정 보 보 호 학 회 지
제 29 권 제3호, 2019. 6

암호통신 기반 사이버공격 탐지를 위한 AI/X-AI 기술연구 동향

이 윤 수*, 김 규 일**, 최 상 수**, 송 중 석***

요 약

인터넷 상에서 개인정보보호 등 안전성 강화를 위해 암호통신이 지속적으로 증가하고 있다. 특히, 해커들도 사이버공격 행위 은닉 및 탐지기법 우회를 목적으로 암호통신을 적극 활용하는 추세이다. 이러한 상황에서, 네트워크 트래픽 상에서 평문형태의 패턴매칭을 통해 사이버공격을 탐지하는 기존의 방법으로는 한계점에 당면한 상황이다. 따라서, 본 논문에서는 암호통신 기반 사이버공격을 효과적으로 탐지하기 위하여 인공지능 및 설명가능 인공지능 기술을 접목하기 위한 연구・개발 동향을 소개한다.

Ⅰ. 서 론

인터넷 기술의 발전에 따른 접근성 및 활용성이 증가하면서 대부분의 단말기가 인터넷에 연결되고 다양한 인터넷 기반 서비스가 개발되면서 현대사회에 필수요소로 자리잡고 있다.

대부분의 정보가 인터넷 환경에 무분별하게 공개되면서 개인정보 등 중요정보에 대한 보호의 필요성이 지속적으로 제기되고 있으며, 이를 해결하기 위한 하나의 방안으로 암호통신이 주목받고 있다.

암호통신은 SSL(Secure Socket Layer), HTTPS(HyperText Transfer Protocol over Secure Socket Layer)와 같은 암호화 프로토콜을 이용하여 인터넷을 통해 전송되는 데이터에 대한 안전성을 확보하는 방법이다. 이에, 국내에서도 지난 2013년부터 개인정보를 취급하는 모든 웹사이트에 개인정보 전송 시 암호화를 의무화하고 있는 상황이다.

이와 대조적으로 사이버공격을 수행하는 해커들은 보안메커니즘 우회를 위한 효과적인 방법으로 암호통신을 활용하고 있는 실정이다. 암호통신을 통해 해커들은 사이버공격 행위를 암호화할 수 있으며, 이를 통해 기존의 네트워크 및 보안장비를 통한 탐지・분석을 효과적으로 우회할 수 있기 때문에 암호통신을 이용한 사이버공격은 지속적으로 증가하고 있다.

이러한 상황에서 사이버공격의 실시간 수집・분석・대응을 전담하는 사이버안전센터들은 네트워크 트래픽 상에서 평문형태의 패턴매칭에 의한 보안관제에만 집중하고 있는 상황으로 암호통신에 대한 효율적인 탐지 및 대응을 위한 기술연구가 시급한 상황이다.

따라서, 본 논문에서는 암호통신 기반 사이버공격을 탐지하기 위해 현재 학계 및 산업계 등에서 추진 중인 다양한 연구들을 소개한다.

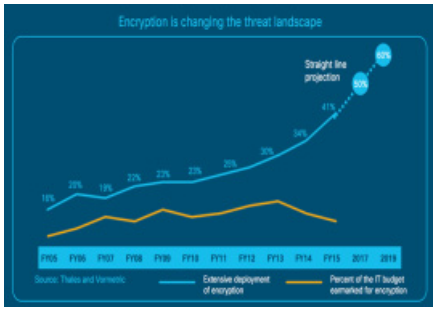
Ⅱ. 암호통신 기반 사이버공격 동향

2.1. 암호통신 트래픽의 폭발적인 증가

인터넷 상에서 개인정보 등 중요정보를 안전하게 보호하기 위하여 그림 1과 같이 암호통신 트래픽이 지속적으로 증가하는 추세이다[1, 2].

구글 서버에 요청된 트래픽의 90% 이상이 암호화되었으며, 가트너그룹은 2019년까지 웹 트래픽의 80%가 암호화될 것으로 추정하고 있다. 또한, 아마존 알렉사(Alexa)에 등록된 글로벌 Top 50 웹사이트 중 95%가

본 연구는 2019년도 한국과학기술정보연구원(KISTI) 주요사업 과제로 수행되었습니다.
* 한국과학기술정보연구원 과학기술사이버안전센터, 고려대학교 대학원 박사과정 (zizeaz@kisti.re.kr)
** 한국과학기술정보연구원 과학기술사이버안전센터 (kisados@kisti.re.kr, choiss@kisti.re.kr)
*** 한국과학기술정보연구원 과학기술사이버안전센터, 과학기술연합대학원대학교 교수, 교신저자 (song@kisti.re.kr)



〔그림 1〕 암호통신 트래픽 증가 추이〔1, 2〕

암호통신을 사용하는 것으로 분석되었다.

