정 보 보 호 학 회 지
제 29 권 제6호, 2019. 12

인공신경망 알고리즘을 통한 사물인터넷 위협 탐지 기술 연구

오 성 택*, 고 웅*, 김 미 주*, 이 재 혁*, 김 홍 근*, 박 순 태*

요 약

사물인터넷 환경은 무수히 많은 이기종의 기기가 연결되는 초연결 네트워크 구성을 갖는 특성이 있다. 본 논문에서는 이러한 특성을 갖는 사물인터넷 환경에 적합한 보안 기술로 네트워크를 통해 침입하는 위협의 효율적인 탐지 기술을 제안한다. 사물인터넷 환경에서의 대표적인 위협 행위를 분석하고 관련하여 공격 데이터를 수집하고 이를 토대로 특성 연구를 진행하였다. 이를 기반으로 인공신경망 기반의 오토인코더 알고리즘을 활용하여 심층학습 탐지 모델을 구축하였다. 본 논문에서 제안하는 탐지 모델은 비지도 학습 방식의 오토인코더를 지도학습 기반의 분류기로 확장하여 사물인터넷 환경에서의 대표적인 위협 유형을 식별할 수 있었다. 본 논문은 1. 서론을 통해 현재 사물인터넷 환경과 보안 기술 연구 동향을 소개하고 2. 관련연구를 통하여 머신러닝 기술과 위협 탐지 기술에 대해 소개한다. 3. 제안기술에서는 본 논문에서 제안하는 인공신경망 알고리즘 기반의 사물인터넷 위협 탐지 기술에 대해 설명하고, 4. 향후연구계획을 통해 추후 활용 방안 및 고도화에 대한 내용을 작성하였다. 마지막으로 5. 결론을 통하여 제안기술의 평가와 소회에 대해 설명하였다.

Ⅰ. 서 론

사물인터넷은 여러 사물들에 정보통신기술이 접목되어 인터넷을 통해 실시간으로 데이터를 공유하는 기술이다. 실생활에서 흔히 사용되는 가전제품 등을 인터넷과 연결하여 사용자가 원격에서 다양한 정보를 확인하고 사물의 제어를 할 수 있는 것이 큰 특징이다. 최근 5G 네트워크가 크게 발달되면서 사물인터넷의 활용도가 커지며 관련 시장이 급격히 확대되고 있다. 시장조사업체 IHS마켓의 분석 결과에 따르면 전 세계 사물인터넷 장비대수는 2020년 400억대에서 2030년 1,400억대로 급증할 것으로 전망되고 있으며, 또한 전 세계 사물인터넷 2019년 상반기 지출은 7,265억 달러로 전년대비 17.1% 증가하였으며 19-23년 기대 연평균성장률은 12.6%에 달한다. 하지만 이와 관련하여 침해 사고의 규모도 매우 커질 것으로 예측되고 있다. KT 경제경영연구소의 조사에서는 2030년 국내 사물인터넷 해킹 피해액만 26조 7천억에 달할 것으로 분석되고 있다. 사물인터넷과 관련된 보안 우려 사항에 대한 조사 결과에서도 정보유출(44.3%), 해킹 및 악성코드 감염(42.7%)에 많은 우려를 보이고 있는 것으로 조사되었다. 사물인터넷이 생활에 밀접해지면서 금전적인 피해뿐만 아니라 생명에도 피해를 입힐 수 있기 때문에 사물인터넷 보안에도 큰 관심이 집중되고 있다. 현재 국내 사물인터넷 보안 기술 연구는 기기 인증 및 암호화를 초점으로 연구개발이 진행되고 있으며, KISA에서는 사물인터넷 제품의 보안내재화를 위해 사물인터넷 하드웨어와 소프트웨어 전반에 걸쳐 준수해야 할 7개의 보안원칙을 제시한 '사물인터넷 공통 보안원칙'을 발표하고 사물인터넷 공통보안 가이드를 제공하였다. 하지만 사이버 침해사고 발생에 대한 대응 기술은 미흡한 상태이다. 국외의 경우 사물인터넷 보안법을 제정하여 기기의 설계 단계부터의 보안 내재화를 법적으로 의무화 하는 등 사물인터넷 보안에 적극적으로 대응하고 있다. 하지만 기존에 사용되고 있는 다양한 사물인터넷 제품들은 여전히 취약한 상태로 인터넷에 연결되어 미라이 등의 악성코드의 공격 대상이 되고 있다. 또한 리소스가 제한된 저사양의 사물인터넷

