KIPS Tr. Comp. and Comm. Sys.
Vol.6, No.3 pp.135~142 pISSN: 2287-5891

https://doi.org/10.3745/KTCCS.2017.6.3.135

CNN Based Real-Time DNS DDoS Attack Detection System

In Hyuk Seo[†] · Ki-Taek Lee[††] · Jinhyun Yu[†] · Seungjoo Kim[†††]

ABSTRACT

DDoS (Distributed Denial of Service) exhausts the target server's resources using the large number of zombie pc, As a result normal users don't access to server. DDoS Attacks steadly increase by many attacker, and almost target of the attack is critical system such as IT Service Provider, Government Agency, Financial Institution. In this paper, We will introduce the CNN (Convolutional Neural Network) of deep learning based real-time detection system for DNS amplification Attack (DNS DDoS Attack). We use the dataset which is mixed with collected data in the real environment in order to overcome existing research limits that use only the data collected in the experiment environment. Also, we build a deep learning model based on Convolutional Neural Network (CNN) that is used in pattern recognition.

Keywords : Deep Learning, DNS DDoS Attack, Real-Time Detection System, DNS Amplification Attack

CNN 기반의 실시간 DNS DDoS 공격 탐지 시스템

서 인 혁[†] · 이 기 택[††] · 유 진 현[†] · 김 승 주[†††]

요 약

DDoS (Distributed Denial of Service)는 대량의 좀비 PC를 이용하여 공격 대상 서버에 접근하여 자원을 고갈시켜 정상적인 사용자가 서버를 이용하지 못하게 하는 공격이다. DDoS 공격발생 사례가 꾸준히 증가하고 있고, 주요 공격대상은 IT 서비스, 금융권, 정부기관이기 때문에 DDoS를 탐지하는 것이 중요한 이슈로 떠오르고 있다. 본 논문에서는 DNS 서버를 이용하여 패킷을 증폭시키는 DNS DDoS 공격 즉, DNS Amplification 공격(이하 DNS 증폭 공격)을 Deep Learning (이하 딥 러닝)을 활용해 실시간으로 탐지하는 방법에 대해 소개한다. 기존 연구들의 한계점을 극복하기 위하여 실험망 환경의 데이터가 아닌 실 환경 데이터를 혼합하여 탐지 시스템을 학습하였다. 또한 이미지 인식에 주로 사용되는 Convolutional Neural Network (이하 CNN)을 이용하여 딥 러닝 모델을 구축하였다.

키워드 : 딥 러닝, DNS DDoS 공격, 실시간 탐지 시스템, DNS 증폭 공격

1. 서 론

PC와 여러 IoT 기기들은 네트워크를 통해 정보를 주고받으며 통신한다. 최근 네트워크를 사용하는 기기들이 많아지고, 통신기술이 발달하면서 네트워크상에 존재하는 위협은 지속적으로 증가하고 있다. 악의적인 공격자들은 네트워크 프로토콜, 소프트웨어 등의 취약점을 이용하여 개인정보 탈취, 제어권한 획득과 같이 서비스 사용자들에게 직접적인 피해를 입히기도 하고, 사용자가 이용하는 서비스 및 서버를 공격하여 간접적인 피해를 입히기도 한다. 서비스 및 서버를 마비시키는 공격으로 DoS (Denial of Service) 공격과 DDoS 공격이 있으며, 이러한 서비스 거부 공격도 크게 두 가지로 나뉜다. 서버에서 제공하는 프로그램이나 프로토콜의 취약점을 찾아 서비스를 마비시키거나 서버의 네트워크 및 시스템 자원을 고갈시켜 마비시키는 공격이 있다.

DDoS 공격은 추적을 방지하기 위해 공격자의 신분을 숨기고 공격 대상 서버의 시스템 및 네트워크 자원을 고갈시켜 마비시키는 것이 가장 중요하다. 그래서 공격에 사용하는 기기들의 IP를 위장하고, 공격 대상 서버를 쉽게 마비시키기 위해 증폭매체를 사용해 패킷을 증폭시키는 DNS DDoS 공격과 같은 기법이 주로 사용되고 있다[1].

Verisign의 2015년 3분기 DDoS 공격 트렌드와 관련된 보고서에 따르면, 전년 대비 DDoS 공격이 전체적으로 85% 증가했으며 DNS나 NTP 프로토콜을 이용한 UDP Flooding

※ 이 논문은 2016년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(R7117-16-0161, 자율주행 스마트자동차용 이상징후 탐지 핵심기술개발).
† 준 회 원 : 고려대학교 정보보호대학원 정보보호학과 석사과정
†† 비 회 원 : 고려대학교 정보보호대학원 정보보호학과 석·박사통합과정 수료
††† 종신회원 : 고려대학교 사이버국방학과/정보보호대학원 정교수
Manuscript Received : November 2, 2016
Accepted : November 20, 2016
* Corresponding Author : Seungjoo Kim(skim71@korea.ac.kr)

공격이 전체 DDoS 공격 중 75%를 차지하고 있다[2].

DNS DDoS를 포함한 DDoS 공격이 지속적으로 발생하고 있기 때문에, 피해가 발생하기 이전에 효과적으로 탐지하는 것이 중요하다. 본 논문에서는 딥 러닝을 활용하여 DNS DDoS 공격을 실시간으로 탐지하는 방법에 대해 연구한다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 DNS DDoS 공격과 딥 러닝, 그리고 기계 학습 기법을 포함한 DDoS 탐지 기법에 대해 설명하고, 3장에서는 DNS DDoS 공격을 실시간으로 탐지하기 위해 제안한 탐지 시스템에 대해 설명한다. 4장에서는 제안한 탐지 시스템의 구현 과정, 실험에 필요한 데이터 셋 수집 및 생성 방법에 대해 설명하고, 구현한 시스템의 탐지 결과를 도출한다. 5장에서는 결론 및 향후 연구 방향에 대해 서술한다.

