https://doi.org/10.33778/kcsa.2019.19.4.077

사이버 방어체계를 우회하는 익명통신의 지능형 탐지모델개발을 위한 개념연구

정 의 섭*, 김 재 현**, 정 찬 기***

요 약

인터넷은 지속적으로 발전하고 이에 따라 사이버 공격도 더욱 정밀하고 은밀하게 이루어지고 있다. 개인의 사생활 보장의 목적으로 사용되는 익명통신도 사이버 공격에 활용되고 있다. 익명통신은 공격자의 IP주소를 숨길 뿐만 아니라 암호화된 트래픽으로 통신이 이루어져 대부분의 기관이나 조직에서 사이버 공격의 방어목적으로 사용하고 있는 정보보호시스템을 우회할 수 있다. 이런 이유로 익명통신은 악성코드의 공격명령을 내리거나, 추가적인 악성코드 다운로드의 통신수단 등으로 활용된다. 그러므로 본 연구는 암호화된 익명통신을 인공지능을 통해 빠른 시간 내에 최대한 정확히 탐지하고 차단하는 방안을 제시하고자 한다. 나아가 이를 국방에 적용하여 악의적인 통신을 탐지하여 중요자료의 외부유출 및 사이버공격 방지에 기여하고자 한다.

A Conceptual Study on the Development of Intelligent Detection Model for the anonymous Communication bypassing the Cyber Defense System

Jung Ui Seob*, Kim Jae Hyun**, Jeong Chan Ki***

ABSTRACT

As the Internet continues to evolve, cyber attacks are becoming more precise and covert. Anonymous communication, which is used to protect personal privacy, is also being used for cyber attacks. Not only it hides the attacker's IP address but also encrypts traffic, which allows users to bypass the information protection system that most organizations and insti tutions are using to defend cyber attacks. For this reason, anonymous communication can be used as a means of attacking malicious code or for downloading additional malware. Therefore, this study aims to suggest a method to detect and block encrypted anonymous communication as quickly as possible through artificial intelligence. Furthermore, it will be applied to the defense to detect malicious communication and contribute to preventing the leakage of important data and cyber attacks.

Key words : Military, Anonymous Communication, Artificial intelligence

접수일(2019년 10월 1일), 게재확정일(2019년 10월 28일)

* 아주대학교/NCW학과
** 아주대학교/NCW학과
*** 아주대학교/NCW학과

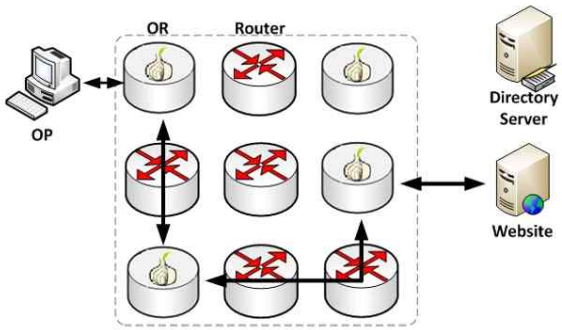
1. 서 론

2017년 인터넷을 사용하는 대한민국의 사용자는 4528만 명에 이르며 이는 만3세 이상 국민 5,017만 명 중 90.3%를 차지하는 숫자이다[2]. 글로벌 인터넷 사용자는 2017년 기준 340억 명(세계 인구 45%)이며 하루에 오가는 글로벌 월별 IP트래픽은 2017년 4.6EB에서 2022년 11.3EB로 약 2.5배 증가할 것으로 예측됐다[3]. 이처럼 네트워크를 통해 이동하는 데이터는 기하급수적으로 증가하고 있으며 이중 많은 데이터들이 암호화되어 전송되고 있으며 익명성을 띄고 있는 데이터의 경우에는 해당 데이터의 출발지조차 확인이 어렵다. 이렇게 암호화된 네트워크 트래픽의 경우에는 복호화 키를 가지고 있지 않은 이상 네트워크에 설치하여 운용중인 정보보호시스템의 경우에도 탐지 및 차단이 어려운 실정이다. 실제 사례로 몇 년 전 이슈가 되었던 NSA 스노든 사건의 경우 Tor(The onion router)와 같은 익명 네트워크를 이용하여 내부의 중요자료를 외부로 유출시켰으며, 국내의 경우 6.25 DDos 사이버테러에 사용되었던 악성코드의 경우에도 악의적인 행위를 숨기기 위하여 익명통신인 Tor를 사용하였다.[1] 이에 본 논문에서는 다양한 사이버 테러의 공격 유형중에서도 익명통신의 도구로 가장 많이 활용되고 있는 Tor에 관하여 분석하고 이를 이용한 익명통신의 효과적인 탐지 및 차단방안에 대하여 논하고자 한다.

