1. 소개

침입탐지 : 네트워크의 핵심 노드에 대한 정보를 수집하고 분석하여 위반된 보안 동작이나 공격 의 징후가 있는지 찾는 것

침입 탐지 시스템(IDS) : 네트워크 시스템의 보안을 보장하기 위해 로컬 네트워크 서비스를 제공 하는 독립적인 시스템

학계와 산업계에서 IDS에서 머신러닝방법을 적용하는 많은 연구가 있다.

전통적인 IDS : 침입 및 공격 모드의 특징을 추출 하고 분석 -> 다음 침입 패턴 라이브러리와 일련의 식 별 규칙을 구축하여 침입을 탐지

Sujendran과 Arunachalam111은 공격을 식별하기 위해 Wiener 필터와 결합된 자동 퍼지 규칙 생성을 제안

**Yaseenet al**

공격 에 SVM(Support Vector Machine)과 익스트림 러닝 머신을 사용하는 다단계 하이브리드 침입탐지 모델을 제안

K-평균 알고리즘은 훈련 시간을 줄이고 IDS의 성능 향상을 위해 전체 원본 훈련 데이터 세트를 나타내는 새롭고 작은 훈련 데이터 세트를 구축하는 데에도 사용됨

**Kaur et al.**

이상 탐지를 위한 K-수단과 firefly 알고리즘의 하이브리드화를 제안

(이 알고리즘은 클러스터링 을 사용하여 훈련 모델을 구축하고 분류를 사용하여 테스트 세트를 평가한다)

결과는 K-means + firefly 와 K-means + bat다른 방법보다 월등히 뛰어나다는 것을 보여줌

**Tahiret al.**

K-means와 SVM을 결합한 하 이브리드 방식을 이용한 공격 시스템 연구

Deep Confidence Network를 이용하여 침입을 탐지하였고, 알고리 좀 테스트를 위해 KDD Cup 99데이터를 사용

결과는 기존 SVM모델 및 ANN모델과 비교하여 정밀도 6% 이상 향상됨

**Lin et al. re**

CANN(Cluster Center and the Nearest Neighbor) 접근 방식을 제안

결과는 KDD99에 기반한 실험 결과는 CANN분류기가 K-NN 및 SVM 훈련된 방법보다 더 우수하거나 유사

[5]트리 가중 나이브 베이지안 알고리즘을 제안

[6]새로운 버 전의 지원 벡터 도메인 설명을 사용하여 추출된 특징을 분류하 고 새로운 침입을 탐지

[12] Dempster–Shafer 신념 이론을 사용하여 다중 메트릭을 융합하여 무선 네트워크에서 주입 유형의 공격을 탐지

규칙기반 머신러닝 : K-means, SVM, K-NN, clustering, regression

분류방법 : Naïve Bayesian, Random Forest

이와 비교하여 DNN은 낮은 오탐률로 더 높은 정확도와 탐지율을 얻는다. 심층 네트워크 구조로 추상적인 침입 특징을 추출할 수 있고 큰 탐지 가능성을 예측할 수 있다.

1. 심층 신경망

침입의 특징학습 및 패턴분류를 위해 계층적 방식의 연속 레이어가 사용됨.

-분류자가 ‘정상’데이터로만 훈련되는 준감독 이상 감지 시스템을 구현하기 위해 머신러닝기술 채택

-RBM(식별 제한 볼츠만 머신)을 사용하여 생성 모델의 표현력을 우수한 분류 기능과 결합 후 불완전한 교육 데이터에서 지식의 일부를 추론(정확도 94%)

-MIXMAD 제안 (다양한 깊이의 신뢰망(DBN)의 앙상블 구성-비지도 탐지 방법보다 우수)

-DBN 과 RBN 혼합사용 전체 10% KDDCUP99테스트 데이터 세트에서 97.9%의 탐지율을 달성

-DBN(차원 축소,최적화) 과 PNN(probabilistic neural network)을 이용한 침입 탐지 방법 제안

텍스트, 스크린샷, 도표, 폰트이(가) 표시된 사진

자동 생성된 설명

왼쪽 : 훈련 과정

오른쪽 : 탐지 과정

NSL-KDD데이터 세트는 독학 학습(STL)을 사용하고 모든 유형의 분류에 98%이상의 정확도 보임

(훈련 시간을 계산하고 탐지 메커니즘의 효율성을 분석하는 데 사용됨)

