편집위원 : 이임영 (순천향대학교)

인공지능과 사물인터넷 융합 보안 기술 연구방안

최종석, 박종규, 김호원
부산대학교

요 약

사물인터넷 기술이 발전하면서, 데이터 및 소프트웨어 보안에 대한 이슈가 발생하고 있다. 사물인터넷은 다수의 이기종 디바이스와 플랫폼을 포함하는 환경으로 다양한 공격기술을 시도할 수 있으며, 이러한 공격기술은 급속도로 변화하고 있다. 반면에 보안기술은 이러한 공격기술의 발전속도를 따라가지 못하고 있으며, 특히 개인정보유출의 문제는 아주 큰 이슈가 되었다. 급격하게 발전하는 공격에 대응하기 위해서는 지능형 알고리즘을 이용한 보안기술을 마련할 필요가 있다. 본고에서는 딥러닝 기반의 보안기술 및 사물인터넷 기술 동향을 살펴보고, 이를 토대로 사물인터넷 환경에서 딥러닝 기반의 보안 기술을 적용하기 위한 연구 방안을 제시한다.

Ⅰ. 서 론

사물인터넷(Internet of Things) 기술이 발전하면서, 빅데이터와 보안에 대한 관심이 높아지고 있다. 사물인터넷이란 다수의 이기종 디바이스를 연결하고, 사물인터넷 디바이스로부터 수집된 사물인터넷 빅데이터를 분석하여, 사용자 중심의 서비스를 제공해주기 위한 네트워크를 의미한다.

사물인터넷을 구축하기 위해서 크게 두가지 이슈를 해결하여야 한다. 첫번째로는 다수의 사물인터넷 디바이스를 하나의 망처럼 연결하기 위해서 각각의 디바이스를 위한 통신을 하나의 망에 연결하여야 한다. 이러한 이슈를 사물인터넷의 연결성(connectivity)이라고 한다. 두번째로는 사물인터넷 디바이스로부터 수집된 데이터를 이용하여 사용자가 원하는 서비스를 제공하여야 한다. 다시 말해서 사물인터넷 데이터로부터 사용자의 상황과 의도를 파악해야 한다는 의미이다. 이러한 이슈를 사물인터넷의 지능화(intelligence)라고 한다.

특히 사물인터넷의 지능화를 위해서는 기존의 서비스에서 경시해왔던 개인정보보호에 대한 문제가 더욱 고려되어야만 한다. 사물인터넷의 지능화의 궁극적 목적은 사용자에게 상황과 의도에 맞는 서비스를 제공해주는 것이다. 이를 위해서는 사용자의 상황을 실시간으로 수집을 해야하며, 이러한 정보는 개인정보와 아주 밀접하게 연관될 수 있다.

뿐만 아니라 사물인터넷에서는 디바이스, 통신, 플랫폼, 서비스에 대한 사물인터넷 4계층 관점에서의 보안을 고려하여야 한다. 일반적으로 사물인터넷의 보안은 플랫폼의 특성에 맞게 설계되어야 한다. oneM2M, LWM2M, IoTivity 등의 주요 사물인터넷 플랫폼은 각각 보안을 위한 방법을 기술하고 있다.

대부분의 보안아키텍쳐 및 보안 기술들은 추출 특징의 정당성(correctness)을 검사한다. 이것을 위해서는 선택된 추출 특징이 공격 기법을 판단할 수 있어야 한다. 다시 말해서 추출 특징에 대한 신뢰성 보장이 선행되어야 한다는 의미이다.

일반적으로 추출 특징을 선택하기 위해서, 전문가가 공격을 꾸준히 분석하여 추출 특징을 찾는 연구를 수행한다. 그리고 추출된 특징을 기반으로 방어하기 위한 알고리즘이 설계되어야 하나의 공격에 대한 탐지 기법을 제공할 수 있다.

사물인터넷은 많은 디바이스, 서비스, 사용자가 연합하여 하나의 서비스를 유동적으로 생성하는 네트워크이다. 또한 이러한 다수의 개체들과 자원을 하나의 플랫폼에서 관리한다. 이것은 기존의 서비스나 소프트웨어보다 공격의 형태가 다양해 질 수 있다는 것이다.

