개미 군집 알고리즘과 인공 신경망을 이용한 미지 공격의 탐지 기법*

김 경 민 †, 김 광 조 ‡

카이스트 전산학부

A Scheme on Detecting Unknown-attacks using Ant Clustering Algorithm and Artificial Neural Network

Kyung-min Kim †, Kwangjo Kim ‡

School of Computing, KAIST

요 약

네트워크 형태의 다양화와 인터넷의 발달으로 기존에 알려진 공격 외에 새로운 형태의 알려지지 않은 미지의 공격이 지속적으로 출현하고 있다. 이에 미지의 공격을 탐지하는 것은 침입탐지시스템의 필수적인 기능이다. 또한 어떤 트래픽에 대해 공격 여부를 표기하는 것은 시스템 관리자가 직접 판단하여 표기하기 때문에 비용 면이나 정확도 면에서 단점이 존재한다. 이에 본 논문에서는 생체 모방 알고리즘(Bio-inspired Algorithm)의 예시인 개미 군집 알고리즘(ACA, Ant Clustering Algorithm)과 인공 신경망(ANN, Artificial Neural Network)를 조합하여 공격 여부가 표기되지 않은 Dataset 상에서 비지도 학습을 이용해 미지의 공격을 탐지하는 기법을 제시한다.

Keywords: IDS, Unsupervised Learning, Unknown Attack, ACA, Ant Clustering, ANN, Artificial Neural Network

I. 서 론

침입 탐지 시스템(IDS, Intrusion Detection System)은 네트워크에서 사용자의 비정상적이거나 악의적인 행위를 탐지하는 시스템이다. 탐지 방식은 크게 흔적 기반 탐지(Signature-based Detection) 방식과 비정상 행위 기반 (Anomaly-based Detection) 방식으로 나뉜다. 흔적 기반 탐지 방식은 알려진 공격에 대해서만 탐지가 가능한 반면 비정상 행위 기반 탐지 방식은 알려진 공격과 미지의 공격 모두를 탐지할 가능성이 있다.

한편 기존 알려진 공격 외에 새로운 형태의 공격이 지속적으로 출현하고 있다. 이에 알려진 공격 탐지 능력과 함께 미지의 공격을 탐지하는 능력이 침입 탐지 시스템의 필수적인 기능이다. 그리고 이러한 공격들에 대한 공격 여부를 표기하는 것은 시스템 관리자가 직접 해줘야하기에 현실적으로 모든 공격에 대한 표기가 되어 있는 데이터를 구하기는 힘들다.

본 논문에서는 개미 군집 알고리즘(ACA, Ant Clustering Algorithm)과 인공 신경망(ANN, Artificial Neural Network)을 조합하여 공격 여부가 표기되지 않은 Dataset에서 비지도 학습을 이용해 미지의 공격을 탐지하는 기법을 제시한다.

* 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 정보통신·방송 연구개발사업의 일환으로 수행하였음. [1391104001, 생체모방 알고리즘(Bio-inspired Algorithm)을 활용한 통신기술 연구]

* This research was supported by the KUSTAR-KAIST Institute, under the R&D program supervised by the Korea Advanced Institute of Science and Technology (KAIST), South Korea.

† saza12345@kaist.ac.kr

‡ kkj@kaist.ac.kr

II. 배경지식

2.1 미지 공격의 탐지

알려진 공격의 특정한 흔적을 이용해 공격을 탐지하는 흔적 기반 탐지 방식은 흔적을 모르는 미지의 공격에 대해서는 탐지할 수 없다. 이에 비해 정상 행위의 프로필을 벗어나는 비정상 행위를 탐지하는 비정상 행위 기반 탐지 방식은 그 방식의 특성상 미지의 공격을 탐지할 수 있다. 그렇기 때문에 미지의 공격 탐지에는 비정상 행위 기반 탐지 방식이 이용되고 있다.

