개미군집 알고리즘과 의사결정트리를 활용한 알려지지 않은 공격 탐지 시스템[1)]

김경민*, 홍진아**, 김광조*,**

*카이스트 전산학부/ **정보보호대학원

Intrusion Detection System for Unknown-attack Detection using Ant Clustering Algorithm and Decision Tree

Kyung-min Kim*, Jina Hong**, Kwangjo Kim*,**

*School of Computing/ **Graduate School of Information Security, KAIST

요 약

다양한 네트워크 환경과 인터넷의 발달로 인해 알려지지 않은 새로운 공격이 끊임없이 출현하고 있다. 이에 따라 침입탐지시스템에 알려지지 않은 공격을 탐지하는 것이 요구되고 있다. 한편, 사람이 직접 어떤 트래픽의 공격 여부를 판단하여 라벨을 생성하는 방식은 실수의 가능성이 존재하고 상당한 비용이 든다. 이에 본 논문에서는 개미군집 알고리즘과 의사결정트리를 조합하여 라벨이 없는 데이터를 바탕으로 스스로 학습하여 알려지지 않은 공격을 탐지하는 새로운 침입탐지시스템을 제안한다. 제안하는 시스템은 알려지지 않은 공격 탐지에 있어 이미 제안된 Hosseinpour 등[1]의 방식보다 더 높은 탐지율을 나타낸다.

I. 서론

침입탐지시스템(IDS, Intrusion Detection System)은 네트워크를 감시하며 사용자의 악의적인 행동을 탐지하는 시스템이다. 침입을 탐지하는 방식은 크게 흔적 기반 탐지(Signature-based Detection)와 비정상 행위 기반 탐지(Anomaly-based Detection)로 나뉜다.

다양한 네트워크 구조와 새로운 형태의 네트워크 출현 등으로 인해 기존에 알려진 공격 외에 알려지지 않은 새로운 공격이 끊임없이 출현하고 있다. Stuxnet과 같은 0-데이 공격(Zero-day Attack) 등 알려지지 않은 공격은 국가와 사회에 막대한 피해를 야기할 수 있다. 이에 알려진 공격 탐지뿐만 아니라 알려지지 않은 공격을 탐지하는 것이 침입탐지시스템의 필수적인 기능이 되었다. 또한 새로운 공격이 출현할 때마다 사람이 직접 공격에 대한 라벨을 만드는 작업은 실수의 가능성이 존재하고 상당한 비용이 드는 작업이다. 이에 끊임없이 출현하는 알려지지 않은 공격을 탐지하기 위해서는 라벨이 없는 데이터에서 스스로 공격 여부를 학습할 수 있어야한다.

본 논문에서는 알려지지 않은 공격 탐지를 위해 생체모방 알고리즘(Bio-inspired Algorithm)인 개미군집 알고리즘(ACA, Ant Clustering Algorithm)과 기계학습의 알고리즘 중 하나인 의사결정트리(DT, Decision Tree)를 조합한 새로운 침입탐지시스템을 제안한다. 새롭게 제안하는 시스템은 개미군집 알고리즘과

*,** (saza12345, jina3453, kkj)@kaist.ac.kr

1) This work was partly supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIP) (B0101-15-1270, Research on Communication Technology using Bio-Inspired Algorithm) and the KUSTAR-KAIST institute, KAIST, Korea.

의사결정트리를 조합하여 라벨이 없는 데이터에서 스스로 학습하여 공격에 대한 사전지식이 없는 알려지지 않은 공격을 탐지할 수 있다.

본 논문의 2장에서는 배경지식에 대해 살펴보고, 3장에서는 관련 연구를 알아본다. 4장에서는 제안하는 시스템의 구조에 대해 설명한 후 5장에서 제안하는 시스템의 실험 및 성능 평가를 하고, 마지막 6장에서 결론을 맺는다.