2. 익명통신 네트워크 구조와 동작과정

2.1 익명통신(Tor) 네트워크의 구조

Tor는 처음 미국의 해군연구소에서 통신의 내용을 다른 사용자가 알기를 원치 않았던 미국정부에 의해 개발을 시작하였고 현재는 EFF(Electronic Frontier Foundation) 프로젝트에서 관리되고 있다. Tor는 사실 인터넷을 사용하는 조직과 개인이 사생활을 침해하지 않으면서 이용할 수 있도록 만들어진 네트워크이다. 강력한 정부검열을 수행하는 중국, 러시아, 아랍 에미리트, 인도 등의 나라들은 해당 국가의 인터넷 사용자를 트래픽 분석이라고 하는 일반적인 인터넷 탐지 기술로 조사를 하는데 Tor를 통하여 통신할 경우 이러한 검열 수단 등을 우회할 수 있다. Tor의 구성요소는 Cell, Circuit, OP(Onion Proxy), OR(Onion Router), DS(Directory Server)이다. 첫 번째, Cell은 Tor 네트워크를 통과하는 512Byte의 고정된 크기의 패킷을 의미하고, 두 번째, Circuit은 각 TCP Stream에 대한 전체 라우팅경로를 의미한다. 세 번째, OP는 Tor 네트워크를 사용하는 실제 사용자를 나타낸다. 네 번째, OR은 Tor네트워크에서 Tor네트워크를 위해 자신의 PC를 다른 Tor네트워크 사용자가 경유에서 가는 중계구간 역할을 해주는 사용자를 의미한다. 마지막으로 DS는 전 세계에 흩어져있는 모든 OR의 정보들은 수집하고 관리하며, 그 정보들을 OP와 OR들에게 배포하는 역할을 수행한다.



(그림 1) Tor 구성요소[4]

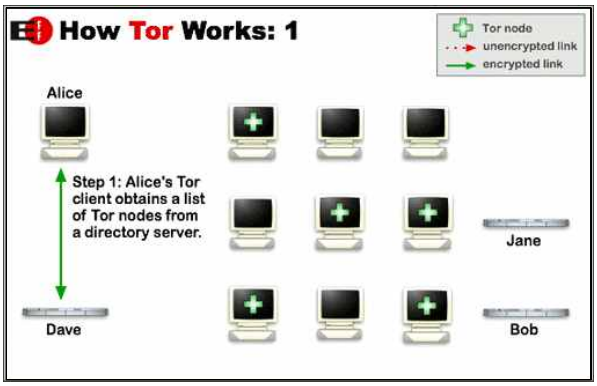
Tor 네트워크 사용자가 웹사이트에 접속할 경우 디렉터리 서버로부터 전 세계의 OR들의 정보를 읽어드린다. 이중 3개의 OR을 선택하여 통신할 수 있는 서킷을 생성하게 된다. 생성된 서킷은 TLS(Transport Layer Security)로 암호화되며, 이 암호화 Key의 길이는 48Byte로 되어있다. 또한 OR과 OR간에도 각각의 Session Key를 통해서 암호화하므로 중간 OR에서 데이터를 가로챈다고 하여도 복호화 할 수 없으므로 어떠한 정보도 알아낼 수 없다. 사용자가 보낸 요청은 마지막 OR이 받아서 최종목적지에 요청하게 되므로 최종

목적지인 웹사이트는 실제사용자가 마지막 OR인 것으로 알게 된다. 이를 통해 실제 사용자인 OP는 자신의 실제 출발지를 숨김으로써 익명성을 보장받게 된다.

2.2 익명통신(Tor) 네트워크의 동작과정

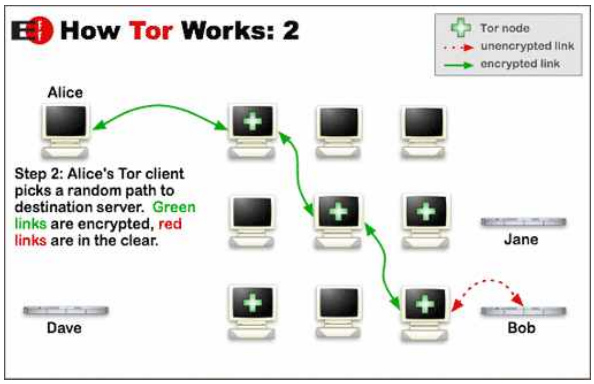
Tor의 동작과정은 초기화단계, 서킷생성단계, 데이터 전송단계로 구분할 수 있다.