2. 관련 연구

2.1 DNS DDoS 공격 및 방어

DNS DDoS 공격은 DNS 증폭 공격이라고도 하며, DNS Response 패킷의 크기가 DNS Query 패킷의 크기보다 크다는 것을 이용한 공격기법이다. DNS와 관련된 다른 공격들을 방어하기 위해 설계된 DNSSEC 때문에 DNS DDoS 공격이 더 용이해졌다. Fig. 1은 DNS DDoS 공격의 흐름을 나타낸다.

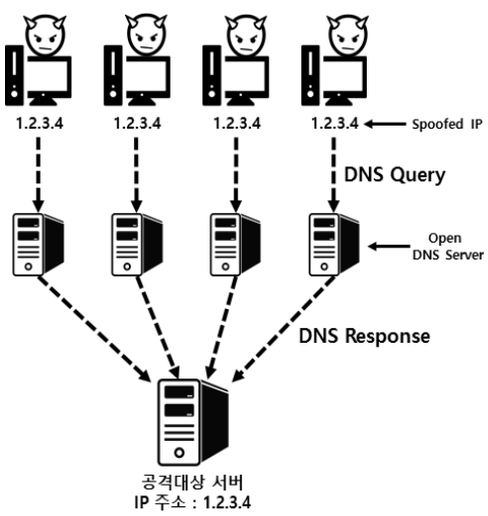


Fig. 1. DNS DDoS Attack

DNS DDoS 공격을 탐지 및 방어하기 위해 현재까지 진행된 연구는 다음과 같다. [3]은 DNS DDoS 공격에 대한 구조를 제안하고, DNS 로그를 바탕으로 Blacklist IP를 설정해 공격을 방어하는 방식으로 탐지와는 거리가 멀다. [4]는 DNS 트래픽들을 IDS로 보내 시각화하여 탐지하도록 설계하였고, 실시간 처리가 불가능하다. [5-7]은 근실시간에 공격을 탐지하는 것이 가능하지만 실험망 환경에서 테스트하여 실제 환경에서의 탐지 효율성은 보장할 수 없다.

[8]은 기존 연구들의 문제점 해결하기 위해 실험망이 아닌 실제 환경에서의 공격을 근실시간에 효율적으로 탐지하도록 설계하였다. DNS Query/Response 트래픽의 응답성공률(Success Rate)을 기반으로 DNS DDoS 공격을 탐지하는 방식이다. 60초 동안 발생한 DNS Query/Response 패킷의 SR(Sucess Rate)를 계산하여 공격을 탐지한다. 특정시간(60초)동안만의 패킷을 모아서 60초가 되는 시점에 SR을 계산하여 공격여부를 판단하기 때문에, 근실시간 방식의 탐지 시스템이다. 또한 전체 DNS 패킷 중 BadQuery의 비율이 높은 경우에 공격으로 탐지하는 방식이기 때문에, 정상적인 쿼리를 이용하여 공격을 진행할 경우 탐지할 수 없는 한계가 있다.

본 논문에서는 기존 연구들의 한계를 극복하기 위하여, 실험망 환경의 데이터가 아닌 실제 환경의 네트워크 트래픽 데이터를 이용하여 학습한 딥 러닝 모델을 기반으로, 설계 및 구현한 실시간 탐지 시스템을 제안한다.

2.2 Deep Learning

딥 러닝은 머신러닝 기술의 일종으로 데이터를 분류 및 예측하는 기술이며 기존 Artificial Neural Network(이하 인공신경망)의 한계점을 극복하기 위해 제안되었다. 인공 신경망은 실제 뇌 신경망을 컴퓨터 처리 시스템에 맞는 형태로 변환시킨 것이다.

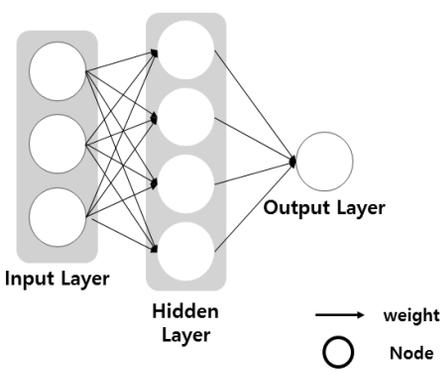


Fig. 2. Artificial Neural Network

Fig. 2는 인공신경망으로 입력 층인 Input Layer와 은닉층인 Hidden Layer, 그리고 출력 층인 Output layer로 이루어져있다. 은닉 층은 N개의 층으로 구성할 수도 있다. 각 층의 노드들이 가진 값이 다음 노드와 연결가중치(weight)를 기반으로 연결된다. 각 노드의 값과 연결가중치는 층마다 존재하는 활성화함수(Activation Function)에 전달되고, 계산된 값들을 통해 다음 노드의 값을 결정한다.