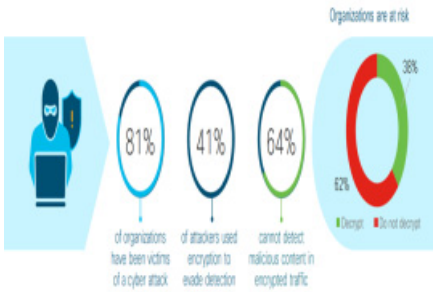
국내의 경우, 정부는 “정보통신망 이용촉진 및 정보보호 등에 관한 법률”에 개인정보 전송 시 암호화를 의무화 하였다(2013년 2월 17일 시행). 특히, 개인정보를 취급하는 모든 웹사이트는 HTTPS, SSL을 반드시 적용해야 하며, 암호화조치 미실시 시 1천만원 이하의 과태료과 부가된다. 따라서, 국내에서도 지속적으로 암호통신이 증가할 것으로 예측되는 상황이다.

2.2. 암호통신 기반 사이버공격 증가

암호통신이 증가하면서 악용사례 역시 급증하고 있는 실정이다. 해커들은 사이버공격 행위를 은닉하고 탐지기법을 우회하기 위한 수단으로 암호통신을 활용하는 것으로 보인다.

특히, 그림 2와 같이 공격자의 41%가 탐지기술을 회피하기 위하여 암호화를 사용하고 있으며, 암호 트래픽의 악성 컨텐츠 중 64%를 탐지하지 못하고 있는 것으로 분석되고 있다[3].

또한, HTTPS 등을 활용한 불법 성인컨텐츠, 악성코드 유포, 내부정보 유출 등 보안위협이 성행하고 있는



〔그림 2〕 암호통신 기반 사이버공격 현황〔3, 4〕

것으로 나타나고 있으며, 주요 원인은 기존 네트워크 및 보안장비가 암호화 트래픽 분석이 불가능하기 때문인 것으로 보인다[4].

2.3. 국내 보안관제센터의 한계점

국내에서는 국가·공공기관의 정보통신망에 대한 사이버공격을 실시간으로 탐지·분석하여 즉각 대응조치를 할 수 있도록, 총 35개의 부문보안관제센터를 운영하고 있다[5].

국내 부문보안관제센터 중 하나인 과학기술사이버안전센터(S&T-CSC)는 지난 2005년부터 과학기술 분야 연구·공공기관 61개에 대한 보안관제 및 침해대응 업무를 전담하고 있으며, 본 논문에서는 과학기술사이버안전센터를 통해 수집·분석 및 대응되는 통계를 중심으로 설명한다.

표 1과 같이 과학기술사이버안전센터에서는 최근 7년간 약 400억건 이상의 사이버 위협정보를 수집하여 총 12,428건의 침해대응 기술지원을 수행하였다.

주목할 만한 점은 2015년을 기준으로 사이버공격과 관련된 보안이벤트 수집 및 침해대응 기술지원이 크게 하향세를 보이고 있는 것이다.

자체적인 분석 결과, 국가·공공기관 웹사이트의 암호화 미조치를 언론에서 문제제기한 2015년 전후로 국내 웹사이트에 대한 HTTPS 및 SSL 적용이 급증하였기 때문인 것으로 판단하고 있다.

국내 보안관제센터는 네트워크 트래픽 상에서 평문 형태의 패턴매칭에 의한 사이버공격 탐지기법에 주로 의존하고 있기 때문에 이러한 현상이 공통적으로 발생되고 있는 것으로 보인다.

〔표 1〕 최근 7년간 보안이벤트 수집 및 침해대응 현황

구분	보안이벤트	침해대응
2012년	1,165,780,019	2,093
2013년	4,457,431,724	2,611
2014년	7,669,366,325	2,329
2015년	9,299,910,213	2,423
2016년	5,142,182,012	1,671
2017년	6,782,338,158	863
2018년	5,826,722,829	438
계	40,343,731,280	12,428

네트워크 기반 침입탐지시스템 운용 이외에도 다양한 형태의 사이버위협정보 수집·분석을 병행하고는 있지만, 암호통신 트래픽의 폭발적인 증가에 따라 차세대 사이버공격 탐지·분석 기술연구가 시급한 상황으로 분석된다.