첫 번째, 초기화 단계는 사용자가 Tor를 실행할 때 DS로부터 모든 OR들의 정보를 받아오는 것을 말한다. 각 OR들의 IP, PORT, VERSION 등이 이 정보에 해당되며, 총 OR개수의 25%이상의 정보를 보유할 때까지 받아오게 된다.[4]



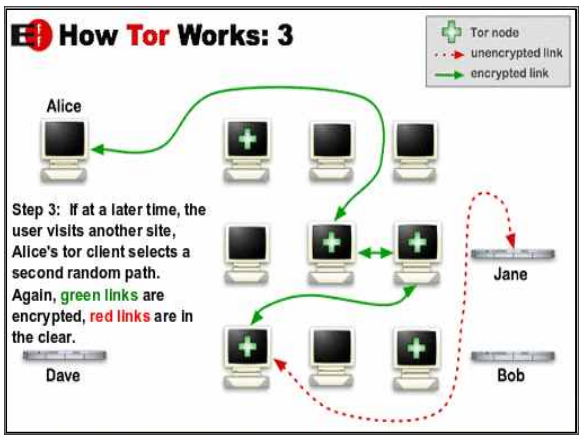
(그림 2) Tor 네트워크의 동작과정 1단계[9]

두 번째, 서킷생성단계, 서킷은 Internal서킷과 Exit 서킷 두 가지가 있다. Internal 서킷은 디렉터리 서버 등 Tor 네트워크를 이용할 때 필요한 정보를 주고받을 때 사용하는 서킷이며 실제 사용자가 주고받은 데이터는 Exit 서킷을 통해 이루어지며, 해당 서킷들은 Tor를 시작하면 미리 최대 12개까지 생성하여 용도에 맞게 이용되게 된다. 서킷생성은 Tor 네트워크에서 데이터의 익명성을 보장하는 가장 중요한 단계이다.



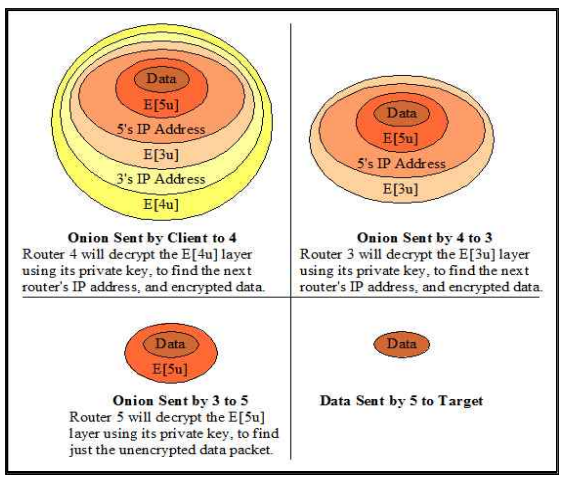
(그림 3) Tor 네트워크의 동작과정 2단계[9]

마지막으로 생성된 서킷을 이용하여 데이터를 주고받는 데이터 전송단계이다.



(그림 4) Tor 네트워크의 동작과정 3단계[9]

이때 전송되는 데이터는 OR간의 겹층 암호화(그림 5)를 통하여 안전하게 전달되어 진다.



(그림 5) 겹층 암호화 동작원리[10]

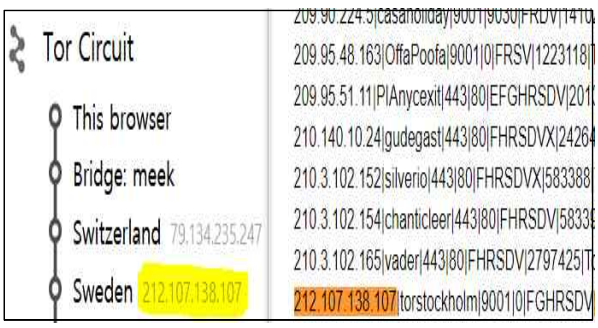
<표 1> Tor nodes[5]

IP	name	router-port	directory-port	flags	uptime	version
1.33.3.146	fwioetwg4utghw4ignc	443	80	FRDV	194523	Tor 0.3.5.7
103.194.170.223	thealgorithm	9001	80	EFGHRSDV	2152664	Tor 0.3.5.8
1.65.177.99	DKRelay	9001	9030	FHRSDV	518458	Tor 0.3.5.8
100.11.96.205	minotor	9001	9030	RSDV	6070489	Tor 0.3.4.9
100.14.173.231	throughhere	9001	9030	FGHRSDV	1548316	Tor 0.3.5.8
...	...	...	...	...	...	...