이와 같은 인공신경망과 관련된 연구는 여러 가지 한계점에 의해 연구가 진전되지 못했다. 인공신경망의 은닉 층이 깊어지더라도 학습의 결과나 성능이 크게 향상되지 않는 Vanishing Gradient Problem이 발생했는데, 인공신경망 내의 노드, 층, 노드 간 연결방법, 활성화 함수 등을 조정하는 것이 어려웠기 때문이다. 또한 높은 성능을 내는 구조를

찾기 위해서는 인공신경망 내의 방대한 요소들의 각 값을 일일이 찾아야 하며 최적화하는 방법론이 없었다. 당시 컴퓨팅 성능으로는 인공신경망의 방대한 계산 량을 처리할 수 없었으며, 인공신경망의 이론과 달리 SVM (Support Vector Machine)과 같은 기타 기계 학습 기법이 인공신경망 이상의 성능을 나타냈기 때문에, 인공신경망이 크게 주목받지 못했다. 인공신경망 내의 각 요소의 값이나 연결방법 등을 최적화하기 위한 연구나 깊은 층의 인공신경망을 학습하거나 최적화하기 위한 연구를 통해 다양한 방법이 제시되었다. 그 이후, 하드웨어를 비롯한 컴퓨팅 성능의 발전을 기반으로 인공신경망을 꾸준히 연구하였고 다수의 은닉층을 가진 Deep Neural Network와 같은 딥 러닝이 주목받기 시작했다.

딥 러닝의 경우 충분한 데이터 셋이 있다면 기존의 머신 러닝 기법에 비해 좋은 효율을 가지며, 데이터를 잘 정제한다면 어떠한 데이터든 상관없이 대용량의 데이터에 대해서도 빠르게 학습이 가능하다. 본 논문에서는 대용량의 데이터를 이용하여 공격 및 정상 트래픽의 특징과 패턴을 인식하기 위하여 이미지 인식에서 주로 활용되는 CNN을 기반으로 실시간 탐지 시스템을 구현한다.

2.3 기존의 기계학습/통계 관련 DDoS 탐지 연구

[9]는 네트워크 트래픽 분석에 퍼지 연관규칙을 이용하여, 트래픽 간의 연관 관계를 기반으로 DRDoS (Distributed Reflection Denial of Service) 공격을 탐지하는 방법에 대해 제안하였다. 네트워크 토폴로지 상에서의 네트워크 트래픽, 스트림을 기반으로 DRDoS가 발생할 수 있는 규칙을 이용해 공격을 탐지한다. 또한 실제 네트워크 환경의 토폴로지나 트래픽이 아닌, 구축한 실험망 환경에서 공격 탐지를 실험하였다. [9]의 탐지기법이 복잡하고 거대한 실제 네트워크 환경에서 제대로 잘 동작할 수 있을지는 보장할 수 없다.

[10]은 인공신경망 기반의 Classifier를 이용하여 DNS DDoS 공격을 탐지하는 방법을 제안하였다. 인공신경망의 학습 자질은 총 8개를 사용했으며, N개의 은닉 층을 가진 Feed-Forward 구조를 사용하였다. 학습. 검증 및 테스트에 사용한 데이터 셋의 개수는 총 2,880개로 본 연구에서 사용한 데이터 셋의 개수보다 현저히 적으며, 쿼리 전송률이 높은 High Rate 공격 데이터 셋만을 가지고 학습을 수행하였다.

[11]은 Rank Correlation을 이용하여 데이터 셋 간의 비교를 통해 DRDoS 공격을 탐지하는 방법을 제안하였다. 두 방법 모두 제안한 탐지 방법을 실험망 환경에서 검증하였기 때문에, 실제 환경에서의 탐지율을 보장할 수 없다. 데이터 간의 연관성이나 비교를 통해 공격을 탐지하는 방법인데, 실제 발생한 공격 데이터나 정상 데이터를 사용하지 않았기 때문이다. 또한 [11]이 제안한 방법의 경우, 네트워크 프로토콜에 관계없이 동일한 출발지 주소와 동일한 목적지 주소를 가진 모든 네트워크 패킷의 흐름과 패킷 수를 기반으로 공격을 탐지한다. 이러한 방법은 단순히 네트워크상의 출발지 및 목적지 주소를 기반으로 주고받은 패킷의 수만 확인하기 때문에, 대규모 서비스를 운영하는 서버에서는 정상적인 트래픽 데이터도 공격으로 탐지할 가능성이 높은 한계가 있다. 본 논문에서는 패킷의 수 뿐 만 아니라 다양한 특징을 고려하여 공격의 패턴을 인식하여 이러한 오탐율을 줄이고자 한다.

[12]는 기계 학습 알고리즘 종류 중 하나인 SVM (Support Vector Machine)을 기반으로 DRDoS 공격을 탐지하는 시스템을 제안하였다. 실험을 통해 얻은 학습, 검증 및 테스트 데이터를 이용하였고, 5개의 자질을 기계 학습에 사용하였다.

이처럼 기존의 기계학습이나 통계 등을 활용하여 DRDoS를 탐지하기 위한 연구들은 실험망 환경의 데이터 셋만을 사용하여 탐지 모델을 학습하였기 때문에 실제 환경에서의 탐지 결과나 효율성을 보장할 수 없으며, 실시간 탐지 시스템에 대한 방법을 구현하지 않았다. 또한 출발지/목적지 주소에 따른 패킷의 양이나 크기와 같이 단편적인 특징들만을 고려하여 학습을 수행하고 학습에 사용한 데이터 셋의 양이 적기 때문에, 변형된 공격에 대해서 탐지 결과를 보장할 수 없다. 본 논문에서는 이러한 한계점을 극복하기 위해, 공격이 발생할 수 있는 여러 가지 상황을 탐지하기 위해. 더 많은 수의 공격 특징을 고려하여 공격의 패턴을 인식하여 오탐율 및 미탐율을 줄이고자 한다. 또한 실제 환경의 데이터 셋을 일부 활용하였고 훨씬 더 많은 양의 데이터 셋을 확보하여 학습을 수행하였다.