사물인터넷 환경에서 지속적으로 발전하는 공격 기술을 빠르게 대응하기 위해서는 사물인터넷의 지능형 프레임워크와 연동하여 사물인터넷 보안 기술을 연구 개발할 필요가 있다.

본고에서는 사물인터넷의 지능형 프레임워크와 사물인터넷 보안 기술의 융합을 위한 연구 방안을 제시한다. 대부분 보안기술에서는 보안아키텍쳐를 독립적으로 분리시켜서 아키텍쳐 단일 보안성을 높이려고 노력하였다. 하지만 사물인터넷 환경에서는 보안아키텍쳐와 지능형 프레임워크가 상호동작을 하여야 한다. 본고에서는 사물인터넷 지능형 프레임워크와 보안아키텍쳐간의 상호동작을 통한 플랫폼 및 게이트웨이 계층에서의 보안기술 연구 방안을 제시한다.

본고의 구성으로 2장에서 딥러닝 기반의 보안기술 동향을 소

개하고, 3장에서는 사물인터넷의 개요 및 주요 보안기술을 소개한다. 그리고 4장에서는 지능형 사물인터넷 보안 기술 연구 방안에 대해서 소개하고, 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 딥러닝 보안기술 동향

1. 악성코드 분석

본 절에서는 딥러닝을 사용하여 악성코드를 분석하는 방법에 대해서 살펴본다. 악성코드는 컴퓨터 사용자에게 피해를 미치는 모든 종류의 소프트웨어를 의미하며, 컴퓨터 바이러스뿐만 아니라 웜, 트로이목마, 스파이웨어 그리고 최근에는 랜섬웨어까지 다양한 종류가 있다.

악성코드 분석 방법으로는 크게 정적분석 방법(Static Analysis)과 동적분석방법(Dynamic Analysis)이 있으며, 정적분석방법은 실행 파일을 역어셈블 하여 분석하는 방법이며 동적분석방법은 소프트웨어를 실행하여 프로세스의 변화를 분석하는 방법이다. 이 중 학습이 필요한 딥러닝 기반의 악성코드 분석은 정적분석방법으로 활용된다.

정적분석방법에서 악성코드를 규명짓는 특징은 Opcode, Header, Byte sequence, API 등 매우 많다. 일반적으로 악성코드를 탐지하기 위해 위에서 열거한 특징들을 이용한 Signature 기반의 탐지기법을 사용한다.

Opcode를 특징으로 하여 악성코드를 분류하는 방법으로는 Opcode sequence와 Opcode frequency를 기반으로 하는 분석 방법 등이 있다. Opcode는 실제로 CPU가 읽고 해석하는 코드로써 MOV, ADD, SUB, CALL 등이 대표적이다. 이러한 Opcode들은 하나의 알고리즘을 위해서 일정한 순서를 가지게 되는데, 일반적으로 연산을 위해 ADD나 SUB의 앞에는 MOV가 먼저 나오는 식이다. 그러나 이러한 Opcode의 순서에는 너무나 많은 경우의 수가 있고, 악성코드 또한 이러한 순서를 당연히 갖고 있으므로 유효하지 않은 경우가 많다. 그리하여 연구된 것은 Opcode frequency 기반의 분석이다[1]. 앞서의 Opcode 들은 각 소프트웨어마다 사용빈도수가 모두 다르다. Daniel Bilar는 임의의 악성코드에서 Opcode의 사용빈도수를 조사하였는데 가장 많이 사용되는 Opcode 5개는 MOV, PUSH, CALL, POP, CMP였다. 또한 사용빈도수가 가장 높았던 Opcode 14개와 사용빈도수가 낮았던 Opcode 14개를 이용해 각종 악성코드들의 연관성을 분석하였다. 이 악성코드와의 연관성을 바탕으로 악성코드를 탐지, 분류하였다.