3. 기존의 익명통신탐지 및 차단방안

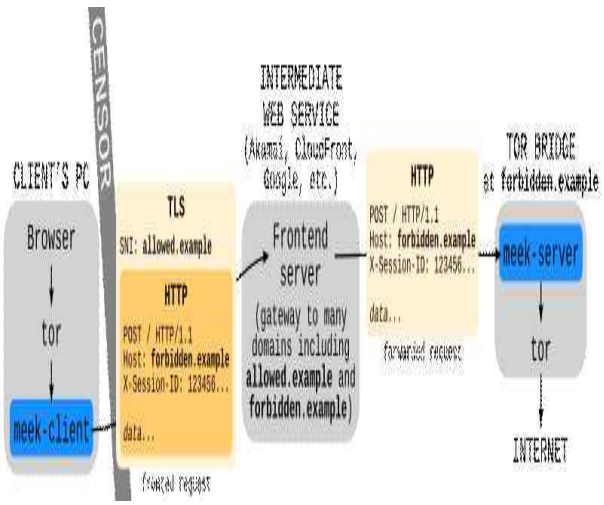
3.1 Tor에 활용되는 node IP차단

앞서 설명한 것처럼 Tor 사용자는 Tor 브라우저를 실행하게 되면 Tor 통신을 위한 서킷생성을 위한 Tor에 사용되는 node정보를 디렉터리 서버로부터 받아오게 된다. 이때 사용하는 node정보들은 랜덤하게 갱신되도록 구성되어 있으며 이에 해당하는 node정보를 IP주소 기반으로 차단할 수 있는 정보보호체계에 적용하면 기본적인 Tor통신을 차단할 수 있다.[8] 세부적으로 설명하면 첫 번째, 주기적으로 Tor node의 IP주소 정보를 데이터화하여 갱신한다. 두 번째, 데이터화된 Tor node IP 주소 정보를 방화벽에 Tor그룹으로 생성하여 이를 차단 적용한다. 세 번째, 주기적으로 해당정책의 Log 확인을 통해 내부에서 익명통신을 사용 시도하는 단말기를 확인하고 식별하여 차단조치하고 악성코드감염 등의 통신을 시도하는 경위를 분석하고 조치한다. node정보는 https://www.dan.me.uk/tornodes를 통해 쉽게 획득할 수 있다.



(그림 6) Tor node와 실제 서킷에 활용된 IP

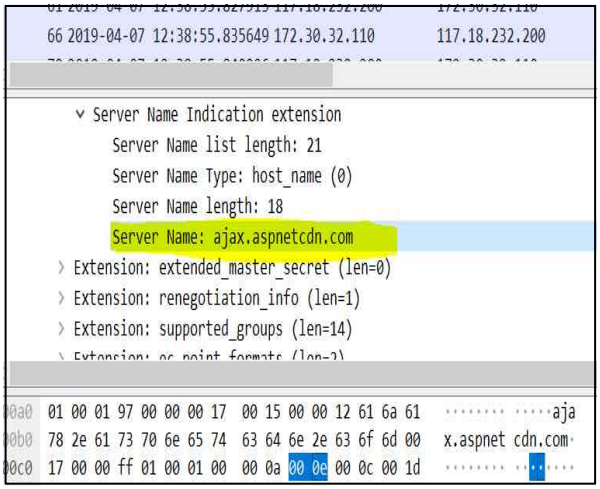
2019년 9월 21일 13시30분 기준으로 총 7434개의 노드가 검색되어 진다.[5] 이중 Exit node만 선별하여 차단할 경우 Flag에 E와 X가 포함된 IP들만 선택해서 차단하면 가능하며, 필요 시 모든 Node들의 IP를 Blacklist로 관리하여 방화벽과 같은 침입차단장비를 활용하여 차단한다면 효과적으로 Tor통신을 차단할 수 있다. 하지만 이방법의 경우 Meek이나 Obfs4와 같은 Pluggable Transports를 사용할 경우 우회가 가능하다. Meek은 http를 사용하고 난독화를 위해 TLS를 사용하는 전송방식으로 트래픽을 타사서버를 통해 릴레이하게 된다. 이렇게 되면 탐지하고자 하는 입장에서는 정상적인 서버와 통신하는 것처럼 보인다.