3. 딥 러닝 기반의 실시간 DNS DDoS 탐지 시스템

이 장에서는 DNS DDoS 공격을 실시간으로 탐지하는 시스템을 구현하기 위해 설계한 시스템에 대하여 설명한다. Fig. 3은 실시간 탐지 시스템의 구성을 나타낸다.

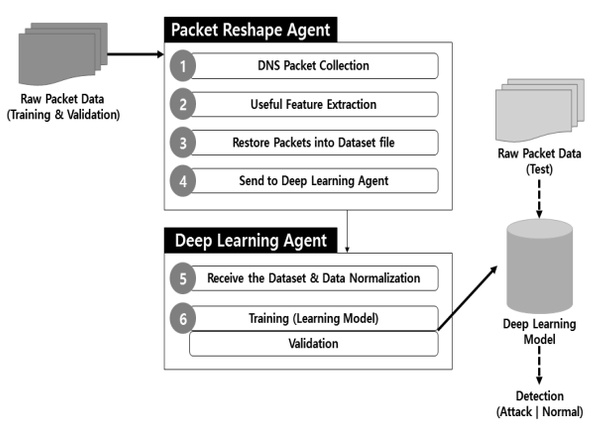


Fig. 3. Deep Learning Based Real-Time Detection System Structure

Raw Packet Data를 학습에 알맞은 형태의 데이터 셋으로 변환하는 Packet Reshape Agent와 기존의 데이터 셋으로 탐지 모델을 학습한 후, 학습한 모델을 기반으로 실시간 탐지를 수행하는 Deep Learning Agent로 구성된다.

3.1 Packet Reshape Agent

Packet Reshape Agent는 Raw Packet Data로부터 feature를 추출하고 학습에 사용하기 알맞은 형태로 변환하는 역할을 한다. Packet Resahpe Agent는 Fig. 4와 같이 ① DNS Packet Collection, ② Useful Feature Selection, ③ Restore Packets into Dataset file, ④ Send to Deep Learning Agent와 같은 단계로 구성된다.

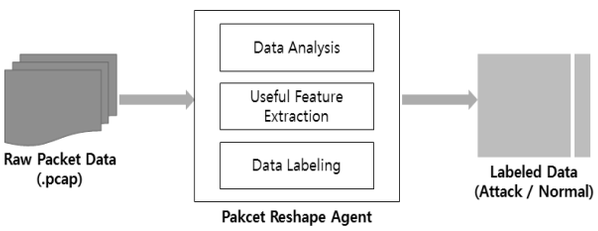


Fig. 4. Packet Reshape Agent Structure

①은 서버로 유입된 DNS 패킷을 수집한다. ②는 feature를 기반으로 수집된 DNS 패킷으로부터 딥 러닝 학습에 사용할 유용한 데이터들을 추출한다. ③은 추출한 데이터를 딥 러닝 학습 모델에 알맞은 형태의 파일인 데이터 셋으로 변환한다. ④는 생성한 데이터 셋 파일을 실제로 학습하기 위해 Deep Learning Agent에 전달한다.

3.2 Deep Learning Agent

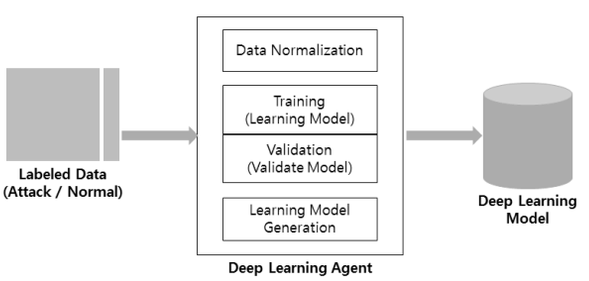


Fig. 5. Deep Learning Agent Structure

Deep Learning Agent는 전달받은 데이터 셋을 기반으로 DNS DDoS 공격을 탐지하기 위한 모델을 학습하고, 학습한 모델을 기반으로 공격을 탐지하는 역할을 한다. Fig. 5와 같이 ⑤ Receive the Dataset & Data Normalization과 ⑥ Training / Validation으로 구성된다.

⑤는 전달받은 데이터 셋의 각 feature들을 동일한 환경에서 비교 및 학습하기 위하여 Data Normalization을 수행한다. ⑥은 실제로 학습을 수행하는 Training과 학습된 모델을 검증하는 Validation을 수행한다. 본 논문에서 제안한 딥 러닝 기반의 탐지 시스템은 과적합(over-fitting) 문제를 해결하기 위하여 총 데이터 셋 중, 70%를 Training에 사용하고, 30%를 Validation에 사용하여 학습 모델을 검증한다. 또한 최종적으로 추가적인 Test 데이터 셋을 이용하여 모델의 탐지 정확도를 확인한다.

4. 구현 및 실험

4.1 데이터 셋(Dataset)

탐지 시스템을 학습하기 위해 사용할 데이터는 기존 연구들의 한계를 극복하고 유연한 탐지 방법을 구축하기 위해, 실제 환경에서의 데이터를 추가하였다. 국내 대형 통신사 서버에서 발생한 실제 트래픽 내 DNS 패킷과 [13]에서 사용한 DNS 기반 DDoS 공격 패킷을 사용하였다. Table 1은 학습에 사용할 각 패킷에 대한 정보를 나타낸다.

