6. 전체 테스트 및 검증

본 논문은 Smurf, Teardrop, Neptune, Land, Back, Pod 등과 같은 서비스 거부 공격을 탐지할 ANN 기반 NIDS의 중요성을 제시한다.

4. 결론

ANN 기반의 NIDS는 Shrub, Teardrop, Neptune, Land, Pod, Back과 같은 다양한 유형의 DoS(서비스 거부) 공격을 빠른 시간 내에 감지하는 데에 사용될 수 있다. ANN MATLAB의 Neural Network Toolbox를 기반으로 하는 NIDS 구현을 위해 사용할 수 있다. 제안하는 NIDS는 낮은 오류율, 높은 학습률 및 빠른 응답률을 가질 수 있다. 더 나은 훈련이 이루어지면 동일한 NIDS를 사용하여 알려지지 않은 공격도 탐지할 수 있다.