II. 배경지식

2.1 알려지지 않은 공격 탐지

알려지지 않은 공격이란 침입탐지시스템이 사전지식을 가지고 있지 않은 공격을 지칭한다. 흔적 기반 탐지 방식은 알려진 공격의 특징, 즉 흔적을 저장한 후 입력 트래픽과 저장된 흔적들을 비교하여 공격 여부를 판단하기 때문에 그 탐지 방식의 한계로 알려지지 않은 공격은 탐지하지 못한다. 이에 비해 비정상 행위 기반 탐지 방식은 정상적인 행위에 대한 프로필을 구성하고 그를 벗어나는 비정상 행위를 탐지해 공격으로 판단한다. 이러한 탐지 방식으로 인해 비정상 행위 기반 탐지는 알려지지 않은 공격을 탐지할 수 있다. 이 때문에 알려지지 않은 공격 탐지에는 비정상 행위 기반 탐지 방식이 연구되고 있다.

비정상 행위 기반 탐지 방식은 그 방식의 특성상 정상 행위에 대한 프로필을 견고하고 정확하게 구성하는 것이 중요하다. 견고하고 정확한 모델링을 위해 k-평균 클러스터링(k-Means Clustering), SVM(Support Vector Machine) 등과 같은 기계학습 관련 알고리즘이 이용되고 있다[2].

2.2 KDD Cup 1999 Dataset

KDD Cup 1999 Dataset은 MIT Lincoln Labs에서 수행된 1998 DARPA Intrusion Detection Evaluation Program의 결과를 바탕으로 구성된 침입탐지시스템의 성능 평가를 위한 Dataset으로, 네트워크상에서 정상적인 연결과 비정상적인 연결을 가지고 있는 트래픽을 포함한다[3]. 이 Dataset은 크게 Probe, DoS, U2R, R2L의 4가지 공격 타입과 정상 트래픽인 Normal로 구성되어 있다.

2.3 개미군집 알고리즘

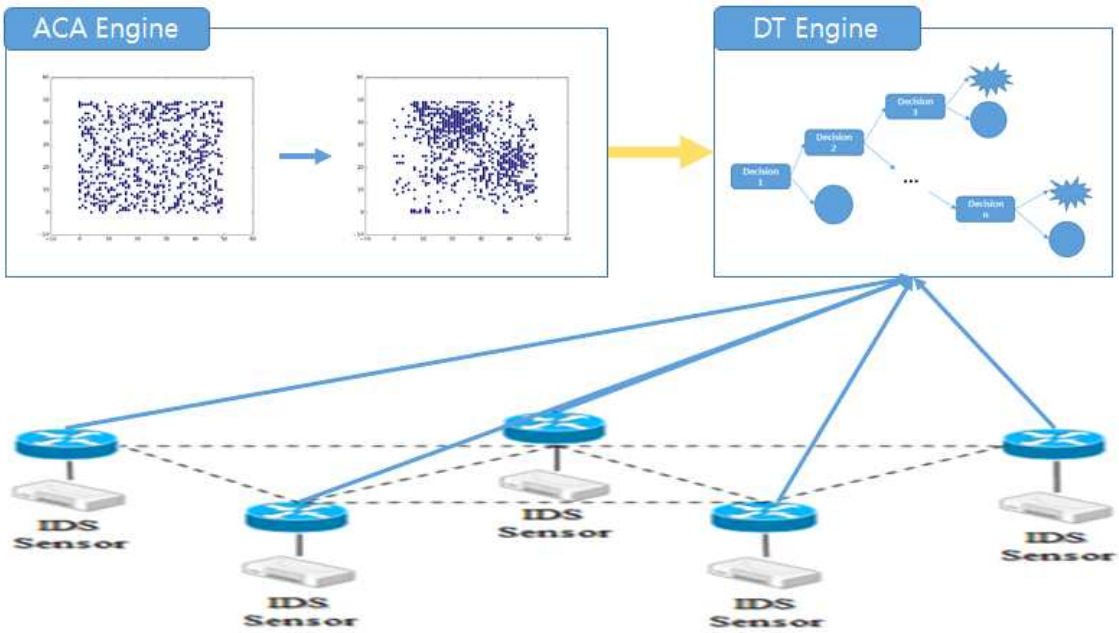
개미군집 알고리즘은 생체모방 알고리즘의 군집 지능(Swarm Intelligence) 관련 알고리즘 중 하나로, 개미들이 시체를 군집화(Clustering)하고 유충을 적절히 분류하여 정렬하는 현상에 영감을 받은 알고리즘이다[3]. 개미군집 알고리즘은 자기조직화(Self-organizing) 특성을 가지고 있어 무질서한 데이터에서 스스로 군집을 형성할 수 있다. 이 알고리즘을 활용해 데이터를 군집화 할 수 있다.