Table 1. DNS Packet list for Dataset

	# of Packet	Query Rate (Per Second)	Type
Booter1.pcap	8,682,985	21,108	Attack
Booter2.pcap	6,759,917	24,571	Attack
Booter3.pcap	4,338,367	15,168	Attack
Booter4.pcap	65,478	2,226	Attack
Booter5.pcap	1,944,062	6,934	Attack
Booter6.pcap	421,904	3,553	Attack
Booter7.pcap	659,191	1,421	Attack
Attack.pcap	3,559,600	1,407	Attack
Normal.pcap	29,116,704	1,560	Normal

탐지 시스템은 pcap 형태의 Raw Packet으로 학습을 수행할 수 없기 때문에, Raw Packet을 딥 러닝 학습에 알맞은 형태의 데이터 셋으로 변환하는 과정이 필요하다. go의 gopacket 라이브러리를 이용해 대용량의 패킷에서 원하는 데이터들을 추출하여 데이터 셋으로 변환하는 과정을 거친다.

하나의 패킷을 하나의 데이터 셋으로 변환하는 것은 실시간 탐지의 목표나 성능에 부적합하다고 판단했다. 그 이유는 서비스를 제공하는 서버의 경우 동시에 적게는 수백 개의 패킷을, 많게는 수천 개의 패킷을 수신하기 때문에 패킷 하나씩 탐지 시스템에 입력할 경우, 탐지 시스템에 입력해야 할 데이터의 수가 많아져 성능에 문제가 발생할 우려가 있기 때문이다. 또한 DDoS와 같은 공격은 하나의 패킷으로 공격의 패턴을 인식할 수 없고, 일련의 패킷 덩어리에서 공격의 패턴을 인식해야하기 때문에, 다수의 패킷을 하나의 데이터로 변환하는 방법을 선택했다. 패킷으로부터 Table 2와 같이 21개의 자질을 추출하며, 약 400개의 패킷의 값들을 압축하여 하나의 데이터로 변환한다.

하나의 패킷이나 일부 소량의 패킷으로부터 추출한 데이터를 기반으로 공격을 탐지하는 것은 탐지 시스템의 성능을 저하시키며, 오탐율이 높아질 가능성이 있다. 그렇기 때문에 Fig. 6과 같이 추출한 각 데이터와 패킷 덩어리를 21x21의 2차원 행렬로 표현한다. 이 경우, 패킷 덩어리 하나의 패턴만 이용하여 공격을 탐지하지 않고 연속된 여러 패킷을 고려하여 공격의 패턴을 인식할 수 있고, 탐지 시스템의 성능에 미치는 영향을 최소화할 수 있다.

Table 2. Feature list for Learning

Feature	Description
Packet Per Second	Query Rate Per Second
# of RR	Total Number of Resource Records
# of Answer	Number of Answer Sections
# of Authority	Number of Authority Sections
# of Additional	Number of Additional Sections
Size of Answer	Size of Answer Section
Size of Authority	Size of Authority Section
Size of Additional	Size of Additional Section
RR Type	Question Section's Resource Record Type
Length of Q-CName	Question Section's CName Length
Class of Answer	Answer Section Class
Class of Authority	Authority Section Class
Class of Additional	Additional Section Class
Answer Type	Answer Section Type
Authority Type	Authority Section Type
Additional Type	Additional Section Type
Name of Answer	Answer Section RR's Name Length
Name of Authority	Authority Section RR's Name Length
Name of Additional	Additional Section RR's Name Length
SDL Length	Second Domain Level's Length
UDP Packet Size	Size of the UDP Packet

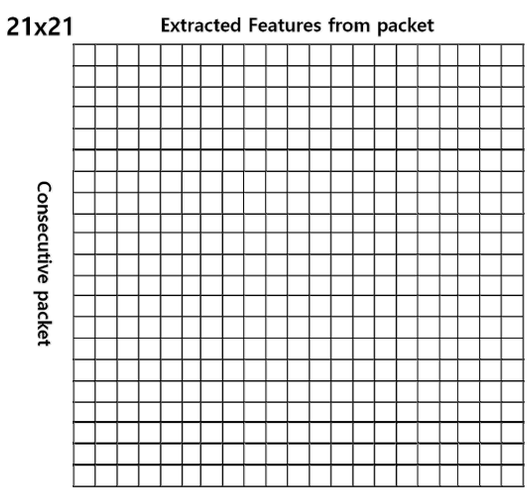


Fig. 6. Dataset Form

Table 3은 패킷 데이터를 압축하여 실제 학습과 학습 모델 검증에 사용할 Training / Validation 데이터 셋을 나타낸다. 과적합(over-fitting) 문제를 해결하기 위해서 전체 데이터 셋 94,182개 중 약 70%인 65,927개를 학습에 사용하고, 약 30%인 28,255를 검증에 사용한다.

Table 4는 탐지 모델이 공격을 정확하게 분류하는지, 그리고 유연하게 탐지하는지 확인하기 위한 Test 데이터 셋을 나타내며, 학습 과정에서 사용하지 않은 Low Rate 공격 패킷을 추가적으로 테스트한다. Low Rate 공격 패킷은 초당 전송률이 기존 공격 패킷보다 낮으며, 정상 트래픽과 유사해 트래픽 량과 같은 기초적인 정보로는 탐지가 어렵다.