-네트워크 데이터의 이상을 식별하기 위해 가속 DNN 아키텍처를 개발

-다양한 유형의 침입 공격에 대한 분류자로서 DNN이 SVM 침입 탐지보다 잘 작동한다는 것을 보여줌

-순환 신경망(RNN-IDS)을 제안 (J48, 인공 신경망, 랜덤 포레스트, SVM 등 머신러닝 방법과 비교)

분류 모델을 모델링에는 RNN-IDS가 높은 정확도를 보여줌

침입 탐지 정확도를 더 향상시키기 위해 새로운 DNN(NDNN) 모델을 구축하고 테스트한다.

IDS는 데이터 전처리, 특징 학습 모듈 , 침입 유형 분류 모듈로 나뉨

1. 데이터 전처리

데이터 확인

KDD99 와 NSL-KDD 데이터셋을 훈련/테스트 데이터셋 사용

텍스트, 폰트, 스크린샷, 화이트이(가) 표시된 사진

자동 생성된 설명

ㄴ원래 침입 데이터 레코드

텍스트, 스크린샷, 폰트, 문서이(가) 표시된 사진

자동 생성된 설명

텍스트, 스크린샷, 폰트, 영수증이(가) 표시된 사진

자동 생성된 설명

ㄴ 침입 유형

X에는 42개의 속성, 41개의 특징 및 레이블

Smurf는 레코드 x의 레이블

1.데이터 필터링

1-1.실제 캡처된 데이터에서는 많은 침입 레코드가 동일하므로 정보 중복 제거와 IDS에 입력되는 데이터의 양을 줄이기 위해 중복 제거를 사용한다. (KDD99 데이터 세트는 이미 중복 제거 됨)

1-2.모든 데이터를 숫자 형식으로 변환

변환규칙 :

1. Protocal type: 1 icmp; 2 tcp; 3 udp; 4 others.
2. Service: 1 domain-u; 2 ecr\_i; 3 eco\_i; 4 finger; 5 ftp\_data; 6ftp; 7 http; 8 hostnames; 9 imap; 10 login; 11 mtp; 12 netstat; 13other; 14 private; 15 smtp; 16 systat; 17 telnet; 18 time; 19 uucp;20 others.
3. Flag: 1 REJ; 2 RSTO; 3 RSTR; 4 SO; 5 S3; 6 SF; 7 SH; 8 OTHERS

land, logging\_in, is\_host\_login, is\_guest\_login을 포함한 기능은 값이 0 또는 1

작은 숫자 속성이 사라지고 계산 반복 횟수를 줄이기 위해 숫자 데이터는 아래 선형 함수를 사용하여 [0.1]로 정규화된다.



xmin 및 xmax는 모든 요소의 최소값과 최대값

x의 42번째 속성을 나타내기 위해 ‘원핫인코딩’ 사용(모두 같은 가중치를 가지며 분류자에게 편향되지 않음)

텍스트, 스크린샷, 폰트, 대수학이(가) 표시된 사진

자동 생성된 설명

1. NDNN 모델 설계

4.1 NDNN 구조 건물

DNN은 하나 이상의 히든 레이어가 존재

DNN은 복잡한 비선형 시스템을 위한 모델링 제공

추가 레이어는 모델의 기능을 향상시키기 위해 훨씬 더 높은 수준의 추상 기능 제공

NDNN : 입력 레이어, 히든 레이어, 출력 레이어로 구성

구조 : 41개의 뉴런이 있는 입력 레이어,

레이어당 100개의 뉴런과 4개의 히든 레이어,

5개의 뉴런이 있는 1개의 완전연결(FC) 레이어,

Softmax 레이어 및 5개의 뉴런이 있는 출력레이어

도표, 라인, 스크린샷, 텍스트이(가) 표시된 사진

자동 생성된 설명

4.1.1 입력 및 히든 레이어 : 입력 벡터 X와 출력 벡터 Y간의 복잡한 매핑 관계

입력 벡터X : 하나의 침입 기록에 대한 41차원 특징 벡터

출력 벡터Y : 0과 1 사이의 값을 갖는 5차원 확률 벡터 (각 값은 입력이 어떤 종류의 침입(4가지 유형의 공격과 1개의 일반 데이터)에 속하는 확률을 나타냄)

숨겨진 레이어 뉴런의 출력 방정식

폰트, 타이포그래피, 화이트, 서예이(가) 표시된 사진

자동 생성된 설명

연결된 모든 레이어 뉴런의 출력 방정식



g(·)는 NDNN 히든 레이어의 활성화 함수.

