
저자 (Authors)	손인수, 이예훈
출처 (Source)	한국통신학회 학술대회논문집 , 2020.2, 657-657(1 pages) Proceedings of Symposium of the Korean Institute of communications and Information Sciences , 2020.2, 657-657(1 pages)
발행처 (Publisher)	한국통신학회 Korea Institute Of Communication Sciences
URL	http://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE09346479
APA Style	손인수, 이예훈 (2020). 딥러닝 기법 기반 침입탐지 기술 연구. 한국통신학회 학술대회논문집, 657-657
이용정보 (Accessed)	송실대학교 59.6.214.*** 2021/04/30 09:15 (KST)

저작권 안내

DBpia에서 제공되는 모든 저작물의 저작권은 원저작자에게 있으며, 누리미디어는 각 저작물의 내용을 보증하거나 책임을 지지 않습니다. 그리고 DBpia에서 제공되는 저작물은 DBpia와 구독계약을 체결한 기관소속 이용자 혹은 해당 저작물의 개별 구매자가 비영리적으로만 이용할 수 있습니다. 그러므로 이에 위반하여 DBpia에서 제공되는 저작물을 복제, 전송 등의 방법으로 무단 이용하는 경우 관련 법령에 따라 민, 형사상의 책임을 질 수 있습니다.

Copyright Information

Copyright of all literary works provided by DBpia belongs to the copyright holder(s) and Nurimedia does not guarantee contents of the literary work or assume responsibility for the same. In addition, the literary works provided by DBpia may only be used by the users affiliated to the institutions which executed a subscription agreement with DBpia or the individual purchasers of the literary work(s) for non-commercial purposes. Therefore, any person who illegally uses the literary works provided by DBpia by means of reproduction or transmission shall assume civil and criminal responsibility according to applicable laws and regulations.

딥러닝 기법 기반 침입탐지 기술 연구

손인수, 이예훈*

동국대학교 전자전기공학부, *서울과학기술대 전자 IT 미디어공학과
isohn@dongguk.edu, * y.lee@snut.ac.kr

1. 서론

IoT 네트워크를 통해 흐르는 대량의 데이터에는 개인 정보, 보안 정보 및 중요한 정보를 포함하고 있으며 악의적인 외부 공격으로부터 컴퓨팅 장치, 네트워크, 소프트웨어 및 데이터를 보호하기 위한 사이버 보안 기술 중 침입탐지 기술은 중요한 부분이다 [1, 2]. 최근에 다양한 분야에서 각광 받고 있는 딥러닝 기술이 침입탐지 시스템에서도 적용되고 있으며 본 논문에서는 딥러닝 기반의 최신 침입탐지 기술 동향 파악을 목표로 한다.

2. 본론

2.1 DBN(Deep Belief Network) 기술

DBN [3]은 다수의 RBM(Restricted Boltzmann Machine)과 BPNN(Backpropagation Neural Network)으로 구성되어 있는 심층신경망이다. DBN 구조는 낮은 수준의 레벨에서 높은 수준의 레벨로 연결되는 다수의 RBM 을 포함하는 RBM 스택 층을 가지며 RBM 의 구조는 그림 1 에서 보여주고 있다. 타 심층신경망과 마찬가지로 DBN 의 핵심 아이디어는 비지도 학습 기법으로 피드 포워드 신경망 (FFNN) 을 초기화 한 다음 레이블이 지정된 데이터를 사용하여 지도학습 기법을 이용하여 FFNN 을 미세 조정한다. RBM 의 비지도 학습 기반의 사전 훈련이 완료되면 최상위 RBM 가중치값이 FFNN 의 초기 가중치 값으로 사용된다.

2.2 초기 DBN 기반 침입탐지 기술

Fiore et al. [4] 은 침입탐지 시스템(IDS: Intrusion Detection System)에 DBN 을 적용한 최초의 DBN 기반 IDS 모델을 제시하였다. 제안된 IDS 는 DRBM 으로 구성되며 레이블이 있는 데이터를 통한 지도 학습 기법을 이용하였다. DRBM 기반 IDS 학습 및 시험 과정에는 두 개의 데이터 세트가 사용되었다. 첫 번째 데이터 세트는 일반 워크 스테이션에서 생성된 트래픽 데이터와 Bot 에 감염된 다른 데이터 세트에서 생성되었다. 두 번째 데이터 세트는 KDD Cup 99 이며 일반 클래스의 데이터 그룹에 포함된 데이터를 추출하였다. 성능실험은 데이터 세트 두 개를 모두 사용하여 수행되었으며 성능 결과 정확도는 첫 번째 데이터 케이스는 0.94 이었으며 두 번째 데이터 케이스는 0.84 였다. 본 연구는 사용된 모델의 정확한 구조 및 파라미터 설명이 미흡한 점이 있으나 DBN 을 이용한 첫 모델이라는 점에서 의미가 있다고 할 수 있다.

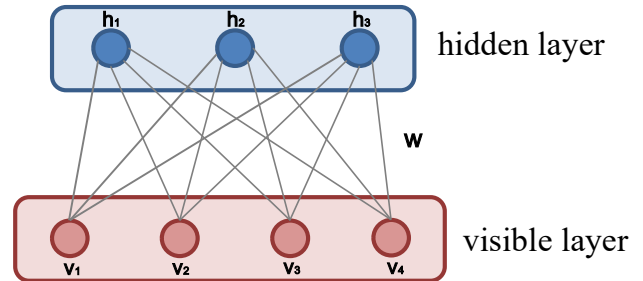


그림 1. RBM 모델

2.3 최신 DBN 기반 기술 동향

Fiore et al. [4] 의 제안된 DBN 기반 IDS 시스템 이후 많은 DBN 기반 기술이 제안되었으며 대부분의 시스템은 1. Training Data Processor 2. DBN Classifier 3. DBN Optimizer 4. Fine-tuning Algorithm 으로 구성되어 있다. 또한 제안된 모델의 대부분은 DBN 에서 3 개의 히든 레이어를 사용하고 역전파 알고리즘을 적용하여 학습된 FFNN 을 미세 조정한다. 최신 연구의 핵심은 DBN 구조의 최적화 연구이며 이를 위해 유전자 알고리즘 및 파티클 스왐 최적화 알고리즘이 적용되었다. 저자는 게임 이론 및 복잡도 네트워크 이론과 같은 강력한 최적화 방법을 기반으로 더욱 발전된 구조 최적화 연구가 필요하다고 생각한다.

ACKNOWLEDGMENT

본 논문은 2018 년도 교육부의 재원으로 한국연구재단(2018R1D1A1B07041981)의 지원을 받아 수행된 기초연구사업입니다.

참고 문헌

- [1] 김동훈, 손인수, “네트워크 침입탐지 기술 연구 동향”, 전자공학회논문지, 제 56 권 제 8 호 (2019 년 8 월) 페이지 3 - 12
- [2] 김동훈, 김정재, 손인수, “KDDCUP99 를 이용한 기계 학습 기반 네트워크 침입 탐지 기법 연구,” 2019 년도 한국통신학회 동계종합학술발표회, 2019 년 1 월.
- [3] G. E. Hinton, S. Osindero, and Y-W. The, “A fast learning algorithm for deep belief nets,” Neural Computation, 18, 1527-1554.
- [4] U. Fiore, F. Palmieri, A. Castiglione and A. De Santis, “Network anomaly detection with the restricted Boltzmann machine,” Neurocomputing, 122, 13-23.