Table 3. Training/Validation Dataset

	Type	#	Total
Booter1.pcap	Attack	20,671	47,091
Booter2.pcap		16,093	
Booter3.pcap		10,326	
Normal.pcap	Normal	47,091	47,091

Table 4. Test Dataset

	Type	#	Total
Booter4.pcap	Attack (Low Rate)	155	12,383
Booter5.pcap		4,628	
Booter6.pcap		1,004	
Booter7.pcap		1,569	
Attack.pcap		5,027	
Normal.pcap	Normal	17,141	17,141

4.2 딥 러닝 기반의 탐지 시스템 구현 및 학습

본 논문에서는 딥 러닝 알고리즘 중 이미지 인식, 영상처리 등에 주로 쓰이는 CNN을 적용하여 탐지 시스템을 구현하였다. 탐지 시스템은 Python으로 작성하였으며, 실제 탐지를 수행하는 딥 러닝 모델은 Tensorflow를 기반으로 작성하였다[14].

1) CNN 기반의 탐지 시스템

CNN은 은닉 층이 깊어져도 정밀도가 떨어지는 문제가 발생하지 않으며, 일련의 패킷 덩어리를 하나의 이미지처럼 변환하고 해당 데이터에서 패턴을 정밀하게 인식하기 위해 딥 러닝 알고리즘으로 선정하였다.

CNN은 데이터로부터 자질을 추출하는 Convolutional Pooling Layer와 추출된 자질을 기반으로 분류를 수행하는 Fully Connected Layer로 구성되어 있다. Convolutional Pooling Layer는 필터와 Stride를 이용하여 2차원 행렬 형태의 데이터로부터 자질을 추출한다. 본 연구에서 구현한 딥 러닝 모델은 3x3 필터를 이용하여 최댓값을 추출하는 Max Pooling 기반의 Convolutional Pooling을 수행한다. Fully Connected Layer를 추출한 자질들과 가중치 값을 활성화 함수에 전달해 실제 입력 데이터의 클래스를 분류한다. Fig. 7은 본 논문에서 구현한 탐지 시스템에서 사용하는 CNN 모델을 나타낸다.

4.3 학습 및 테스트 결과

go 언어의 gopacket 라이브러리를 기반으로 패킷 분석을 통해 데이터 셋을 생성하는 Packet Reshape Agent와 Python Tensorflow를 기반의 딥러닝 모델을 통해 실제 학습 및 탐

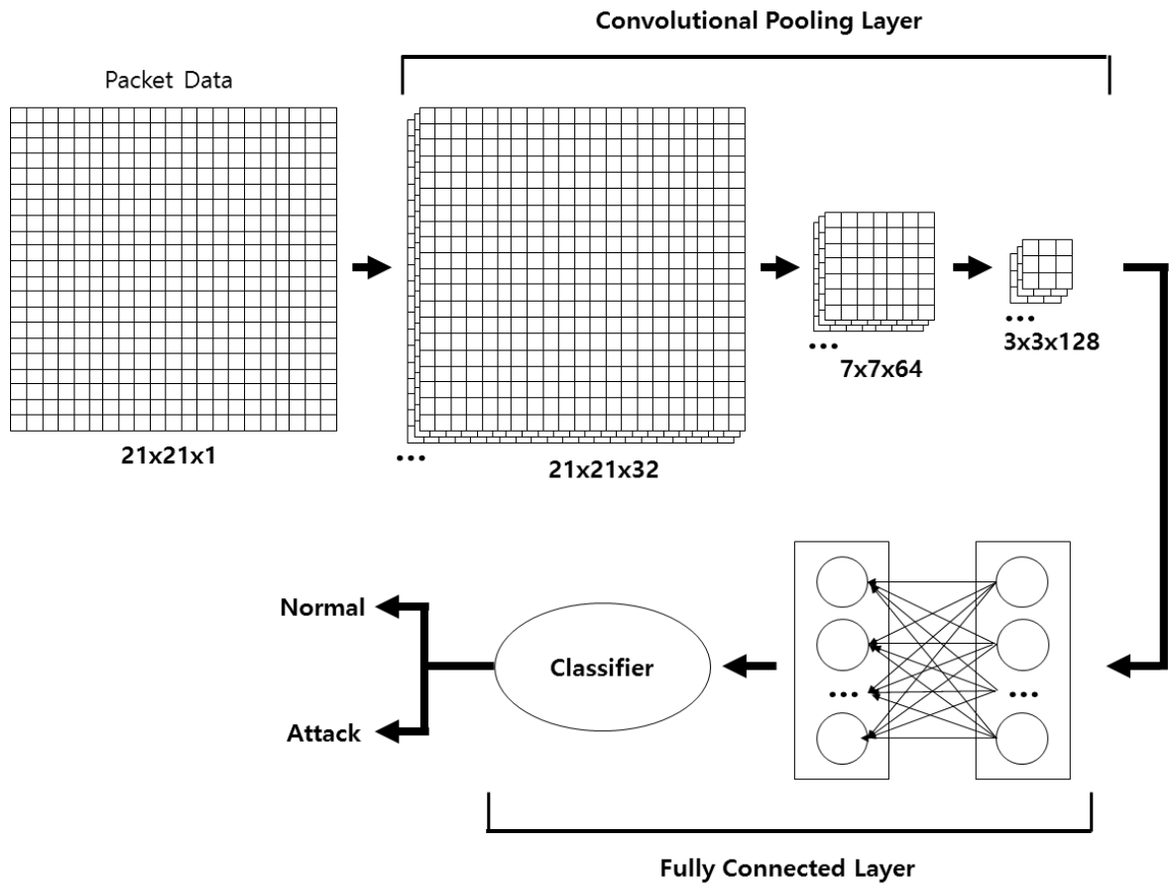


Fig. 7. CNN Model for Real-Time Detection System

지를 수행하는 Deep Learning Agent를 구현하였다. High Rate 기반의 공격 데이터로 구성된 Training/Validation 데이터 셋으로 딥 러닝 모델을 학습시키고, 모델의 탐지 성능을 확인하기 위해 Low Rate 기반의 공격 데이터가 혼합된 Test 데이터를 사용하여 테스트를 수행한다. Figs. 8과 9는 각각 학습/검증에 사용할 데이터 셋과 테스트에 사용할 데이터 셋의 초당 패킷 전송률을 나타낸다. 테스트 데이터 셋의 경우 정상 패킷과 비슷한 전송률을 보이는 Low Rate 공격이 포함되어 있다.

