김일성종합대학학보
정보과학
주체110(2021)년
제67권 제3호

중첩신경망을 리용한 망악성통화검출방법

박성호, 한송윤

망통화에 대한 분류문제, 망악성통화검출문제는 망침입검출 특히 미지의 공격을 검출하기 위한 이상검출의 첫 단계로 되며 망보안 및 망관리분야에서 중요한 의의를 가진다.

망통화분류방법에는 크게 규칙에 기초한 방법과 기계학습에 기초한 방법이 있는데 최근에 기계학습에 기초한 망공격 특히 새로운 공격을 검출하기 위한 많은 연구들에 의하여 망통화분류를 통한 망침입검출에서 큰 전진이 이룩되였다.[1] 그러나 전통적인 기계학습방법들은 특징공학에 기초하고있는데 특징설계과정이 매우 복잡하고 많은 시간을 소비한다는 약점을 가지고있다.

론문에서는 최근에 화상분류와 자연언어처리를 비롯한 여러 분야에서 좋은 성능을 보여주고있는 심층학습방법을 망통화분류에 적용하여 생통화자료로부터 특징을 자동추출하며 그것에 의하여 높은 정확도로 망통화를 분류하기 위한 악성통화검출방법을 제안하였다.

1. 중첩신경망을 리용한 망통화분류의 원리

망통화를 분류하는 방법에는 우선 규칙에 기초한 방법으로서 포구에 기초한 방법과 심층파케트검사(DPI)에 기초한 방법 등이 있는데 여기서는 미리 정의된 규칙들과 정합하는 방법으로 통화분류를 진행한다.

다음으로 기계학습에 기초한 방법들로서 인공신경망이나 지지벡토르기계(SVM), 베이즈분류 등을 리용하는 방법이 있는데 이러한 전통적인 기계학습방법들에서는 분류에 적당한 특징들을 설계, 추출, 선택하여야 하는 복잡한 문제들이 제기되고있으며 이에 대한 연구가 많이 진행되고있다.

인공지능분야에서 최근에 빨리 발전하는 기계학습방법인 표현학습(representation learning)은 원시자료로부터 자동적으로 특징들을 학습하는 방법으로서 수동적인 특징설계문제를 일정한 정도에서 해결하였다. 그리고 표현학습의 전형적인 수법인 심층학습방법 특히 중첩신경망(CNN : Convolutional Neural Network)은 콤퓨터시각과 자연언어처리를 비롯한 인공지능의 여러 령역들에서 높은 성능을 보여주었다.[2, 3]

중첩신경망은 화상분류에서 직접 생화상들을 입력으로 하여 중첩연산을 통하여 특징들을 자동추출한다. 중첩신경망이 높은 성능을 달성할수 있는 리유의 하나는 그것이 국부적인 령역특징들을 추출할수 있다는것이다.

마찬가지로 망자료흐름에서 파케트의 머리부부분은 상대적으로 독립적인 마당들로 이루어져있으나 유효자료부분은 서로 련관되는 특정의 결합패턴들을 포함하고있으며 이러한 결합패턴들은 정상 또는 비정상의 망통화와 관련되여있다.

중첩신경망은 중첩연산에 의하여 유효자료부분의 특징들을 추출한다. 훈련단계에서 특정의 패턴들이 발견되고 학습되며 정상 또는 이상의 통화를 구분할수 있는 고준위의 의미론적특징들을 추출할수 있다.

그러므로 중첩신경망에 의하여 령역특징들이 추출되고 학습에 의하여 정상 또는 이상통화를 구분할수 있는 능력을 가지게 된다.

이로부터 생파케트흐름을 입력으로 하는 중첩신경망에 의하여 통화분류의 목적을 달성할수 있으며 망침입검출의 성능을 크게 개선할수 있다는것을 예측할수 있다.

2. 망통화분류를 위한 중첩신경망의 구성

1) 자료전처리

자료전처리는 생파케트흐름자료를 중첩신경망의 입력자료로 변환하는 과정이다. 생파케트자료를 바이트흐름으로 간주하고 매 바이트가 0～255범위의 수값으로 표현되는 특징벡토르로 변환한다. 다음에 이 자료를 척도변환을 하여 [0, 1]값범위에 놓이도록 정규화한다. 학습이나 검사에 리용되는 파케트들을 표현하는 특징벡토르들은 고정된 길이인 중첩신경망의 입력크기 N차원벡토르로 정리된다.

2) 망구조

중첩신경망은 여러개의 중첩층과 공유층, 전결합층, 분류층으로 구성된다.

입력층은 $N=784$차원의 벡토르를 입력하며 3개의 중첩층+공유층구조와 하나의 전결합층, 마지막분류층으로 구성된다.

사용된 중첩신경망의 구조는 그림과 같다.

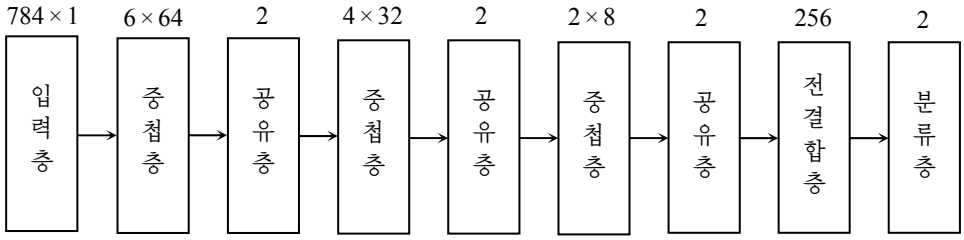

그림. 사용된 중첩신경망의 구조

첫번째 중첩층에서 핵벡토르의 크기는 망파케트자료에서의 바이트들의 상관령역을 고려하며 비교평가를 위하여 $M = 6$과 $M = 12$로 정하였으며 통로수 64, 걸음크기 1을 적용하였다.