이 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2018-0-00232, 클라우드 기반 IoT 위협 자율 분석 및 대응 기술개발)

* 한국인터넷진흥원 정보보호R&D기술공유센터 보안위협대응R&D팀 ({angelrick, wgo, mijoo.kim, jaehyuk, kimhg, stpark12}@kisa.or.kr)

제품들은 보안 내재화에 한계가 존재한다. 이러한 보안이 미흡한 사물인터넷 기기를 대상으로 하는 공격이 증가하고, 기존의 ICT 환경의 주요 침해사고가 향후 사물인터넷 환경으로 전이·확산될 것으로 예상된다. 보안에 대한 전문 지식이 부족한 사물인터넷 기기 사용자는 침해사고의 발생여부조차 인지하기 어려우며, 인지하여도 대응하기가 쉽지 않다. 본 논문에서는 이러한 사물인터넷 환경적 특성을 고려하여 사용자의 개입 없이 사물인터넷 장치의 네트워크 패킷 정보를 활용하여 위협을 탐지하며 다양하고 리소스가 제한된 사물인터넷 기기들을 대상으로 이뤄지는 위협의 탐지와 대응을 위한 인공신경망 알고리즘 기반의 탐지 기술을 제안한다.

Ⅱ. 관련연구

2.1. 기계학습

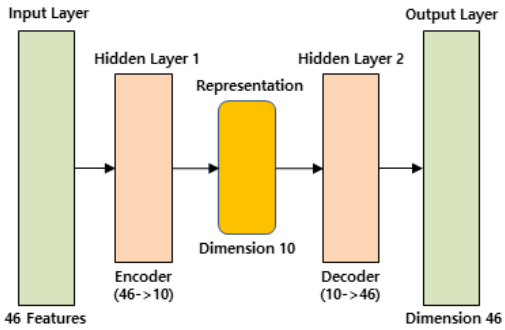
기계학습은 명시적으로 작성된 프로그램에 따라 동작하는 것이 아닌 데이터로부터 학습을 통해 작업을 수행할 수 있도록 가르치는 것이다. 이러한 기계학습은 인공지능의 한 분야로 컴퓨터가 여러 데이터를 이용하여 학습한 내용을 바탕으로 예측이나 결정을 도출하기 위해 특정한 모델을 구축한다. 기계학습은 학습하는 환경 혹은 데이터의 속성 형태에 따라 지도학습, 비지도학습, 강화학습으로 나뉜다. 지도학습 방식은 정답이 정해진 문제에 대해 정해진 특성 정보를 통해 학습을 하고 모델을 생성한다. 그리고 생성된 모델을 통해 주어진 문제의 정답을 분류(Classification)한다. 비지도학습 방식은 지도학습의 정답의 분류와는 다르게 정답이 없는 데이터의 패턴을 분석 및 학습하여 유사한 데이터로 군집화(Clustering)하거나 유사한 데이터의 군집과 동떨어진 이상 데이터의 탐지에 활용된다.

2.2. 심층학습

심층학습은 하나 이상의 숨겨진 계층을 포함하는 학습 작업들에 인공신경망을 적용하는 것이다.