W는 입력/히든 레이어 사이의 가중치 .

b는 히든 레이어의 편향 .

β는 히든/FC 레이어 사이의 가중치.

D는 FC 레이어의 편향

텍스트, 친필, 폰트, 도표이(가) 표시된 사진

자동 생성된 설명H는 히든 레이어의 출력 행렬.

Β는 히든 계층과 FC 계층 간 연결 가중치 행렬

Z 는 FC레이어의 출력 행렬

NDNN에서는 히든 레이어의 활성화 함수로 ReLU(비선형)를 사용

텍스트, 스크린샷, 문서, 폰트이(가) 표시된 사진

자동 생성된 설명

텍스트, 영수증, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명

무작위 최적화 방법인 Adam 사용

LR의 초기값 0.001

4.1.2 FC 계층

-NDNN 은 알려지지 않은 침입 데이터를 식별하고 분류하는데 사용

-히든 레이어의 출력은 데이터의 상위 수준 기능을 나타내며 이러한 데이터는 5가지 유형의 침입으로 분류

FC 계층은 특징을 5개의 클래스로 매핑하도록 설계

5개의 노드 중 네 번째 계층의 100차원 특징은 5개의 클래스로 매핑

마지막 계층은 softmax 분류기

* 1. 텍스트, 라인, 도표, 스크린샷이(가) 표시된 사진

     자동 생성된 설명네트워크 매개변수 선택

네트워크 계층 번호, 네트워크 노드 번호가 다른 네트워크 구조의 여러 테스트 정확도를 보여줌

4개의 히든 레이어와 100개의 노드가 있을 때 최고의 성능을 나타냄

1. 실험

KDDCUP 1999 데이터셋과 NSL-KDD 데이터셋을 사용

Intel Core i7–5820k(R) 중앙 처리 장치(3.70GHz), 16GB 메모리 및 GeForce GTX10 60 GPU가 장착된 PC의 tensorflow 1.0에서 실행

5.1데이터셋

-세트에는 Probe, Dos, U2R 및 R2L 네가지 유형의 침입이 있다.

-KDD99 데이터셋에서는 전체의 10%만 선택

-‘kddcup.data\_10\_percent’의 데이터셋에는 494021개의 연결 레코드(그 중 90%는 훈련 세트로 무작위로 선택 10%는 테스트셋으로 사용.(이전에 발생하지 않은 공격 유형도 포함)

-NSL-KDD에서도 테스트

5.2실험 결과 분석

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

텍스트, 영수증, 폰트, 화이트이(가) 표시된 사진

자동 생성된 설명

많은 실험 후에 최상의 매개변수를 선택하고 저장하며 훈련된 IDS 모델이 보존됩니다. 그런 다음 나머 지 10% 데이터를 테스트 데이터 세트로 사용합니다. 테스트 데이터는 네트워크에 입력되어 단일 유형 공격의 탐지 성능을 테스트합니다.

텍스트, 스크린샷, 평행, 도표이(가) 표시된 사진

자동 생성된 설명

데이터 규모(침입 기록이 더 많이 수집될수록)가 클수록 탐지 결과가 더 좋다.

훈련 데이터의 수는 DoS>Normal>Probe>R2L>R2L

5.3 다른 방법의 비교 결과

RBM 사용시 정확도 0.94%

Adaboost, Auto-e ncoder Network, Bayesian Network, Flexible NeuralTree, Radial SVM은 실험 결과

LSSVM만큼 정확도가 높지 않음

1. 결론

실험 결과 NDNN 기반 IDS의 기능과 성능이 기존 기계 학습 방법에 기반한 방법보다 우수함을 보여줍니다.

미해결 문제 :

1. 노드 및 계층 수와 같이 매개변수가 너무 많다.
2. IDS는 지역 네트워크 환경에서 테스트 되어야 한다.

(데이터셋에 대한 높은 탐지율이 실제 탐지에서 유사한 성능을 의미하는 것이 아님)