검증 데이터 셋과 테스트 데이터 셋에 대한 TP(True Positive), TN(True Negative), FP(False Positive), FN(False Negative)과 Recall(재현율), Precision(정밀도), Detection Accuracy(탐지 정확도)를 나타내며, 각 항목은 다음과 같이 계산한다.

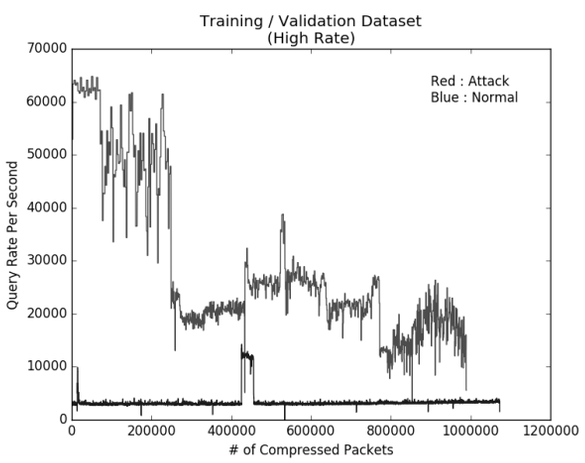


Fig. 8. Query Rate of Training / Validation Dataset

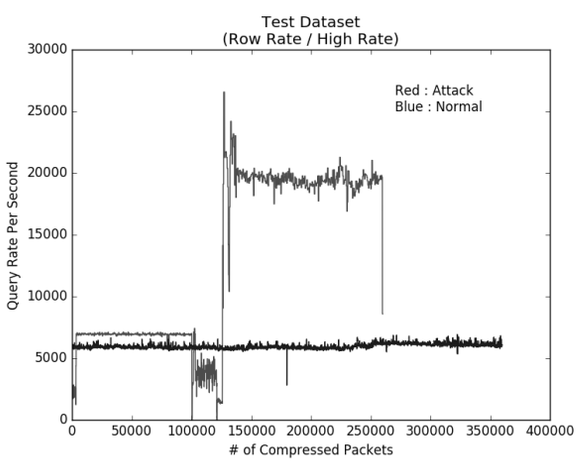


Fig. 9. Query Rate of Test Dataset

Table 5. Validation/Test Dataset Recall, Precision, Detection Accuracy

		Attack		Normal		Recall(%)	Precision(%)	Detection Accuracy (%)
		TP	FN	TN	FP			
Validation Dataset		47,039	52	46,732	359	99.88%	99.24%	99.56%
Test Dataset	[10]	45	10	377	0	81.81%	100%	97.68%
	[11]	NA	NA	NA	NA	97.51%	59.35%	78.43%
	[12]	NA	NA	NA	NA	95.86%	99.65%	97.76%
	ours	11,968	415	17,130	11	96.64%	99.90%	**98.55%**

본 논문에서 제안한 시스템은 공격 트래픽을 탐지하는 것이 목적이기 때문에 TP는 공격 패킷을 공격으로 탐지한 것을 의미하며, FN은 공격 패킷을 정상으로 탐지한 경우를 의미한다. 또한 TN은 정상 패킷을 정상으로 제대로 탐지한 것을 의미하며, FP는 정상 패킷을 공격으로 탐지한 것을 의미한다. 이 때, Recall은 실제 DDoS 공격인 데이터 셋 중에서 딥 러닝 모델이 공격으로 예측한 비율로 TP / TP + FN을 통해 계산하며 Precision은 딥 러닝 모델이 공격으로 예측한 것 중 실제로 공격 데이터 셋이 얼마나 차지하는 지를 나타내는 비율로, TP / TP + FP를 통해 계산한다. 최종적으로 Detection Accuracy는 TP + TN / TP + FN + TN + FP를 이용하여 계산한다.

Table 5와 같이 기존 연구들과의 탐지 결과를 비교하였다. 기존 연구들과 다른 데이터 셋을 사용하였지만, 본 연구의 경우 기존 연구에 비교하여 많은 양의 데이터 셋을 사용하였고, 기존 연구들은 실험망 환경에서 시뮬레이션을 통해 획득한 데이터 셋을 사용하여 학습 및 테스트를 수행하였다. 하지만 본 논문은 실 환경의 정상 및 공격 패킷 및 트래픽을 기반으로 생성한 데이터 셋을 활용하였으며, 언급되지 않은 Low Rate 공격과 관련된 공격 패킷도 혼합하여 탐지 시스템을 테스트 하였다.

[10]의 경우 본 논문과 비교하여 테스트에 사용한 데이터 셋이 극히 적으며, [11, 12]의 경우 테스트 데이터 셋의 개수가 명시되지 않아, 언급된 TPR(True Positive)과 FPR(False Positive Rate)을 이용하여 Recall과 Precision, 최종 탐지 정확도의 평균을 계산하여 비교하였다. 본 논문의 다른 기존 연구들에 비해 높은 탐지 정확도를 가지며, 실제 환경 데이터로도 높은 탐지율을 나타냈다.