2.4 의사결정트리

의사결정트리는 기계학습 알고리즘 중 하나로, 많은 수의 입력과 그에 대한 출력 혹은 라벨을 바탕으로 결정 규칙(Decision Rule)을 추론하여 자료를 분류(Classification)하는 알고리즘이다. 학습의 결과를 트리 구조로 나타낼 수 있고, 각 결정 규칙에서의 분기에 따라 최종 출력이 결정된다. 결정 트리의 학습은 학습에 사용되는 집합을 적절한 결정 규칙에 따라 부분 집합들로 나누는 과정이다. 이 학습 과정은 학습 대상인 Dataset에서 모든 데이터가 결정 규칙에 의해 알맞은 출력으로 할당될 때까지 반복된다. 의사결정트리는 훈련 대상인 Dataset의 라벨이 다소 틀리게 표기되어 있다고 해도 안정적으로 잘 동작하는 장점이 있다.

III. 관련 연구

Ramos 등[4]은 개미군집 알고리즘의 자기조직화 특성을 이용해 군집화한 결과를 이용하는 침입탐지시스템을 제안하였다. 하지만 알려진 공격을 탐지하는 것에 대한 실험만 하여 알려지지 않은 공격에 대한 실험과 검증은 없다. 한편 Hosseinpour 등[1]은 개미군집 알고리즘과 다른 군집화 알고리즘 중 k-평균 클러스터링, DBSCAN과 인공 면역 체계(AIS, Artificial Immune System)를 조합한 침입탐지시스템을 제안하고 라벨이 없는 Dataset에서 알려지지 않



[그림 1] 제안하는 침입탐지시스템 구조

은 공격을 탐지하였다. 현재까지 개미군집 알고리즘과 의사결정트리를 조합하여 알려지지 않은 공격을 탐지하고자 하는 연구는 수행되지 않고 있다.

IV. 침입탐지시스템 제안

본 논문에서는 개미군집 알고리즘과 의사결정트리를 조합하는 새로운 기법의 침입탐지시스템을 제안한다. 제안하는 시스템은 개미군집 알고리즘을 이용해 Dataset을 군집화하고 그 결과에 따라 공격 여부에 관한 라벨을 생성하는 ACA Engine과 ACA Engine으로부터 결과를 받아 침입 탐지기를 훈련하는 DT Engine으로 이루어져 있다. 제안하는 시스템의 구조는 [그림 1]과 같다. 이러한 구조를 가짐으로써 제안하는 시스템은 공격 여부 라벨이 없는 Dataset에서도 학습이 가능하다.

4.1 ACA Engine

ACA Engine은 개미군집 알고리즘을 이용하여 Dataset을 군집화하고 결과를 바탕으로 자체적으로 공격 여부의 라벨을 생성한다. 라벨을 필요로 하지 않은 비지도 학습(Unsupervised Learning) 방식의 군집화를 수행하기 때문에 사전지식이 없는 알려지지 않은 공격 탐지에 적합하다. 군집화 결과로 생성한 라벨과 Dataset을 ANN Engine으로 전달한다.

4.2 DT Engine

DT Engine은 ACA Engine으로부터 라벨과 함께 Dataset을 받아 지도 학습(Supervised Learning) 방식으로 의사결정트리를 훈련한다. 훈련된 의사결정트리를 이용해 대상 네트워크에서 알려지지 않은 공격을 탐지하게 된다.

V. 실험 및 평가

실험은 KDD Cup 1999 Dataset을 바탕으로 수행되었다. KDD Cup 1999 Dataset에서 라벨을 제외한 상태로 실험을 하였다. Dataset은 Training set과 Testing set으로 나뉘었는데, KDD Cup 1999 Dataset은 정상 트래픽의 수에 비해 공격 트래픽의 수가 비정상적으로 높아 보통의 네트워크 환경을 나타내지 못한다[5]. 따라서 본 논문에서는 보통의 네트워크 환경을 가정하여, 90%의 정상 트래픽과 10%의 공격 트래픽으로 조정하여 실험과 검증을 수행하였다. 두 개의 Dataset의 구성은 [표 2], [표 3]과 같다.