비정상 행위 기반 탐지 방식에서 좋은 성능을 나타내기 위해서는 적절한 정상 행위의 프로필을 설정하는 것이 중요하다. 이를 더 견고하고 정확하게 설정하기 위해 기계학습 및 데이터마이닝의 기법들이 주로 이용되고 있다.

2.2 개미 군집 알고리즘

개미 군집 알고리즘은 생체 모방 알고리즘(Bio-inspired Algorithm)의 군집 지능(Swarm Intelligence) 관련 알고리즘 중 하나로, 개미들이 시체들을 묘지의 형태로 군집화하는 현상과 그들의 유충을 적절히 분류하여 정렬하는 현상에 영감을 받아 제안된 알고리즘이다[1]. 이 알고리즘을 활용하여 데이터를 군집화할 수 있다.

2.3 인공 신경망

인공 신경망은 생물의 신경망에서 영감을 얻은 통계학적 학습 알고리즘이다. 인공 신경망은 뇌를 구성하는 뉴런들과 그 사이의 시냅스 연결을 통한 상호작용을 본 딴 구조로, 인공 뉴런과 그 사이의 연결 강도를 변화시켜 문제 해결 능력을 가지게 하는 모델 전반을 일컫는다. 인공 뉴런 사이의 가중치를 조절하며 학습하기 때문에 입력에 따른 비선형적인 함수 형태로도 학습을 할 수 있어 복잡한 구조를 가지는 데이터에도 활용이 가능하다.

III. 선행연구

Ramos 등[2]은 인공 개미 알고리즘을 이용한 군집화 결과를 이용하는 침입탐지 기법을 제안하였다. 그리고 Poojitha 등(3)은 인공 신경망을 이용한 침입탐지 기법을 제안하였다. 이를 통해 각각의 알고리즘은 침입탐지 기법으로 제안이 되었지만, 두 가지 모두 알려진 공격에 대한 탐지에 국한되어 있어 미지의 공격에 대한 연구 결과는 없다. 한편 Hosseinpour 등[4]은 군집 알고리즘인 DBSCAN과 인공 면역 체계(Artificial Immune System)를 조합하여 침입탐지시스템에서 미지의 공격을 탐지하고자 하였다. 이런 면에서 현재까지 개미 군집 알고리즘과 인공 신경망을 조합하여 미지의 공격을 탐지하는 시도는 없었다.

IV. 탐지기법 제안

본 논문에서는 개미 군집화 알고리즘과 인공 신경망을 조합하여 미지의 공격을 탐지하는 기법을 제안한다. 제안하는 탐지 기법은 비지도 학습을 통해 Dataset을 군집화하고, 그 결과에 따라 공격 여부를 표기하는 ACA Engine, ACA Engine으로부터 공격 여부가 표기된 Dataset을 받아 지도 학습을 통해 침입 탐지기를 훈련하는 ANN Engine으로 나뉜다. 제안하는 기법은 Fig. 1과 같다.

3.1 ACA Engine

ACA Engine에서는 공격 여부가 표기되어 있지 않은 Dataset 상에서 개미 군집화 알고리즘을 이용해 비지도 학습을 하여 Dataset을 군집화한다. 그 후에 군집화된 결과를 바탕으로 많은 수의 데이터가 속한 군집들을 정상 행위의 프로필로 인식하여 정상으로, 나머지 Outlier 혹은 적은 수의 데이터가 속한 군집들을 비정상으로 공격 여부를 표기하여 그 결과를 ANN Engine으로 전달해준다.

3.2 ANN Engine

ANN Engine에서는 ACA Engine으로부터 전달받은 공격 여부가 표기된 Dataset을 이용해 지도 학습 방식으로 탐지기를 학습하여 침입탐지를 수행한다. 인공 신경망은 입력층(Input Layer), 은닉층(Hidden Layer), 출력층(Output Layer)로 이루어지고 역전파(Back Propagation) 방식으로 학습한다.