(그림 7) meek의 동작방식[9]

3.2 DPI를 활용한 Tor 통신 탐지

앞서 설명한 Tor node의 차단에 대해서 IP와 Port기반으로 작동하는 L3계층의 방화벽을 통해서 대응하였다면 DPI(Deep Packet Inspection)기술은 네트워크를 OSI 7 LAYER로 보았을 때 Network계층에서 Application계층까지를 모두 검사하는 기술이다. 즉, 패킷의 출발지와 목적지의 IP와 Port만 검사하는 것이 아니라 해당 패킷의 Header와 Payload의 내부정보까지도 암호화가 되어있지 않다면 검사가 가능하다는 것을 의미한다. 그렇기 때문에 Tor를 사용하는 사용자의 단말기에서 통신 연결 초기부터 발생하는 트래픽에서 특정한 Signature를 추출해 낼 수 있다면 해당 Signature를 DPI기술을 사용하는 IPS(Intrusion Protection System)나 , IDS(Intrusion Detection System)에 등록하여 실시간으로 오가는 패킷을 검사하여 Tor통신을 사용하는 사용자를 탐지해 낼 수 있다.



(그림 8) Tor 통신에 사용된 도메인 이름

이와 같은 방법을 통하여 앞서 방화벽으로 차단하는 방법을 사용할 때 주기적인 Tor node의 갱신과 방화벽의 적용하는 기술의 우회나 갱신되는 시간사이의 이루어지는 Tor통신을 탐지 및 차단할 수 있다. 하지만 DPI를 사용하는 기술은 통신의 내용을 모두 검사하고 통신을 진행시키게 되어 통신의 지연은 어쩔 수 없이 일부 발생 할 수 있으며 도메인과 같은 정보를 이용할 경우 해당 도메인을 정상적으로 이용하는 서비스 사용자에게 피해가 발생 할 수도 있다. 그러므로 기본적으로는 방화벽을 활용하여 대다수의 Tor node를 차단하고 이를 통과하고 우회되는 패킷들에 대해서 DPI를 활용한 방법을 적용한다면 효율적인 차단이 가능할 것이다. 또한 군(軍)이나 정부기관과 같이 보안이 중요시 되는 경우에는 사용자의 서비스 불편보다는 보안이 중요시 되므로 관리자의 판단에 따라 적극적인 차단이 가능하다.

3.3 머신러닝을 활용한 Tor 통신 탐지

최근에는 머신러닝을 활용한 익명통신탐지에 대한 연구도 활발하다. Tom M.mitchell은 머신러닝을 'A computer program is said to learn from experience E with respect to some class of tasks T and performance measure P, if its performance at tasks in T, as measured by P, improves with experience E' [7]라고 정의하였다. 즉, 특정작업 T에 대해 지속적인 경험E를 통해서 작업T에 대한 성능P를 높이는 것을 말한다. 머신러닝을 통한 익명통신 탐지는 탐지하고자 하는 익명통신 트래픽의 Feature를 추출하여 추출된 Feature를 수치로 입력하여 데이터를 다양한 알고리즘을 활용해 학습시켜 Tor뿐만 아니라 I2P, JonDonym과 같은 다양한 익명통신 트래픽에 대해서 Naive Bayes, Bayesian Network, C4.5, Random Forest의 분류알고리즘을 통해 분류가 가능한 것을 증명하였다.[6] 하지만 머신러닝의 경우 데이터의 feature를 해결하고자하는 문제영역의 전문가를 통해 수동으로 식별하여 머신러닝 모델에 입력과 출력으로 제공 하여 학습시켜야 한다는 단점이 있다.

4. 하이브리드 방식의 인공지능을 활용한 익명통신 탐지모델

4.1 머신러닝과 딥러닝의 비교

머신러닝과 딥러닝의 가장 큰 차이점은 데이터의 입력과 출력이 나오는 과정에서 딥러닝의 경우에는 전문가가 수동으로 처리해야하는 Feature extraction 과정이 생략된 것이다. 즉 사람이 데이터

를 처리하여 결과에 중요한 영향을 미치는 특성들을 추출해 주었어야 하는데 딥러닝의 경우에는 가지고 있는 데이터를 모두 넣어주면 딥러닝 시스템이 알아서 중요한 특성을 추출하고 문제를 해결하는 방식이다. 딥러닝의 복잡한 정보의 계산처리를 위해 고성능의 GPU가 필수적으로 필요하며, 모델의 높은 정확성을 위해 많은 데이터가 필요하다.