Ⅲ. 암호통신 사이버공격 탐지기술 연구동향

본 장에서는 급증하는 암호통신 트래픽에서 사이버공격 정보를 수집·탐지하기 위한 다양한 연구·개발 동향을 소개한다.

특히, 본 논문에서는 관련 연구들을 암호통신 보안관제 기술과 인공지능(AI : Artificial Intelligence) 기반 정보보호 기술로 분류하여 제시하였으며, 사이버안전 분야의 특성 상 사이버공격 판단근거 및 원인규명, 재발방지대책 등을 위해 AI 기반 사이버공격 탐지기술에서 필수적으로 고려되어야 한다고 판단되는 설명가능 인공지능(X-AI : eXplainable AI) 기술을 추가적으로 분류하여 소개한다.

3.1. 암호통신 보안관제 기술

현재 암호통신 트래픽에서 사이버공격을 탐지하기 위한 다양한 연구들이 진행되고 있으나, 대부분 암호화 트래픽에서 통계정보를 기반으로 악성코드를 탐지하는 기술 및 솔루션 개발이 주를 이루고 있다.

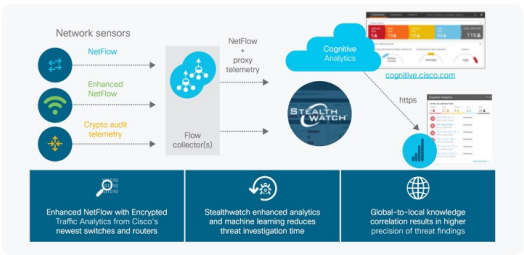
첫 번째 유형은, SSL 프록시 서버를 이용하여 암호화된 트래픽을 복호화한 후 오용탐지 방식으로 악성행위를 탐지하는 방식이다.

대표적인 사례로는 소만사의 암호화웹(HTTPS) 프록시, 모니터랩의 AISVA, 블루엔텍의 F5 WAF, 스텝소프트의 ePrism SSL 등이 있다[6, 7, 8, 9].

그러나, 이러한 접근방법은 암호통신 내용에 대한 복호화를 위한 사용자 동의가 선행되어야 하며 필연적으로 프라이버시 침해 문제가 발생될 수 있다.

두 번째 유형은, 암호화된 트래픽의 특성을 분석한 후 이상탐지 방식으로 악성행위를 탐지하는 방식이다.

대표적인 사례로는 시스코의 ETA(Encrypted Traffic Analytics)로써 그림 3과 같이 네트워크 트래픽 상에서 각각의 어플리케이션이 갖는 고유한 특성(패킷 크기, 방향, 패킷 도착 시간간격 등)을 분석하는 방식을



〔그림 3〕 시스코 ETA 개념도〔10, 11〕

이용하고 있다[10, 11].

그러나, IP 플로우 기반의 통계정보에 주로 의존하고 있으며, 특정 유형의 악성코드 탐지에만 적용이 가능하다는 한계점이 존재한다.

3.2. 인공지능 기반 정보보호 기술

4차 산업혁명 시대의 핵심기술인 인공지능과 블록체인 등에 대한 관심과 기술개발이 지속적으로 증가하고 있는 추세이다.

국내 정부는 AI 기반 정보보호 기술 연구·개발을 적극적으로 장려하고 있으며, AI 기반 사이버 보안위협 대응체계 구축을 핵심 국정과제로 선정하고 과학기술 발전이 선도하는 4차 산업혁명을 위한 역기능 대응방안으로 고려하고 있다[12]. 또한, “2019년도 정부연구개발 투자방향 및 기준(안)”에 사이버 자가방어형 기술개발 지원을 포함하여 기업의 기술수준이 성숙된 수동형 탐지 보안기술 지원은 축소하고 초연결 시대에 대비한 AI 기반의 사이버위협 자동대응 기술 지원을 추진하고 있으며[13], “제1차 정보보호산업진흥계획(K-ICT 시큐리티 2020)”에 관련 분야를 선정하고 AI 기반의 이상행위 탐지기술 연구·보급의 확산 및 지원 계획 등을 주요 항목으로 명시하고 있다[14].

선진 각국에서도 AI 기반 보안기술 연구·개발을 장려하기 위한 다양한 정책들을 발표하고 있는 상황이다. 미국은 “Preparing for the future of artificial intelligence” 보고서를 발표하고, 사이버보안 관련 유관기관들이 효율적인 연구·개발을 위해 정부·민간 부문의 AI 전문가들과 교류해야 한다는 점을 강조하고 있다[15]. 일본은 “인공지능 기술전략회의”에서 AI 산업화 로드맵을 발표하고, 일본의 경제발전과 초스마트사회 실현을 위한 중점 4개 분야 중 “정보보안”을 선정하였

다[16].