2.2.1. Autoencoder

입력되는 데이터를 조합하고 압축하여 데이터를 더욱 효율적으로 표현하는 성질이 있다. 신경망이 다층 구조인 경우 학습이 제대로 되지 않는 문제가 있었으나 2006년 제프리 힌튼 교수가 오토인코더 학습 방식을 제안하였다. 오토인코더 신경망 구조는 각 층을 순차적으로 학습하며 최종 출력이 최초 입력과 동일하게 재현되도록 특성을 압축하고 조합한다. 입력 층과 출력 층의 노드의 개수는 동일하며, 은닉 층은 노드 개수를 줄여야 한다. 은닉 층의 노드 개수가 적기 때문에 신경망은 데이터를 압축하고 조합하며 특징을 추출하게 된다.



(그림 1) 오토인코더 신경망 모델 구조

Ⅲ. 제안기술

3.1. NSL-KDD 데이터 셋

기존 DARPA'98 침입탐지시스템 평가 프로그램에서 수집된 데이터를 기반으로 만들어진 KDD CUP(KDD'99)에서 중복된 레코드를 삭제하고, 크기를 줄여 특정 공격에 치우치게 학습되지 않도록 가공한 데이터 셋 이다[1]. 분류 알고리즘이 bias 되지 않은 결과를 도출할 수 있도록 중복된 레코드를 제거하였다. 학습 및 검증 데이터 셋에서 적절한 수의 레코드를 사용할 수 있으며, 학습 셋은 125,973건, 검증 셋은 22,544건의 레코드로 축소하였다. 총 42개의 특성으로 41개의 서로 다른 특성과 1개의 분류한 공격 클래스로 구성되어 있으며, 각 특성들은 다른 데이터 유형을 갖고 있다[2]. 각 샘플들은 '정상' 또는 '공격'으로 분류되어 있으며, 그림 3과 같이 39개의 다른 공격 유형은 4개의 클래스로 분류할 수 있다. 정상, DoS, Probe, R2L, U2R 총 5개 클래스로 분류하였다.

네트워크 트래픽 데이터에서 가공하여 공격 탐지에 유효한 41개 특성으로 구성되어 있다. 4가지 유형(기

데이터 타입	속성
Nominal (3)	protocol_type, Service, Flag
Binary (6)	land, logged_in, root_shell, su_attempted, is_host_login, is_guest_login
Numeric (32)	duration, src_bytes, dst_bytes, wrong_fragment, urgent, hot, num_failed_logins, num_compromised, num_root, num_file_creations, num_shells, num_access_files, num_outbound_cmds, count, srv_count, serror_rate, srv_serror_rate, rerror_rate, srv_rerror_rate, same_srv_rate, diff_srv_rate, srv_diff_host_rate, dst_host_count, dst_host_srv_count, dst_host_same_srv_rate, dst_host_diff_srv_rate, dst_host_same_src_port_rate, dst_host_srv_diff_host_rate, dst_host_serror_rate, dst_host_srv_serror_rate, dst_host_rerror_rate, dst_host_srv_rerror_rate

(그림 2) 특성 별 데이터 타입

Category	Attack Type	Description
Probing (Probe)	satan	probing of a network for some well-known weaknesses
	ipsweep	pinging of multiple hosts to reveal the target's IP
	portsweep	scanning of ports to discover services on a host
	nmap	various means of network mapping
Remote to Local (R2L)	warezclient	downloading illegal software uploaded previously by the warezmaster
	guess_passwd	guessing password over telnet
	warezmaster	uploading illegal software (warez) on FTP server exploiting wrong write permissions
	imap	illegal access of local user account using vulnerabilities
	ftp_write	creating rhost file in anonymous FTP to obtain local login
	multihop	multi-day scenario where a user breaks into a system
	phf	CGI script enabling to execute arbitrary commands on a machine with a misconfigured web server
	spy	breaking into system via vulnerabilities to discover important information
User to Root (U2R)	buffer_overflow	the ffbconfig UNIX system command causes buffer flow leads to root shell
	rootkit	enables to access admin level
	loadmodule	gaining root shell by resetting IFS
	perl	creating root shell by perl attack which sets the user id to root
Denial of Service (DoS)	smurf	flooding of ICMP echo reply
	Neptune	flooding of SYN on port(s)
	back	requesting of a URL having many backslashes from a webserver
	teardrop	causing system reboot or crash using mis-fragmented UDP packets
	pod	pinging with malformed packets causing reboot or crash
	land	ending UDP packet having the same source and destination address to remote host

(그림 3) 클래스 별 공격 유형

본, 패킷 콘텐츠, 타임 윈도우, 호스트)으로 분류하였으며, IP주소와 Port 정보는 포함되어 있지 않다. 본 논문에서는 5튜플 정보와 패킷 길이와 연관된 특성을 위주로 분석하였다.