최근 일상화된 스마트폰 사용 환경과 스마트폰에서 활용되는 개인 정보들의 중요성에 따라 안드로이드 기반의 모바일 환경에서의 악성코드 탐지도 많은 연구가 이루어지고 있다. 대표적으로는 ComDroid, ScanDroid, Andromaly, TaintDroid 등이 있다. 안드로이드 기반의 모바일 환경에서는 SDK(Software Development Kit)로 제작된 특히 어플리케이션 형태의 트로이목마 형태의 악성코드가 많이 발견된다. 위에서 언급한 안드로이드 분석 툴들은 바이트 코드나 IPC(Inter-Process Communication), 퍼미션 타입, 파라미터, 데이터 흐름 등을 주로 분석한다.

그러나 이와 같은 악성코드 분석들은 알려진 유형의 공격방법에 대해서만 유효하며 새로운 유형의 공격에 대해서는 취약한 것이 사실이다. 이에 위의 기법을 기반으로 기계학습을 적용시켜 악성코드를 분류해내는 연구가 많이 이루어지고 있다. 하지만 악성코드를 구분 짓는 무수히 많은 특징들 때문에 일반적인 기계학습으로는 학습을 시키기 어렵거나 탐지율이 저하될 수도 있다.

딥러닝을 사용한 악성코드의 분석으로는 George E. Dahl이 Random Projection과 뉴럴 네트워크를 이용하여 악성코드를 분류하였다[2]. Random Projection은 173,000개에 달하는 특징들을 4,000개로 줄이는 역할을 하며 뉴럴 네트워크는 이를 이용해 일반 악성코드 및 변종 악성코드 등의 136개의 클래스로 분류한다.

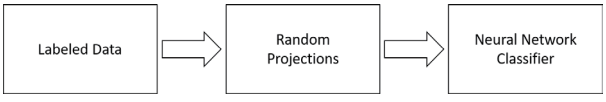

그림 1. Dahl의 악성코드 분류기 구조도

표 1. Dahl의 악성코드 분류 결과

Method	Test Err	Test Two-Class Err	FPR	FNR	Training Time(m)
Logistic Regression All Features	11.70%	0.86%	1.49%	0.60%	187.2
Logistic Regression Random Projection	12.37%	1.27%	2.41%	0.80%	105.7
One-Layer Neural Network w/o Pre-Training	9.53%	0.49%	0.83%	0.35%	167.1
One-Layer Neural Network with Pre-Training	9.76%	0.50%	0.90%	0.34%	287.0
Two-Layer Neural Network w/o Pre-Training	9.55%	0.50%	0.85%	0.35%	244.0
Two-Layer Neural Network with Pre-Training	9.83%	0.54%	0.98%	0.36%	402.3
Three-Layer Neural Network w/o Pre-Training	9.74%	0.51%	0.87%	0.36%	215.0

Dahl의 실험은 의미 있는 분류 결과를 보였는데 〈표 1〉에서 보듯이 선행학습과 레이어의 개수는 결과에 크게 영향을 미치지는 않았다. 테스트 에러는 전체 분류에서 악성코드로 잘못 분류한 확률, 2클래스 테스트 에러는 악성코드로 분류된 것에서 실제 악성코드를 잘못 분류한 확률이다.

2. 신원인식

본 절에서는 딥러닝을 사용하여 사용자의 신원인식을 하는 방법에 대해서 살펴본다. 신원인식은 일반적인 아이디와 패스워드 쌍의 입력을 통한 전통적인 방법이나 자필서명, 최근에는 얼굴인식, 홍채인식, 지문인식, 성문인식 등 다양한 생체인식 기술이 연구되고 있다. 특히 CNN은 딥러닝 기술 중 이미지 학습에 강점을 보이는 기술로써 CCTV나 카메라에 의존한 생체인식에서 특히 많이 연구되고 있다.

지문인식은 신원인식 중에서도 그 방법이 비교적 간단하면서도 인식 속도나 정확성 등에서 우수한 점을 보이기 때문에 가장 일반적인 생체인식 방법이다. 그러나 지문은 라텍스나 젤라틴, 실리콘 등의 일상에서 볼 수 있는 물질로도 쉽게 위조될 수 있다는 취약점이 존재한다. 따라서 지문은 위조 여부를 판별하는 것이 필요하다. 이에 하드웨어적인 방법으로는 지문과 동시에 손가락의 혈압이나 혈류 등을 채취하는 방법이 있는데 부가적인 센서가 필요하므로 추가 비용이 발생한다. 소프트웨어적인 방법으로는 지문 이미지에서 융선의 밀도나 크기, 연속성과 같은 세부적인 지문의 특징들을 추출하여 정밀하게 분석하는 방법이나 일반적인 지문 이미지인 밝기, 대조, 주파수 영역에서의 대조값 등을 이용하는 방법도 있다.