이와 같이 각국 정부의 대폭적인 정책・예산 지원을 기반으로 다양한 정보보안 솔루션에 AI 기술 적용을 시작하는 단계이다.

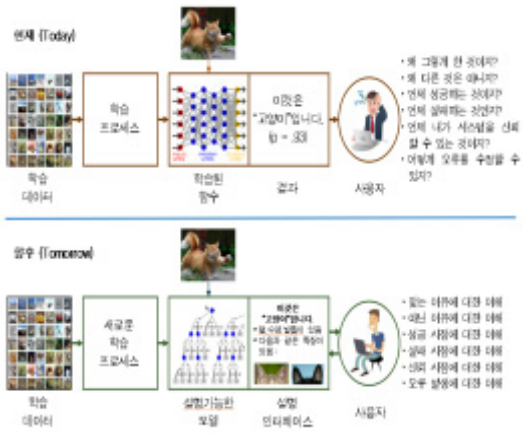
국내의 경우, 2017년 기준 보안관제 시장규모가 전체 정보보호 서비스 시장의 42.5%를 차지하고 있으며 특히, 보안관제 전문기업들은 서비스 차별화와 시장확대를 위해 AI 기술적용을 적극 추진하고 있다. 대표적인 사례로는 에스케이인포섹의 “Secudium”으로 머신러닝 기술을 접목하였고, 시큐아이의 “AI 기반 보안관제”는 인지기반 AI인 IBM Watson을 접목하였으며, 이글루시큐리티의 “D-Security”는 지도학습 AI 알고리즘을 접목하였다[17, 18]. 또한, 정보보안 전문기업들도 AI 기술을 다양한 분야에 적용하여 상용 솔루션 개발을 추진 중이다. 대표적인 사례로는 세인트시큐리티의 “MAX”의 경우 머신러닝 엔진을 장착한 국내 첫 AI 백신임 점을 부각시키고 있으며, 파수닷컴의 “스패로우”는 머신러닝 기술을 적용하여 단순반복작업을 획기적으로 차감한 점을 특징으로 볼 수 있다[19, 20].

해외의 경우, 소규모 신생기업을 중심으로 AI 기반 보안기술을 보유한 업체들이 두각을 나타내고 있다. 대표적인 사례로는 영국의 사이버보안 벤처기업인 “다크트레이스(DarkTrace)”로서 네트워크 상의 비정상행위 및 위협탐지가 가능한 기술을 개발하여 삼성SDS를 포함한 다수의 기업들로부터 기술의 우수성을 인정받아 투자를 받았다. 미국의 신생기업인 “크라우드스트라이크(CrowdStrike)”는 AI 기반 보안위협 대응 솔루션을 보유하여 회사 가치가 수십억 달러에 이루는 것으로 평가되고 있다[21]. 또한, 글로벌 IT 기업들은 AI 기반 사이버보안 스타트업을 인수하여 자사 보안역량과 사업영역 강화를 지속적으로 추진 중이다[22].

3.3. 설명가능 인공지능 기반 정보보호 기술

AI에 대한 연구・개발이 증가되고 다양한 제품과 솔루션이 등장하면서 “왜? 어떻게?”라는 문제에 당면하게 되었다. 이것은 인간 중심의 의사결정에서 AI를 활용한 의사결정으로 전환하기 위해 필연적으로 거쳐야 하는 과정이며, 이 문제를 해소하기 위해 선진국을 중심으로 다양한 논의가 진행 중이다.

유럽연합은 AI의 투명성과 신뢰성 제고를 위한 규제



〔그림 4〕 X-AI에 대한 개념도〔26〕

메커니즘의 필요성을 제기하고 일반정보보호규정(GDPR: General Data Protection Regulation)에 관련 규제조항을 신설하였다. 특히, 정보주체의 정보보호 및 AI에 의한 의사결정의 투명성을 위해 “설명요구권리(Right to Explanation)”를 규정하였으며, 2018년 5월 발효 이후 규정 위반 시 해당 기업의 전 세계 매출의 최대 4%까지 벌금을 부과할 수 있다[23, 24].