3.2. 기술 검증을 위한 데이터 셋

공개된 공격 도구를 활용하여 사물인터넷 공격 데이터 셋을 그림 4와 같이 생성하였다. Pyrai, LOIC, scapy를 활용한 스크립트를 활용하여 임의의 PC에서 공격을 수행한 후 IP, MAC 주소를 수정하여 사물인터넷 환경에서 발생한 것처럼 보이도록 조작하였다.

유형	세부 유형	패킷 수 (비율)
Normal (정상)	Normal	1,849,264 (62.11%) * 공격 파일 내 정상 패킷 포함
Reconnaissance (정찰)	Host Discovery	2,454 (0.08%)
	Port Scanning	20,939 (0.70%)
	OS and Service Detection	1,820 (0.06%)
Man In The Middle (MITM)	ARP Spoofing Attack	540 (0.02%)
Denial of Service (DoS)	SYN Flooding Attack	64,646 (2.17%)
Mirai Botnet – 전파 단계	Host Discovery	949,284 (31.88%)
	Telnet Bruteforce	75,632 (2.54%)
Mirai Botnet – DDoS 공격 단계	UDP Flooding Attack	10,464 (2.54%)
	HTTP Flooding Attack	673 (0.02%)
	ACK Flooding Attack	1,924 (0.06%)

(그림 4) 생성된 데이터 셋

3.3. 인공신경망 기술을 적용한 위협 탐지 기술

본 논문에서 제안하는 인공신경망 기반의 사물인터넷 위협 탐지 기술은 오토인코더 신경망 구조와 소프트맥스 함수의 적용을 통해 비지도 학습 방식인 오토인코더의 결과를 소프트맥스 함수에 연결하여 탐지하고자 하는 위협을 분류하는 기술이다. 이를 위해 사물인터넷 환경에서 주로 발생하는 위협에 대해 분석하고 분석정보를 통해 탐지를 위한 특성 정보를 도출하였으며, 오토인코더의 인코더 부분과 소프트맥스 함수를 연결하여 위협을 식별하였다. 오토인코더가 사물인터넷 네트워크 패킷을 효율적으로 압축할 수 있다고 판단하였고, 공격의 탐지를 위하여 오토인코더를 지도학습 기반의 분류기로 확장할 수 있도록 소프트맥스 함수를 연결하여 모델을 생성하였다.

3.3.1. 사물인터넷 환경 위협 분석

사물인터넷 환경에서의 침입 탐지 연구 논문들에서 공통적으로 다루는 공격 유형을 표1과 같이 분류하였으며, U2R(User to Root)과 같은 네트워크상에서 확인하기 어려운 공격은 제외하였다.

3.3.2. 오토인코더 알고리즘

본 논문에서 제안하는 연구를 위해 1차적으로 네트워크 패킷 데이터로부터 특성을 추출하였지만 몇 개의 특성이 조합되었을 때 패킷의 특성을 더욱 잘 나타낼 수도 있기 때문에 이러한 가능성을 염두에 두어 오토인코더를 활용하였다. 감시 네트워크와 사물인터넷 환경을 세팅하여 크지 않은 규모의 로컬 네트워크에서 여러 개의 오토인코더를 앙상블 하여 공격을 효과적으로 탐지할 수 있음을 기존 연구를 통하여 확인하였다[3].