<표 2> 머신러닝과 딥러닝의 비교

	머신러닝	딥러닝
학습 데이터세트	작다	크다
전문가의 feature 추출	그렇다	아니다
학습 시간	짧다	길다
고성능 GPU 필요성	아니다	그렇다

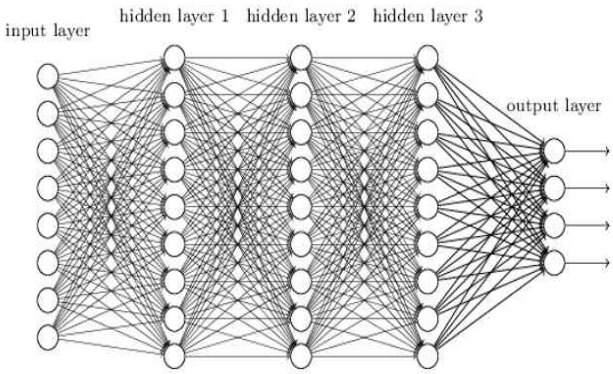
4.2 하이브리드 방식의 익명통신 탐지모델

앞서 설명했듯이 다수의 조직이나 기관은 지역적으로 떨어져있는 지사와 중앙에서 정보를 가공처리하는 본사(중앙기관)를 운영하는 형태로 운영되고 있다. 즉, 지역별로 별도의 LAN을 구성하고 WAN구간을 통해 본사의 서버와 통신하는 형태의 네트워크를 구성하고 있다. 군(軍)의 경우에도 별도의 부대별로 별도의 LAN영역을 구성하고 중앙에 집중되어 있는 정보자원에 접근하게 된다. 정보보호시스템의 구성에서도 마찬가지의 구성을 가지고 있다. 지역별로 지역네트워크를 보호하기 위한 방화벽 및 IPS, IDS등의 정보보호체계를 운영하고 있으며. 중앙의 경우에는 보호해야할 자산의 중요도와 데이터의 양이 많기 때문에 그에 적합하게 더 다양하고 많은 SIEM이나 WFW과 같은 정보보호시스템을 운영하고 있다. 고도의 기능을 가진 정보보호체계의 경우 고비용이 발생할 수밖에 없는 것이 현실이다. 만약 모든 지역에 동등한 수준의 정보보호시스템을 유지하고 운영하려면 그 시스템을 운영하기 위한 인력과 예산이 증가할 것이며 이것은 조직에 부담으로 작용한다. 이에 본 논문에서는 딥러닝과 머신러닝의 장점을 조합한 하이브리드 방식의 익명통신 탐지모델을 제안한다. 고성능의 하드웨어와 지역의 정보보호시스템이나 에이전트들이 전송하는 각종 로그가 모두 모이는 중앙에서 빅데이터와 고성능의 하드웨어를 활용해 딥러닝시스템을 구축하고 해당 딥러닝 시스템을 통해 학습한 후 해당모델에서 특성을 추출한다. 그 후 지역에는 상대적으로 저 사양으로 학습이 가능한 머신러닝 모델을 배치하고 중앙에서 식별된 중요 특성을 지역의 머신러닝 모델에 입력하여 빠른 시간에 탐지하고자 하는 통신을 탐지할 수 있도록 하는 것이다. 이렇게 하면 중앙의 고성능 딥러닝 시스템을 통해 빠르게 익명통신의 특징과 행위를 추출한 후 지역에 적용하여 빠른 사이버 위협에 대응 할 수 있다.