미국은 국방성 산하 방위고등연구계획국(DARPA: Defense Advanced Research Projects Agency)을 중심으로 소속 과학자, 산업계 및 학계의 전문가로 팀을 구성하여 X-AI 개발 프로젝트를 추진하고 있으며, 연구주제 및 필요성은 그림 4와 같다. 특히, 2017년부터 2021년까지 약 800억원의 예산을 투입하고 있는 것으로 발표하였다[25, 26, 27].

X-AI 관련 특허출원 현황을 살펴보면 2017년 기준으로 X-AI와 관련된 한국의 특허출원은 33건으로 차세대 인공지능 관련 기술개발 투자는 선진국 대비 매우 저조한 상황으로 나타났다. 반면, 해외에서는 미국과 중국을 중심으로 X-AI를 위한 새로운 네트워크 구조에 관한 특허출원이 중점적으로 이루어지고 있는 상황이다. 주요 유형으로는 네트워크 구조(54%), 해석가능 인터페이스(25%), 시각화(21%) 순으로 나타났으며, 대표적인 기업으로는 마이크로소프트(57건), 구글(18건), IBM(17건) 순으로 나타났다[28].

구글에서는 AI의 각 뉴런이 무엇을 식별하려고 시도하는지에 대한 설명을 제공하기 위하여 X-AI 도구를 개발 중이라고 발표하였다. 특히, 영상인식용 AI의 뉴런들이 사진 상의 사물식별을 위해 어떻게 결합하는지

방법을 제공하는데 초점을 맞추고 있다.

X-AI는 AI의 발전과 맞물려 연구·개발의 필요성이 제기되는 단계로, 현재까지 X-AI와 관련된 상용 솔루션이나 공개된 연구·개발 결과가 전무한 상황이다. 그러나, 사이버공격 탐지에 AI를 적용하기 위해서는 이 분야에 대한 고려가 반드시 요구된다.

Ⅳ. 향후 연구·개발의 방향성 모색

본 장에서는 3장에서 소개한 기술들의 현재 수준을 분석해 보고, 암호통신 기반 사이버공격을 위한 AI 기술 연구·개발 시 필수적으로 고려되어야 하는 사항을 제시한다.

4.1. 현재 기술수준 분석

암호화된 사이버공격 자동탐지를 위해 AI 및 X-AI 기술을 적용하기 위해서는 다양한 사항들이 고려되어야 한다. 본 논문에서는 학습·검증 데이터 확보, 암호화된 사이버공격 자동탐지 정확도, 암호화된 사이버공격 자동탐지 비율, 그리고 X-AI 모델의 효용성 부분으로 구분하여 현재 기술수준을 분석하였다.

첫 번째 분석 영역은 학습 및 검증 데이터 확보 수준이다. AI 알고리즘의 성능을 보장하기 위해서는 학습에 필요한 데이터의 양이 충분히 제공되어야 함은 이미 학술적으로 증명되어진 사실이다[29].

미국 A&T 연구소는 가상환경 기반에서 암호트래픽에 대한 데이터를 수집하는 방식으로 IPsec 740개 플로우와 PPTP 740개 플로우를 학습에 이용하였으며, 13,700개의 플로우를 검증에 이용하였다[29].

미국 시스코의 경우 가상환경 기반에서 악성 데이터와 정상 데이터를 수집하는 방식으로 표 2의 데이터를 학습 및 검증에 이용하였다[10, 11].

그러나, 기존 연구들은 사용된 데이터가 특정 환경에서 수집한 가상데이터이며 학습 및 검증 데이터 전체 건수도 충분하지 않은 것으로 판단된다.

두 번째 분석 영역은 암호화된 사이버공격 자동탐지의 정확도 수준이다. 기존 연구들은 주로 암호화 트래픽의 종류를 구분하는데 초점을 맞추고 있으며 암호화 트래픽의 악성행위 여부를 판단하기 위한 연구는 매우 부족한 상황으로, 대표적인 연구사례를 중심으로 분석된 결과는 표 3과 같다.

시스코의 ETA는 머신러닝과 IP 플로우 데이터를 활용한 네트워크 행위분석을 통해 악성코드에 의해 생성되는 네트워크 트래픽을 탐지하고 있으나, 탐지 정확도는 명확히 제시하지 않고 있다[10, 11].

SSHCure는 IP 플로우 데이터를 활용하여 SSH 서버에 대한 Brute-Force 공격을 탐지하는 방법을 제시하였다. 특히, SSH 기반 네트워크 침입을 탐색 → 시도 → 침입의 3단계로 구분하여 공격을 탐지하여 그 정확도가 100%임을 제시하였다[30].