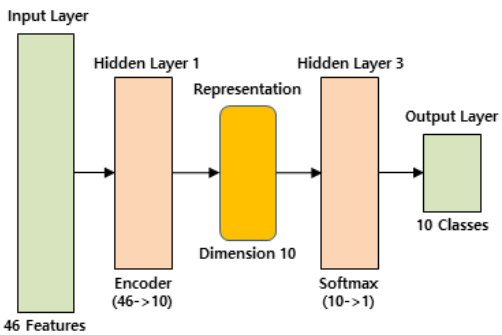
3.3.3. 소프트맥스 함수 적용

오토인코더의 인코더 출력 값을 N개의 클래스로 분류하기 위해 소프트맥스 함수를 적용하였다. 정상 패킷과 공격 패킷의 주요한 특징을 추출하여 패킷의 종류를 분류할 수 있다. 소프트맥스 함수는 인공신경망 구조에서 출력 층의 정규화를 위한 함수로 인공신경망의

〔표 1〕 공격 유형 분류

클래스	정의
DoS attack	· 컴퓨터의 리소스나 메모리를 소모시켜 유효한 사용자의 접근을 막는 공격 · neptune, teardrop, ping of death, back, mail bomb, smurf, land
Probe attack	· 보안을 피해 네트워크상의 컴퓨터에서 데이터를 가져오는 공격 · nmap, ipsweep, satan, portsweep
R2L attack (Remote to Local)	· 계정을 소유하지 않은 사용자가 시스템 취약점을 이용하여 유효한 사용자 계정의 로컬에 접근 · phf, warezclient, warezmaster, spy, ftp, write, imap, multihop
U2R attack (Users to Root)	· 유효한 사용자 계정을 통해 시스템에 접근하여 시스템 약점을 악용하여 루트 구성 요소에 접근 · buffer overflow, load-module, rootkit, perl

노드의 출력 값에 대하여 클래스 분류를 위하여 마지막 단계에서 출력 값에 대해 정규화 한다.



〔그림 5〕 소프트맥스 함수 적용 모델 구조

3.3.4. Feature Engineering

현재 사물인터넷 환경에서도 실제로 사용하는 프로토콜은 일반 환경에서도 흔히 쓰이는 프로토콜을 사용한다. 그렇기 때문에 공격을 탐지하는데 있어 특성 정보가 크게 달라지기 어려운 부분이 있다. 하지만 사물인터넷 환경에 특화된 특성 정보를 연구를 통해 분석하였다. 사물인터넷 환경에서의 주로 발생하는 공격은 미라이 봇넷 공격이다. 이러한 분산 서비스 거부 공격 유형에 집중된 특성 정보를 추출하였다. 전송된 패킷 간의 시간차를 특성정보로 활용하거나 출발지와 목적지의 주소정보 간의 패킷 수와 같이 기존 연구에서도 본 논문에서 분석한 특성정보와 유사한 특성을 활용하고 있다[10-11]. 아직은 사물인터넷 네트워크상에서 실제 사물인터넷 데이터 셋을 활용한 침입탐지 모델에 대한 연구가 충분히 많이 이루어지지는 않았기에 어떤 모델이 사물인터넷 침입 탐지에 적합하다고 판단하기 어려우며, 어떤 특성 정보가 기존 환경과 달리 사물인터넷 환경에 특히 적합하다고 선정하기도 어려운 부분이 있었다. 특성 연구를 통하여 추출된 특성 정보를 오토인코더 알고리즘을 활용하여 한 번 더 압축하여 표현하였고, 좀 더 성능을 보완할 수 있었다. 본 논문에서는 24개의 특성정보를 추출하였으며, 이중 4개의 특성 정보는 One Hot 인코딩을 통하여 26개 특성 정보를 늘려 총 46개 특성 정보를 활용한다.

3.3.5. ICMP 관련 특성 정보

ICMP 관련 특성 정보는 ICMP 프로토콜을 이용한 DoS 공격을 탐지하기 위하여 추가한 특성정보이다. ICMP 공격에는 Ping 플러딩, ICMP echo 플러딩, smurf 공격 등이 있다. 플러딩 공격에는 ICMP 프로토콜의 특정 Type과 Code의 패킷을 이용하므로 ICMP의 Type과 Code 필드 부분을 특성 정보로 활용하였다. ICMP를 통한 플러딩 같은 특수한 공격 상황에서 ICMP 패킷의 비율이 늘어나며 다른 패킷 대비 ICMP 패킷의 비율 또한 특성 정보로 활용하였다.