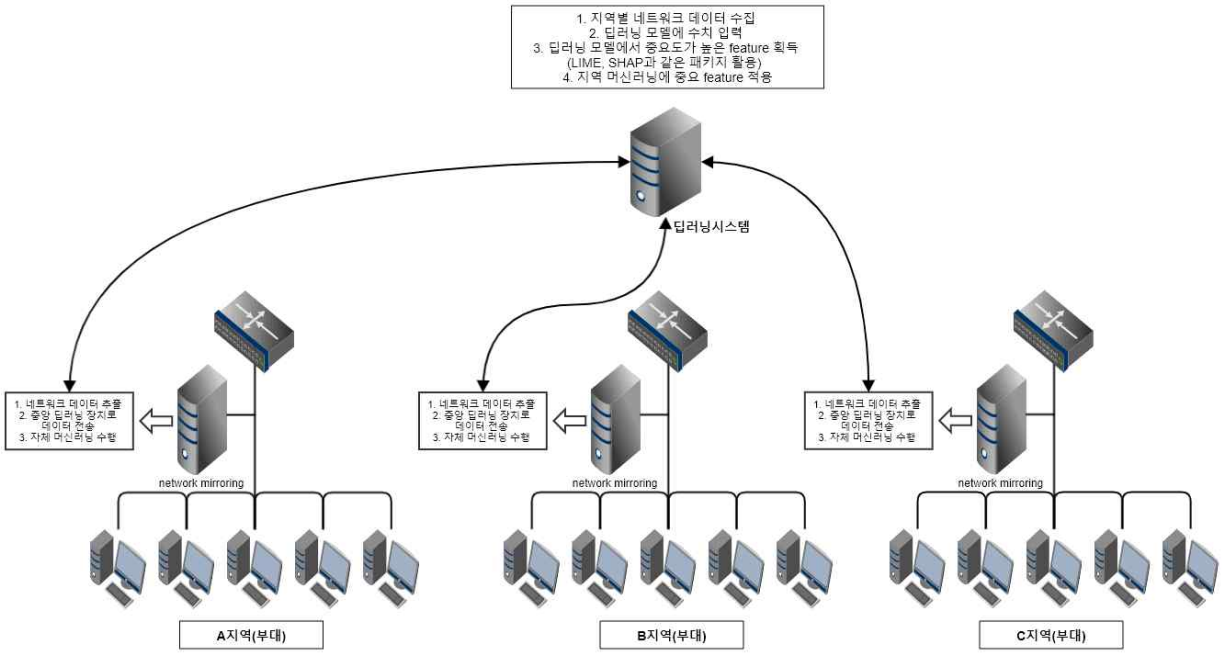
제안 모델을 이용하는 방식을 적용한 방안은 (그림 10)과 같으며 아래와 같은 절차로 진행된다.

1 각 지역의 트래픽의 정보를 추출하여 중앙으로 전송한다.

2 중앙의 딥러닝 시스템은 수집된 트래픽의 정보를 입력으로 하여 목표로 하는 익명통신 탐지의 적합한 모델을 생성한다.



(그림 9) 심층 신경망 모형



(그림 10) 제안하는 익명통신 지능형 탐지모델 개념

3 생성된 딥러닝 모델에서 해당모델이 익명통신을 탐지해낸 특성을 추출한다. 현재 알려진 대표적인 방법으로 LIME(Local Interpretable Model-Agnostic Explanation)이나 SHAP (SHapley Additive exPlanations)등이 있다.

4 추출된 특성들은 중요도에 따라 분류하고 학습 영향성이 높은 특성만 머신러닝 모델에 적용하여 빠르고 정확한 익명통신 탐지를 수행한다.

4.3 기존 탐지방법들과의 비교

본 논문에서 제안한 방식을 기존의 방식들과 비교해보면 IP차단 방식이나 DPI방식의 경우에는 정해진 IP나 Signature를 매칭 하여 차단하는 방식이므로 IP가 변경되거나 Signature가 변경되면 탐지가 불가능하다. 또한 머신러닝을 통한 탐지의 경우에도 알려지진 않은 히든브리지를 사용하거나 새로운 Pluggable transport를 사용하는 경우에는 처음부터 다시 label된 데이터를 수집하고 전처리하여 적합한 모델을 만들어야만 새롭게 변경된 통신의 탐지가 가능하다. 하지만 제안한 시스템의 경우에는 탐지요소에 대한 변화가 발생하여도 트래픽의 주요특징을 활용하고 특성을 추출하는 단계를 사람이 아닌 딥러닝 시스템이 대체하기 때문에 딥러닝의 성능에 영향을 받을 뿐 빠르게 대응할 수 있는 장점이 있다. 또한 제안하는 모델은 익명통신 탐지에만 국한되는 것이 아니라 다른 목적의 모델에도 쉽게 적용이 가능하다. 다수의 정보체계 및 단말기, 정보보호시스템에서 발생시키는 다수의 로그와 이벤트들을 종합하여 딥러닝 시스템에 적용할 경우 다양한 행위에 대한 분류가 가능하고 분류모델의 특징을 추출하여 전체 기관의 머신러닝 시스템에 적용하면 원하는 목적에 따라 빠르게 탐지하고 대응이 가능하다. 이러한 제안모델이 최적화된 상태로 적용되어 운용된다면 정보보호를 위해 기존의 사용자 단말기에 설치된 에이전트 방식의 정보보호프로그램들을 대체할 수 범위까지도 확장할 수 있을 것 이다.