그러나, 기존 연구들은 악성코드, Brute-Force 등 특정 공격유형을 대상으로만 정확도를 제시하고 있어 사이버공격 전체 유형을 대상으로 확대가 필요한 것으로 판단된다.

〔표 2〕 시스코에서 이용한 학습 및 검증 데이터

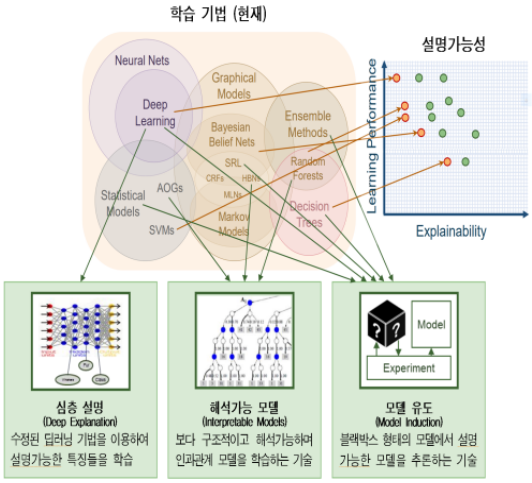
수집 기간	정상	악성
Pre-May	620,072	208,368
May	616,823	15,316
June	596,848	8,832
July	619,859	18,836
August	553,164	13,429
September	545,931	21,114
September	735,195	N/A
Total	4,287,892	285,895

〔표 3〕 암호통신 사이버공격 자동탐지 정확도 비교

구 분	탐지 정확도	특징
ETA	미제시	- 데이터 : IP FLOW - 탐지범위 : 악성코드에 의한 악성 행위
SSHCure	100%	- 데이터 : IP FLOW - 탐지범위 : Brute-Force 공격 탐지

〔표 4〕 암호통신 사이버공격 자동탐지 비율 비교

구 분	탐지 비율	특징
ETA	약 72 ~ 83%	머신러닝 알고리즘 종류에 따라 탐지 비율이 매우 상이함
SSHCure	96.6%	상대적으로 탐지가 용이한 임계치 기반 공격만 탐지 가능



〔그림 5〕 X-AI 연구분야 및 접근방법〔26〕

세 번째 분석 영역은 암호화된 사이버공격 자동탐지 비율이다. 현재 암호화된 사이버공격에 대한 종합적인 탐지가 가능한 모델에 대한 연구는 전무한 상황으로, 위에서 보인 대표 연구사례를 중심으로 분석된 결과는 표 4와 같다.

그러나, 기존 연구들은 특정 공격유형에 제한적이기 때문에 전체 공격유형에 대한 자동탐지가 가능한 AI 모델 개발이 시급한 것으로 판단된다.

네 번째 분석 영역은 X-AI 모델의 효용성 수준이다. 현재까지 X-AI 모델 및 효용성 측면에 대한 연구결과는 전무하며, 방향성에 대한 기초연구만 진행되고 있는 실정이다. 따라서, 여기서는 가장 활발하게 X-AI 분야에 대해 연구를 추진하고 있는 DARPA의 사례를 소개한다.

미국 DARPA에서는 X-AI 연구분야 및 접근방법을 그림 5와 같이 제시하고 있다. 특히, X-AI의 효용성을 측정하기 위한 5개 지표와 13개 세부항목을 제시하였으며, X-AI 시스템이 제공하는 의사결정 과정 및 결과에 대한 명확성·유용성은 실제 사용자(시스템 운영자 및 이용자)만 판단 가능하므로 “사용자 만족도”를 핵심 지표로 설정하고 있다[26, 27].

4.2. 향후 고려사항

현재, 사이버공격 탐지 분야에서 AI를 적용하기 위한 다양한 연구·개발이 진행되고 있지만 앞서 분석한 것처럼 실제 운용환경에서 최적의 성능 및 품질을 보증하기는 어려운 단계라 할 수 있다. 특히, 암호통신 및 X-AI에 대한 고려는 시작 단계에 불과한 상황이다.

향후, 암호통신 기반 사이버공격 탐지를 위한 AI 및 X-AI 연구·개발에 있어서 당면한 문제는 다음과 같이 정리할 수 있다.