3.3.6. ARP 관련 특성 정보

본 논문에서 분석한 공격 유형 중에 ARP 스푸핑 공격이 있다. ARP 스푸핑 공격의 특성상 ARP 패킷이 발생하고 이 발생된 패킷의 ARP operation 정보를 활용하면 해당 공격을 탐지할 수 있다.

3.3.7. DoS 및 DDoS 공격 관련 특성 정보

사물인터넷 환경에서 미라이 봇넷과 같은 DDoS 공격은 대표적인 공격 유형 이다. DDoS 공격은 출발지

의 주소정보나 도착지의 주소정보를 수정한 패킷을 송신하여 이루어지므로 짧은 시간동안 전달된 패킷의 출발지 및 도착지의 고유한 주소정보의 개수가 많다는 특징이 있다.

3.3.8. SYN 관련 특성 정보

DoS 공격에는 TCP 프로토콜의 플래그 중 SYN이 설정되어 있는 패킷으로 공격하는 SYN 플러딩 공격이 존재한다. DoS 공격의 특성상 SYN 플래그가 설정되어 있는 패킷의 비율이 평소보다 커질 것으로 예측 가능하며 해당 공격을 탐지하기 위해서는 SYN 패킷의 비율과 SYN 패킷과 ACK 패킷의 차이 값을 특성정보로 활용할 수 있다. 정상적인 통신 상황에서는 ACK 패킷의 수가 SYN 패킷보다 많다. 또한 미라이 봇넷에서 흔히 사용하는 유형 중 하나인 ACK 플러딩도 평소보다 ACK 플래그 비율이 늘어나게 되며 이로 인해 활용하는 특성 정보 값에 영향을 줄 수 있다.

Ⅳ. 향후연구계획

4.1. 대응 가능한 위협 및 현재 연구 진행사항

본 논문에서는 총 5개 유형 별 10개 세부 공격 유형을 식별할 수 있으며 다음 [표 2]와 같다. 사물인터넷 환경에서 가장 많이 발견되는 공격 유형을 탐지할 수 있다. 사물인터넷 환경에서의 침입탐지 논문들에서 공통적으로 다루고 있는 공격 유형들을 분석하였고 인공신경망 학습을 위하여 사물인터넷 환경에서의 대표적인 공격 중 실제로 이를 재현할 수 있는 공격을 선정하였다[4-9]. 대표적인 분류로는 Probing, R2L(Remote to Local), U2R(User to Root), Denial of Service(DoS)이며, U2R의 경우 네트워크상에서 확인하기 어려운 공격이기에 제외하였다.

〔표 2〕 탐지 가능 공격 유형(10종)

유형	세부 공격
Reconnaissance	Host Discovery
	Port Scanning
	OS and Service Detection
Man In The Middle	ARP Spoofing Attack
Denial of Service	SYN Flooding Attack
Mirai Botnet - 전파	Host Discovery
	Telnet Bruteforce
Mirai Botnet - 공격	UDP Flooding Attack
	HTTP Flooding Attack
	ACK Flooding Attack

Ⅴ. 결 론

본 논문에서 제안하는 탐지 모델의 구조는 오토인코더의 디코더 부분을 대신하여 소프트맥스 함수를 표현계층에 연결한 구조이며, 비지도 학습 방식의 오토인코더의 결과를 소프트맥스 함수에서 9개 세부 공격으로 탐지한다. 본 논문에서 제안한 탐지 모델의 성능 검증을 위해 총 3번의 실험을 하였으며, 학습 데이터와 검증 데이터의 비율은 9:1, 데이터가 많은 클래스를 랜덤 샘플링 하여 비율을 낮추었다. 결과는 그림 6, 7, 8과 같다. 첫 번째 실험의 경우 오토인코더의 표현층 차원 수를 20으로 설정하였으며, 두 번째 실험의 경우 오토인코더의 표현층 차원 수를 10으로 설정하였으며, 세 번째 실험의 경우 오토인코더의 표현층 차원 수를 5로 설정하였다. 오토인코더와 소프트맥스의 학습률은 0.001로 고정하였다.