<표 4> 제안방식과 기존방식들과의 비교 평가

구분 \ 방안	IP 활용	DPI 활용	Machine Learning 활용	**제안 방식**
차단유형	알려진 IP만 차단가능	Signature 규칙에 등록된 통신만 차단가능	전문가의 특성 추출과정을 통해 식별 후 통신차단가능 (정확도는 모델에 따라 다름)	**특성 추출과정을 딥러닝을 통해 대신하고 머신러닝모델에 빠르게 적용**
유연한 대응	IP변경 시 불가능	Signature 변경 시 불가능	새로운 Pluggable Transport나 히든 브리지 사용 시 불가능	**딥러닝 속도에 따라 대응가능**
보안효과	중	중	중	**상**
다른 목적 (사이버 위협) 으로의 확장성	X	X	△	O

5. 결론 및 향후연구

본 연구를 통해서 세계에서 가장 많은 사용자들이 사용하고 있는 익명통신의 하나인 Tor의 동작원리에 대해서 살펴보았으며 Tor를 탐지하고 차단하기 위해 사용한 방법들에 대해서 알아보았다. 본 논문은 이번 연구를 통해서 인공지능의 한 영역인 머신러닝과 딥러닝을 효율적으로 활용하여 익명통신의 트래픽을 탐지하고 차단하는 모델을 제안하였다. 기존 연구들이 한 가지 방식에 다양한 알고리즘을 활용하여 익명통신의 탐지에 기여하였다면 본 논문은 딥러닝과 머신러닝의 조합을 통하여 고성능의 하드웨어와 빅데이터를 보유한 중앙에 딥러닝을 적용하여 학습을 시키고 해당모델에서 추출한 특성을 지역의 머신러닝모델에 적용하여 고효율의 익명통신 탐지모델을 제안하였다. 향후 연구에서는 익명통신의 탐지 외에도 각종 정보체계 및 정보보호시스템에서 발생되는 로그들을 활용하여 알려지지 않은 사이버위협에 대한 탐지에 대해 연구하고자 한다.

참고문헌

[1] 한국인터넷진흥원, Tor 네트워크의 원리와 관련 악성코드 사례 분석, 2014. 05

[2] 한국인터넷진흥원, 2017년 인터넷이용실태조사, 2018. 03

[3] Cisco 비주얼 네트워킹 인덱스 2017-2022년 전망 및 추세, 2018. 01

[4] 홍성대, Tor 네트워크 분석과 익명성 저해에 관한 연구, 성균관대학교 일반대학원, 2015.

[5] https://www.dan.me.uk/tornodes, 검색일 : 2019. 9. 21.

[6] A. Montieri, D. Ciuonzo, G. Aceto and A. Pescapé, "Anonymity Services Tor, I2P, JonDonym: Classifying in the Dark," 2017 29th International Teletraffic Congress (ITC 29), Genoa, 2017, pp. 81-89.

[7] Mitchell, T. (1997). Machine Learning. McGraw Hill. p. 2. ISBN 978-0-07-042807-2.

[8] 이정현,안관준,박원형,임종인. (2011). 익명네트워크를 이용한 사이버공격에 대한 대응방안 연구. 융합보안논문지, 11(3), 31-37.

[9] https://2019.www.torproject.org

[10] Sangeetha, K & Ravikumar, K. (2013). CONTROL THE TRADEOFF BETWEEN PERFORMANCE AND ANONYMITY THROUGH END-TO-END TUNABLE PATH SELECTION. International Journal of Computer Engineering and Technology 0976-6375. 4. 282-288.

[저자소개]

정 의 섭 (Ui-Seob Jung)
2016년 2월 아주대학교 석사
2017년 3월 ~ 현재
공군 정보체계관리단 정보보호팀 근무
2017년 3월~ 현재
아주대학교 박사과정
email : heaven22@hanmail.net

김 재 현 (Jae-Hyun Kim)
1987년~1996년 한양대학교 전산과 학사 및 석/박사 졸업
1997년~1998년 미국 UCLA 전기전자과 박사 후 연수
1998년~2003년 Bell Labs, NJ, USA, 연구원
2003년~현재
아주대학교 전자공학부 교수
email : jkim@ajou.ac.kr

정 찬 기 (Chan-Ki Jeong)
1986년 공군사관학교 전자공학 학사
1994년 플로리다공대 전산공학 석사
2001년 플로리다공대 전산공학 박사
2017년 3월 ~ 현재
아주대학교 NCW학과 교수
email : ckjung34@gmail.com