첫 번째, 학습 및 검증에 필요한 데이터세트 확보 문제이다. 현재, 사이버공격 탐지 분야에서 AI 적용 시 가장 많이 활용되는 데이터세트는 KDD CUP 99와 Kyoto 2006+로 실험 환경에서 제작되었으며 랜섬웨어, APT 등 최신 사이버공격 유형이 반영되지 않아 그대로 적용하는 것은 현실적으로 어려운 상황이다[31, 32]. 따라서, 사이버공격 탐지를 위한 AI 알고리즘의 성능을 보장하기 위해서는 실제 네트워크 환경에서 암호화된 사이버공격 데이터를 수집·정제하는 방법을 통해 학습 및 검증 데이터를 확보하는 것이 가장 중요하다.

두 번째, 탐지 유형의 확대 문제이다. 기존 연구들은 악성코드, Brute-Force 등 특정 사이버공격 유형을 대상으로 탐지 정확도 및 비율을 제시하고 있으며, 실제 사이버공격을 탐지·분석·대응하기 위해서는 사이버공격 전반(권한 탈취, 감염신호 전송, 악성사이트 접근, 정보 유출, 홈페이지 위변조 등)에 대한 고려가 필요하다. 따라서, 전체 사이버공격 자동탐지를 목표로 하는 AI 모델에 대한 접근이 중요하다.

세 번째, 탐지된 사이버공격의 원인규명 문제이다. AI 모델을 통해 사이버공격을 탐지하였다 하더라고 악성으로 판단한 근거를 제시할 수 없으면 실제 사이버안전 분야에서 활용은 불가능하다. 즉, 사이버공격 판단근거 및 원인규명이 가능해야 침해대응 및 재발방지대책 수립이 가능하므로, 이 문제를 해소하기 위해 X-AI에 대한 고려가 매우 중요하다.

Ⅴ. 결 론

본 논문에서는 암호통신 기반 사이버공격 탐지를 위한 AI 및 X-AI 기술연구 동향을 소개하였다. 특히, 암호통신 트래픽과 암호통신을 이용한 사이버공격이 증가하면서 AI 모델을 적용하기 위한 다양한 연구 및 솔루션들이 소개되고 있으나, 특정 사이버공격 유형에 집중하고 있으며 가상 환경에서 수집된 데이터세트를 주로 사용하고 있다는 한계점을 갖는다. 또한, 사이버안전 분야의 특수성으로 인해 AI 모델의 악성 사이버공격 판단

근거를 제시하기 위한 X-AI에 대한 연구는 전무한 실정이다.

향후, 사이버공격 탐지를 위한 AI 및 X-AI 모델 연구·개발 시 데이터세트 확보, 탐지 유형의 확대 및 원인규명 문제를 해결해야만 실제 사이버안전 분야에서 활용 가능할 것으로 예측된다.

참 고 문 헌

[1] Cisco White Paper, *Encrypted Traffic Analytics*, CISCO, 2009.

[2] S. Radhakrishnan, “Detect threats in encrypted traffic without decryption, using network based security analytics,” CiscoLive!, June 2017.

[3] Cisco, *Cisco 2018 연례 사이버 보안 보고서*, 2018.

[4] SOOSAN INT, *SOOSAN INT Traffic ANalysis Report 2017*, 2018.

[5] 국가정보원, 과학기술정보통신부 등, 2018 국가정보보호백서, 2018년 5월.

[6] 소만사, https://www.somansa.com/.

[7] 모니터랩, http://www.monitorapp.com/kr/.

[8] 블루엔텍, http://www.bluentech.co.kr/.

[9] 스템소프트, http://www.stemsoft.co.kr/.

[10] Anderson, B., & McGrew, D., “Identifying encrypted malware traffic with contextual flow data,” In Proceedings of the 2016 ACM Workshop on Artificial Intelligence and Security, pp. 35-46, 2016.

[11] Anderson, B., & McGrew, D., “Machine learning for encrypted malware traffic classification: accounting for noisy labels and non-stationarity,” In Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 1723-1732, 2017.

[12] 국정기획자문위원회, *문재인정부 국정운영 5개년 계획*, 2017,

[13] 국가과학기술심의회 운영위원회, *2019년도 정부 연구개발 투자방향 및 기준(안)*, 2018.

[14] 관계부처 합동, *제1차 정보보호산업 진흥계획*, 2016.

[15] Executive Office of the President National Science and Technology Council Committee on Technology, *Preparing for the Future of Artificial Intelligence*, 2016.

[16] 정보통신기술진흥센터 해외 ICT R&D 정책동향, *일본의 인공지능(AI) 정책 동향과 실행전략*, 2017.

[17] 보안뉴스, 정보보안 서비스 매출 1위 : 보안관제 3강·3대 키워드, 2018년 7월.

[18] 디지털데일리, 인공지능 보안관제시장 격돌, 2018년 9월.