단순히 트래픽에 대한 공격 여부만을 아는 것으로는 보안 대책을 수립하는데 한계가 있으며 각 공격 유형별 원인이 상이하기에 이를 공통적으로 탐지하는 것은 원인 파악에 어려움을 줄 수 있다. 각각의 공격 유형이 갖는 특징이나 공격 대상 등이 상이하기 때문에 공격 유형에 대한 정밀한 식별을 수행하고 그에 맞는 피해 경감 방안을 적용하는 것이 필요하다. 탐지 규칙을 세우는 데 있어 각 공격 유형 별로 자세한 탐지 규칙을 설정할 수 있기 때문에 공통적인 특징을 이용한 탐지

Class	Recall	Precision	F1-score	# Test Data
normal	1.00	1.00	1.00	20,000
arp_spoof	0.98	1.00	0.99	54
syn_flood	1.00	1.00	1.00	6,465
host_discovery	0.99	0.99	0.99	313
port_scan	1.00	1.00	1.00	2,094
os_svc_detect	0.97	0.96	0.96	182
udp_flood	1.00	1.00	1.00	20,000
ack_flood	1.00	1.00	1.00	7,563
http_flood	1.00	0.99	1.00	1,047
telnet_bruteforce	0.87	0.84	0.85	192
Macro Average	0.98	0.98	**0.98**	

(그림 6) 모델 실험 결과(1/3)

Class	Recall	Precision	F1-score	# Test Data
normal	1.00	1.00	1.00	20,000
arp_spoof	0.98	1.00	0.99	54
syn_flood	1.00	1.00	1.00	6,465
host_discovery	0.98	1.00	0.99	313
port_scan	1.00	1.00	1.00	2,094
os_svc_detect	0.95	0.92	0.94	182
udp_flood	1.00	1.00	1.00	20,000
ack_flood	1.00	1.00	1.00	7,563
http_flood	1.00	0.99	0.99	1,047
telnet_bruteforce	0.85	0.74	0.79	192
Macro Average	0.97	0.96	**0.97**	

(그림 7) 모델 실험 결과(2/3)

Class	Recall	Precision	F1-score	# Test Data
normal	0.99	1.00	1.00	20,000
arp_spoof	0.98	1.00	0.99	54
syn_flood	1.00	1.00	1.00	6,465
host_discovery	0.97	0.99	0.98	313
port_scan	1.00	1.00	1.00	2,094
os_svc_detect	0.83	0.87	0.85	182
udp_flood	1.00	1.00	1.00	20,000
ack_flood	1.00	1.00	1.00	7,563
http_flood	0.99	0.98	0.98	1,047
telnet_bruteforce	0.83	0.57	0.67	192
Macro Average	0.96	0.94	**0.95**	

(그림 8) 모델 실험 결과(3/3)

에 비해 미탐을 줄일 수 있을 것이다.

참 고 문 헌

[1] M. Tavallaee, E. Bagheri, W. Lu, A. Ghorbani, “A detailed analysis of the KDD CUP 99 data set”, Second IEEE Symposium on Computational Intelligence for Security and Defense Applications, CISDA, 2009.

[2] L. Dhanabal, Dr. S.P. Shantharajah, A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithmss, International Journal of Advanced Reserarch in Computer and Communication Engineering, IJARCCE, 2015

[3] Mirsky, Yisroel, et al. "Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection." Network and Distributed Systems Security (NDSS) Symposium 2018

[4] Restuccia, Francesco, Salvatore D’Oro, and Tommaso Melodia. "Securing the internet of things in the age of machine learning and software-defined networking," IEEE Internet of Things Journal, 5(6), pp. 4829-4842, 2018.