5. 결 론

CNN을 이용한 딥 러닝 알고리즘을 통하여 DNS DDoS 공격을 탐지하는 시스템을 제안하였다. 초당 전송률과 같은 단편적인 자질들 이외에 다른 자질들을 이용하여 탐지 모델을 학습시켰고, 그 결과 High Rate의 DNS DDoS 공격 뿐 아니라 기본적인 공격보다 전송률이 현저히 낮거나 정상 트래픽과 비슷한 Low Rate에 대한 공격도 약 90%~95% 정도 탐지하는 것을 확인하였다.

향후 실 환경 데이터를 추가하여 변형된 다양한 공격에 대해 탐지할 수 있는 유연한 탐지 시스템으로 확장시킬 예정이며, DNS 뿐만 아니라 다른 프로토콜을 이용한 증폭 공격 및 DDoS 공격에 대한 탐지 시스템으로 확장시킬 예정이다.

References

[1] DNSSEC and DNS Amplification Attacks [Internet], https://technet.microsoft.com/en-us/security/hh972393.aspx.

[2] 2015 Q4 DDoS Attack Trends Verisign [Internet], https://www.verisign.com/assets/infographic-ddos-trends-Q42015.pdf.

[3] Ye, Xi and Yiru Ye, “A practical mechanism to counteract DNS amplification DDoS attacks,” *Journal of Computational Information Systems*, Vol.9, No.1, pp.265-272, 2013.

[4] Yu, Huiming et al., “A visualization analysis tool for DNS amplification attack,” *Biomedical Engineering and Informatics (BMEI), 2010 3rd International Conference on*, Vol.7. IEEE, 2010.

[5] Wei-Min, Li, Chen Lu-Ying, and Lei Zhen-Ming, “Alleviating the impact of DNS DDoS attacks,” *Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second International Conference on.*, Vol.1. IEEE, 2010.

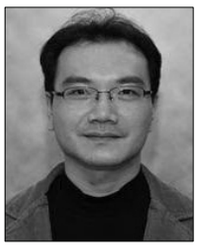
[6] Rozekrans, Thijs, Matthijs Mekking, and Javy de Koning, “Defending against DNS reflection amplification attacks,” University of Amsterdam, Tech. Rep., Feb., 2013.

[7] Zdrnja, Bojan, Nevil Brownlee, and Duane Wessels, “Passive monitoring of dns anomalies,” Detection of Intrusions and Malware, and Vulnerability Assessment. Springer Berlin Heidelberg, pp.129-139, 2007.

[8] Lee, Ki-Taek, Seung-Soo Baek, and Seung-Joo Kim, “Study on the near-real time DNS query analyzing system for DNS amplification attacks,” *Journal of the Korea Institute of Information Security and Cryptology*, Vol.25, No.2, pp.303-311, 2015.

[9] Yang, Xinyu et al., “The Detection and Orientation Method to DRDoS Attack Based on Fuzzy Association Rules,” *Journal of Communication and Computer,* Vol.3, No.8, pp.1-10, 2006.
[10] Wu, Jun et al., “Detecting DDoS attack towards DNS server using a neural network classifier,” International Conference on Artificial Neural Networks, Springer Berlin Heidelberg, 2010.
[11] Wei, Wei et al., “A rank correlation based detection against distributed reflection DoS attacks,” *IEEE Communications Letters*, Vol.17, No.1, pp.173-175, 2013.
[12] Gao, Yuxuan et al., “A Machine Learning Based Approach for Detecting DRDoS Attacks and Its Performance Evaluation,” *Proc. of the 11th Asia Joint Conference on Information Security*, 2016.
[13] Santanna, José Jair et al., “Booters－An analysis of DDoS-as-a-service attacks,” *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*. IEEE, 2015.
[14] Abadi, Martın et al., “Tensorflow: Large-scale machine learning on heterogeneous distributed systems,” arXiv preprint arXiv:1603.04467 (2016).

서 인 혁
e-mail : inhack@korea.ac.kr
2015년 한양대학교 ERICA 캠퍼스 컴퓨터공학과(학사)
2015년～현 재 고려대학교 정보보호대학원 정보보호학과 석사과정
관심분야 : Software Testing, Software Security, Machine Learning



이 기 택
e-mail : zizihacker@korea.ac.kr
2000년 동아대학교 컴퓨터공학과(학사)
2001년～2003년 ㈜해커스랩
2005년～현 재 SK브로드밴드 정보기술원 매니저
2011년～현 재 고려대학교 정보보호대학원 정보보호학과 석・박사통합과정 수료
관심분야 : OS Security, Android Security, IoT Security, Data Analysis

유 진 현
e-mail : gnyun@korea.ac.kr
2014년 전북대학교 컴퓨터공학부(학사)
2015년～현 재 고려대학교 정보보호대학원 정보보호학과 석사과정
관심분야 : Mobile Security, Software Security, Machine Learning

김 승 주
e-mail : skim71@korea.ac.kr
1994년 성균관대학교 정보공학과(학사)
1996년 성균관대학교 정보보호학과(석사)
1999년 성균관대학교 정보보호학과(박사)
1998년～2004년 KISA 팀장 (舊한국정보보호진흥원)
2004년～2011년 성균관대학교 정보통신공학부 조교수, 부교수
2011년～현 재 고려대학교 사이버국방학과/정보보호대학원 정교수
관심분야 : Security Engineering, Security Threat-Risk Modeling, Security Testing, Security Evaluation, Usable Security