[19] BylineNetwork, 세인트시큐리티 국내 첫 AI 백신 ‘맥스’ 국내외 공식 출시, 2018년 3월.

[20] 전자신문, [미래기업포커스] 파수닷컴, ‘인텔리전트 플랫폼’ 강화로 SW 경쟁력 갖춘다, 2017년 4월.

[21] 이승민, 송근혜, 정보보호동향 및 보안위협 분석, 2017.

[22] Paul, S., Microsoft confirms it is to acquire Israeli cybersecurity startup Hexadite to bring AI to Windows 10 enterprise security, venturebeat, 2017.

[23] 이원태, EU의 알고리즘 규제 이슈와 정책적 시사점, 2016.

[24] 한국정보화진흥원, EU의 인공지능 新 규제메카니즘: 설명가능 인공지능(XAI), 2018년 3월.

[25] 경향비즈, 결과만 알려주는 AI 넘어…“왜”까지 설명해주는 XAI(설명가능 인공지능) 뜬다, 2018년 2월.

[26] David Gunning, Explainable Artificial Intelligence(XAI), Retrieved August 11, 2016,

[27] 금융보안원, 설명 가능한 인공지능(eXplainable AI, XAI) 소개, 2018년 3월.

[28] 정보통신기술진흥센터, 설명 가능한 AI 기술을 포함한 인공지능의 IP-R&D 전략, 2018년 9월.

[29] Yuichi K., Shingo A., Nobuyuki N., Yoshihiro N., Ikuo O., “Towards real-time processing for application identification of encrypted traffic,” 205(29), pp.136-140, 2014.

[30] Hellemons, L., Hendriks, L., et al., “SSHCure: A Flow-Based SSH Intrusion Detection System,” Lecture notes in computer science,

v.7279, pp.86-97, 2012.
[31] The third international knowledge discovery and data mining tools competition dataset KDD99-Cup, http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html, 1999.
[32] Jungsuk Song, Hiroki Takakura, et al., “Statistical Analysis of Honeypot Data and Building of Kyoto 2006+ Dataset for NIDS Evaluation,”

〈저 자 소 개〉

이 윤 수 (Yunsu Lee)
정회원
2007년 2월 : 전남대학교 산업공학과 (공학사)
2010년 2월 : 충남대학교 대학원 컴퓨터공학과 (공학석사)
2017년 2월～현재 : 고려대학교 대학원 컴퓨터공학과 박사과정
2007년 3월～현재 : 한국과학기술정보연구원 과학기술사이버안전센터 선임기술원
<관심분야> 차세대 보안관제기술 연구・개발, 보안이벤트 실시간 가시화, 정보시스템 취약점 점검・분석

김 규 일 (Kyuil Kim)
정회원
2005년 2월 : 성균관대학교 대학원 컴퓨터공학과 (공학석사)
2010년 2월 : 성균관대학교 대학원 컴퓨터공학과 (공학박사)
2010년 6월～현재 : 한국과학기술정보연구원 과학기술사이버안전센터 선임기술원
<관심분야> 차세대 보안관제기술 연구・개발, 악성코드 분석, AI 기반 대용량 위협데이터 자동분석

최 상 수 (Sangsoo Choi)
정회원
2001년 2월 : 한남대학교 컴퓨터공학과 (공학사)
2003년 2월 : 한남대학교 대학원 컴퓨터공학과 (공학석사)
2006년 2월 : 한남대학교 대학원 컴퓨터공학과 (공학박사)
2006년 3월～현재 : 한국과학기술정보연구원 과학기술사이버안전센터 책임기술원
<관심분야> 차세대 보안관제기술 연구・개발, 사이버공격 실시간 자동탐지, 플로우 기반 침입탐지

송 중 석 (Jungsuk Song)
정회원
2003년 2월 : 한국항공대학교 항공통신정보공학과 (공학사)
2005년 2월 : 한국항공대학교 대학원 정보통신공학과 (공학석사)
2009년 3월 : 교토대학교 대학원 지능정보학 (정보학박사)
2009년 4월～2011년 9월 : 일본정보통신연구원(NICT) 선임연구원
2011년 10월～현재 : 한국과학기술정보연구원(KISTI) 과학기술사이버안전센터 책임연구원
2012년 9월～현재 : 과학기술연합대학원대학교(UST) 데이터 및 HPC 전공 부교수
<관심분야> 네트워크 보안, 차세대 보안관제 기술, 기계학습, 데이터마이닝, 사이버공격 가시화