[5] A. John, R. Peter, “Electric Communi- cation Development,” *Communications of the ACM*, 40, pp. 71-79, May 1997.

[6] Midi, Daniele, et al. "Kalis－A system for knowledge-driven adaptable intrusion detection for the Internet of Things." 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS). IEEE, 2017.

[7] Alaba, Fadele Ayotunde, et al. "Internet of Things security: A survey." Journal of Network and Computer Applications 88 (2017): 10-28.

[8] Hodo, Elike, et al. "Threat analysis of IoT networks using artificial neural network intrusion detection system." 2016 International Symposium on Networks, Computers and Communications (ISNCC). IEEE, 2016.

[9] Diro, Abebe Abeshu, and Naveen Chilamkurti. "Distributed attack detection scheme using deep learning approach for Internet of Things." Future Generation Computer Systems 82 (2018): 761-768.

[10] Doshi, Rohan, Noah Apthorpe, and Nick Feamster. "Machine learning ddos detection for consumer internet of things devices." 2018 IEEE Security and Privacy Workshops (SPW). IEEE, 2018.

[11] Nobakht, Mehdi, Vijay Sivaraman, and Roksana Boreli. "A host-based intrusion detection and mitigation framework for smart home IoT using OpenFlow." 2016 11th International conference on availability, reliability and security (ARES). IEEE, 2016.

〈저 자 소 개〉

오 성 택 (Sungtaek Oh)

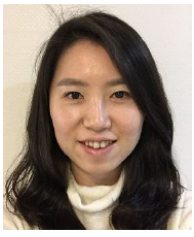
정회원

2013년 2월 : 아주대학교 정보컴퓨터공학부 졸업
2016년 2월 : 아주대학교 컴퓨터공학과 석사
2015년 2월~현재 : 한국인터넷진흥원 보안위협대응R&D팀 선임연구원
<관심분야> 머신러닝, 침입탐지, 정보보호

고 웅 (Woong Go)

정회원

2010년 2월 : 순천향대학교 정보보호학과 석사
2013년 8월 : 순천향대학교 정보보호학과 박사
2014년 1월~현재 : 한국인터넷진흥원 보안위협대응R&D팀 책임연구원
<관심분야> IoT, 기계학습, 정보보호



김 미 주 (Mijoo Kim)

정회원

2006년 2월 : 순천향대학교 정보보호학과 졸업
2008년 2월 : 순천향대학교 정보보호학과 석사
2008년 9월~현재 : 순천향대학교 정보보호학과 박사과정
2008년 4월~현재 : 한국인터넷진흥원 책임연구원
<관심분야> 정보보호, IoT 및 모바일 보안, 융합보안

이 재 혁 (Jaehyuk Lee)

학생회원

2014년 2월 : 학점은행제 정보보호학사
2018년 2월 : 고려대학교 정보보호석사
2017년 4월~현재 : 한국인터넷진흥원 보안위협대응R&D팀 주임연구원
<관심분야> 빅데이터, AI, 정보보호

김 홍 근 (Kim Hong-Geun)

종신회원

1985년 2월 : 서울대학교 전자계산기공학과 졸업
1987년 2월 : 서울대학교 전자계산기공학과 석사
1994년 2월 : 서울대학교 컴퓨터공학과 박사
1994년 5월~현재 : 한국인터넷진흥원 연구위원
<관심분야> 병렬알고리즘, 사이버보안, 컴퓨터보안

박 순 태 (SoonTai Park)

정회원

1992년 2월 : 단국대학교 전자계산학과 졸업
1998년 8월 : 국민대학교 정보과학대학원 정보통신학과 석사
2010년 8월 : 전남대학교 대학원 정보보안협동과정 박사
2000년 4월~현재 : 한국인터넷진흥원 팀장
<관심분야> IT보안성 평가, 정보보호 인력 양성, 정보통신기반보호, 조직 정보보안/개인정보보호 실무, 정보보호 R&D