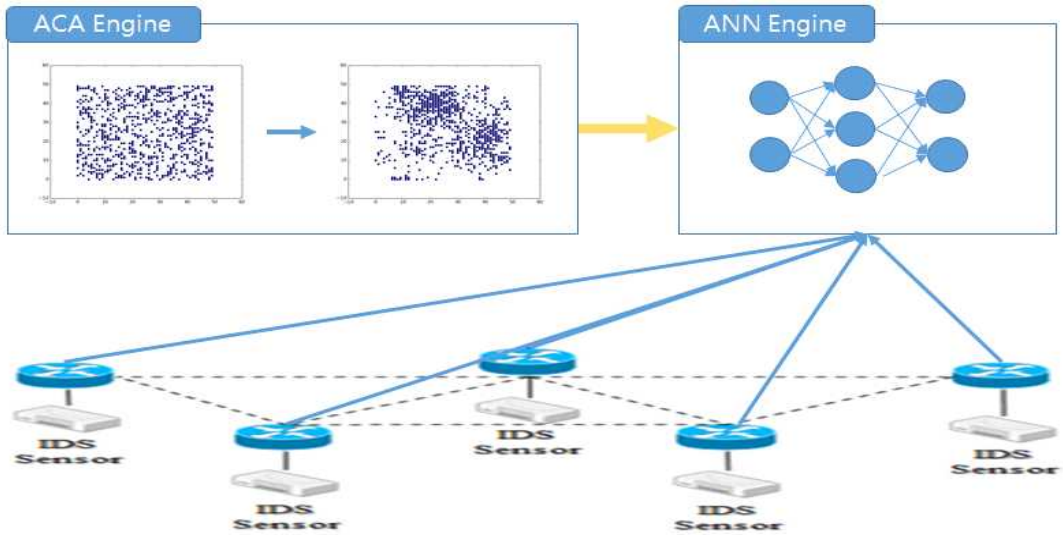

Fig. 1. Architecture of Proposed IDS

3.3 분석

제안하는 기법은 개미 군집화 알고리즘을 사용하기 때문에 공격 여부가 표기되어 있지 않은 데이터를 대상으로 학습을 할 수 있는 장점이 있다. 또한 인공신경망 알고리즘도 사용하고 있기 때문에 비선형 구조를 학습할 수 있다. 이러한 장점으로 인해 기존에 제안된 타 기법들에 비해 복잡한 관계와 구조를 가지는 미지의 공격 등도 효율적으로 탐지할 수 있다.

V. 결 론

본 논문에서는 침입 탐지 시스템에서의 미지의 공격 탐지를 위한 새로운 탐지 기법을 제시하였다. 제안하는 기법을 통해 복잡한 관계와 구조를 가지는 미지의 공격을 효율적으로 탐지할 수 있을 것이다. 향후 연구로 제안된 아이디어의 실제 구현과 실험을 통한 실증적인 성능 검증이 있을 것이다.

References

[1] C. Elkan, "Results of the KDD'99 classifier learning", ACM SIGKDD Explorations Newsletter 1.2, 2000, 63-64.

[2] V. Ramos and A. Abraham, "ANTIDS: Self Organized Ant-Based Clustering Model for Intrusion Detection System", Proceedings of the Fourth IEEE International Workshop, WSTST'05, Muroran, Japan, 2005, 977-986.

[3] G. Poojitha, K. Nandha Kumar, and P. Jayarami Reddy, "Intrusion Detection using Artificial Neural Network", Computing Communication and Networking Technologies (ICCCNT), 2010 International Conference on IEEE, 2010.

[4] F. Hosseinpour, P. Vahdani Amoli, F. Farahnakian, J. Plosila, and T. Hämäläinen, "Artificial Immune System Based Intrusion Detection: Innate Immunity using an Unsupervised Learning Approach", International Journal of Digital Content Technology & its Applications 8.5, 2014.

[5] U. Boryczka, "Ant clustering algorithm", Intelligent Information Systems, 2008, 377-386.