다음층들에서 핵의 크기는 적당히 감소되며 통로수는 32, 8로 정하였다. 모든 공유층들에서는 크기 2인 최대공유(max-pooling)연산을 진행하여 3개의 중첩층 + 최대공유층의 출력마디수는 각각 392, 196, 98로 된다. 전결합층은 256개의 마디로 구성되며 분류층은 2개의 마디를 가지고 softmax연산을 진행하여 정상통화와 이상통화의 분류결과를 출력한다.

중첩층들에 의하여 학습된 중간표현들은 해당한 특징지도들을 구성한다.

중첩층의 매 출력에 대하여 특징지도값들은 다음과 같이 계산된다.

$$x_j^l = f\left(\sum_{i=j}^{j+M-1} x_j^{l-1} k_{i-j}^l + b_j\right) \tag{1}$$

여기서 x_j^l은 l번째 중첩층의 출력특징지도의 j번째 값이며 k_m^l은 l번째 중첩층에서 쓰인 중첩핵벡토르의 해당한 원소값이다. 또한 b_j는 편위이고 f는 활성화함수로서 론문에서는 정규선형함수(ReLU)이다. 중첩핵벡토르와 편위는 학습단계에서 학습된다.

중첩층뒤의 공유층은 미끄럼창문방식으로 최대공유(max-pooling)연산을 진행한다. 창문의 크기는 2이며 걸음은 2로 하였다.

3) 학습

학습이 순조롭게 되도록 하기 위하여 묶음정규화(Batch Normalization)를 진행한다.

매 중첩층+공유층구조의 출력들에 대하여 다음의 변환이 적용된다.

$$\hat{x}_i = \frac{x_i - E[x_i]}{\sqrt{Var[x_i] + \varepsilon}} \tag{2}$$

여기서 $E[x_i]$와 $Var[x_i]$는 각각 평균과 분산을 표시한다.

묶음정규화에 의하여 학습이 빨리 진행되고 초기값에 크게 의존하지 않으며 과적합문제가 일정하게 해결될수 있다.

과적합문제를 피하기 위하여 또한 마지막전결합층에서 솎음(dropout)을 적용하였다.

학습률은 0.001, 학습세대수는 50으로 정하였다.

3. 실험 및 결과분석

실험에서는 망침입검출과 관련하여 많이 쓰이는 DARPA 98자료모임을 리용하였다.

DARPA 98자료모임의 파케트의 유효자료부분을 바이트렬로 보고 그것을 직접 중첩신경망의 입력으로 한다. 자료모임으로부터 20 000개의 파케트자료를 선택하되 정상자료(normal)와 공격자료(attack)를 각각 50%로 정하였다. 그리고 각각 절반씩의 자료를 학습과 검사에 리용하였다.

분류모의실험은 Matlab R2017a에서 진행하였다.

평가척도로는 우선 분류정확도를 리용하였는데 이 지표는 다음과 같다.

$$Ac = \frac{TP + TN}{TP + FP + FN + TN} \times 100 \tag{3}$$

여기서 TP와 TN은 각각 공격표본과 정상표본을 정확히 분류한 수이며 FP와 FN은 각각 공격과 정상을 부정확하게 분류한 수이다. 또한 망침입검출체계의 성능에서 중요한 오경보률을 반영하는 지표인 FN에 대하여서도 평가를 진행하였다.

비교를 위하여 같은 자료모임에 대하여 41개의 특징표현을 리용하는 BP신경망에 의한 전통적인 기계학습에 기초한 통화분류실험을 진행하였다. 또한 중첩신경망에서는 두가지의 중첩핵크기 즉 $M=6$과 $M=12$에 대한 분류성능을 비교하였다.(표)

표. 성능평가(분류정확도와 오경보률)

방법	자료	분류정확도	FN
BP망	학습자료	94.7	3.6
	검사자료	93.5	4.3
제안방법($M=6$)	학습자료	96.9	2.3
	검사자료	96.4	2.2
제안방법($M=12$)	학습자료	97.3	2.2
	검사자료	96.7	2.0

표로부터 1차원중첩신경망에 의한 망통화분류정확도가 전통적인 기계학습방법에 의한 것보다 2%이상 높다는것을 알수 있다. 이것은 생통화자료로부터의 자동특징학습이 높은

수준에서 진행되였다는것을 보여준다. 또한 중첩핵의 크기는 바이트단위의 망통화흐름에 대하여 $M=12$가 보다 적당하다는것을 보여준다. 망통화분류를 위한 중첩신경망의 중첩핵의 최량크기는 보다 더 연구되여야 한다.

맺 는 말

망침입검출의 첫 단계로서 망악성통화분류를 위한 1차원중첩신경망을 구성하고 그것에 의한 망통화분류가 전통의 기계학습방법에 의한 분류에 비하여 높은 정확도를 달성한다는것을 확증하였다.

참 고 문 헌

[1] Omar Y. Al-Jarrah et al.; Digital Communications and Networks, 4, 277, 2018.

[2] Jun Ou, Yujian Li; Neurocomputing, 11, 1, 2018.

[3] Zhiyuan Tan et al.; IEEE Transactions on Computers, 64, 9, 2519, 2015.

주체110(2021)년 5월 5일 원고접수

A Method of Network Malware Traffic Detection Using Convolutional Neural Networks

Pak Song Ho, Han Song Yun

In this paper, we propose one-dimensional convolutional neural network model for network traffic classification and show that its feature learning is better than those of the traditional machine learning methods in network traffic classification.

Keywords: network traffic classification, convolutional neural network, network security