[표 2] Training set의 구성

유형	트래픽의 수
Normal	78,010
DoS	3,712
U2R	35
R2L	1,125
Probe	3,796
합	86,678

[표 3] Testing set의 구성

유형	트래픽의 수
Normal	19,268
DoS	1,812
U2R	17
R2L	1
Probe	311
합	21,409

침입탐지시스템을 훈련하여 성능을 검증하는 데에는 탐지율(DR, Detection Rate), 오탐율(FPR, False Positive Rate), 정확도(ACC, Accuracy) 등이 쓰인다. 탐지율은 침입탐지시스템이 공격이라고 판단한 트래픽들 중 실제 공격인 트래픽의 비율이다. 오탐율은 실제 정상 트래픽 중 침입탐지시스템이 공격이라고 판단한 트래픽의 비율이다. 정확도는 전체 트래픽 중 침입탐지시스템이 정상 혹은 공격을 제대로 판단한 트래픽의 비율이다. 본 논문에서는 탐지율, 오탐율, 정확도를 모두 계산하여 침입탐지시스템의 성능을 검증한다. 실험을 통한 성능은 [표 4]와 같다. [표 4]에서는 본 논문과 유사한 접근방식을 통해 알려지지 않은 공격 탐지 성능을 검증한 Hosseinpour 등[1]의 침입탐지시스템의 성능을 함께 비교한다.

[표 4] 제안하는 IDS의 성능 비교표 (단위 : %)

IDS / 척도	[1] k-평균	[1] DBSCAN	제안하는 IDS
탐지율	43.1	58.9	78.09
오탐율	15.6	0.8	15.74
정확도	60.7	77.1	83.64

Hosseinpour 등[1]의 결과와 비교해서 제안하는 침입탐지시스템은 k-평균 군집화 알고리즘과 비슷한 오탐율을 가지면서 동시에 월등히 높은 탐지율과 정확도를 나타낸다.

VI. 결론

본 논문에서는 알려지지 않은 공격 탐지를 위해 생체모방 알고리즘 중 하나인 개미군집 알고리즘과 의사결정트리를 조합한 새로운 침입탐지시스템을 제안하고, 성능을 검증하였다. 제안하는 침입탐지시스템은 자기조직화 특성을 통해 데이터를 스스로 군집화할 수 있어 라벨이 없는 Dataset에서도 학습이 가능하다. 또한 Hosseinpour 등[1]의 방식과 비교해 월등히 높은 탐지율을 나타낸다. 향후 연구 방향으로 오탐율을 낮출 수 있는 방안을 연구하여 적용하는 것이 예정되어 있다.

[참고문헌]

[1] Farhoud Hosseinpour, Payam Vahdani Amoli, Fahimeh Farahnakian, Juha Plosila and Timo Hamalainen, “Artificial Immune System Based Intrusion Detection: Innate Immunity using an Unsupervised Learning Approach”, International Journal of Digital Content Technology & its Applications 8.5, 2014.

[2] 김경민, 김광조, “개미 군집 알고리즘과 인공 신경망을 이용한 미지 공격의 탐지 기법”, 2015 정보보호학술발표회논문집 충청지부, 2015, 63-65.

[3] Charles Elkan, “Results of the KDD’99 classifier learning”, ACM SIGKDD Explorations Newsletter 1.2 , 2000, 63-64.

[4] Vitorino Ramos and Ajith Abraham, “ANTIDS: Self Organized Ant-Based Clustering Model for Intrusion Detection System”, Proceedings of the Fourth IEEE International Workshop, 2005, 977-986.

[5] Leonid Portnoy, Eleazar Eskin, and Sal Stolfo, “Intrusion Detection with Unlabeled Data Using Clustering”, Proceedings of ACM CCS Workshop on Data Mining Applied to Security, 2001