앞서 소개한 CNN을 이용한 지문 이미지 학습으로 위조지문 판별을 내리는 연구도 진행되고 있으며, Nogueira는 위조지문 판별대회인 LivDet2015에서 CNN을 이용한 알고리즘을 사용하여 우승하였다[3]. 국내 연구에서는 CNN을 이용한 지문 이미지 학습에서 CAM(Class Activation Map)을 사용하여 지문 이미지를 학습할 때 실제로 지문의 어느 영역이 학습이 되는지를 시각화 하였다. 또한 위조지문을 판별할 때도 지문의 어느 영역에 주로 반응하여 위조 판별을 내리는지도 시각화 하여 CNN을 이용한 위조지문 판별의 기준을 확인하였다[4].

또 다른 신원인식 방법으로써 일반적으로 보안 분야에서 알려진 전자서명(Digital Signature)과는 달리 실제로 사용자가 POS나 PDA와 같은 디지털 기기에 자필서명을 하는 경우도 있다. 특히 최근에는 스마트폰의 펜터치 인식기능을 활용하여 서명을 하는 경우도 많다. 이에 위조서명을 방지하기 위해 서명 데이터를 학습하는 방법도 있다. 국내의 연구에서는 스마트폰에서 사용자가 손가락으로 서명할 때 발생하는 사용자의 서명을 32ms마다 샘플링하고 샘플링 간격마다 발생하는 서명 포인트의 가속도 값 등을 수집하여 Auto Encoder 기반의 1-Class 분류 모델을 학습시켜 위조서명을 판별하였다[5].

이 외의 딥러닝을 이용한 신원인식 방법으로 얼굴인식의 정확도를 높이기 위해 얼굴인식에 헤어스타일, 위치정보, 걸음걸이뿐 아니라 CNN을 이용하여 인식대상의 의복정보를 추가하여 인식하는 연구도 진행되고 있다[6].

3. 핀테크 보안

본 절에서는 스마트폰 응용 기반의 핀테크 보안 기술 중 기계학습이나 딥러닝을 사용하는 분야와 그 사례에 대해 살펴본다. 핀테크는 금융(Financial)과 기술(Technology)의 합성어로, IT의 발전에 따라 금융 서비스와 금융 산업이 변화 발전하면서 생긴 용어이다. 특히 스마트폰과 같이 모바일 컴퓨팅 환경의 발전으로 인해 개인의 금융 서비스 접근성은 좋아졌지만 그에 따른 보안 위협도 증가하여 핀테크 분야에서 보안은 더욱 중요한 위치를 차지하게 되었다.

스마트폰은 터치 센서나 가속도, 마이크, 카메라 등의 다양한 센서를 가지고 있으며 사용자가 핀테크 서비스를 받을 때 이러한 센서들을 사용하여 사용자 식별이나 인증을 하게 된다. 앞서 2.2절의 자필서명도 이에 해당한다. 그 외에 키 입력이나 터치 패턴, 마우스 포인트 이동, 음성 인식 등 사용자 행동을 분석하는 기술을 행위기반 인증기술로 분류한다.

키 입력은 여러 행위기반 인증기술 중에 가장 연구가 많이 된 분야이다[7]. 이는 사용자가 키를 누르고 떼는 시간을 측정하여 표준과 편차 등을 이용하는 기술인데, 최근에는 스마트폰의 터치스크린 기술로 인하여 키 입력 외에 탭, 스와이프, 제스쳐 등의 패턴도 포함한다. 이러한 사용자 입력을 뉴럴 네트워크나 SVM 등을 이용하여 학습한다. 이러한 학습 정보를 바탕으로 사용자가 핀테크 서비스를 이용할 때 평소와 다른 터치스크린 탭 패턴을 보이거나 암호 입력 속도가 차이가 나면 인증에 실패한다. 또한 스마트폰에 내장된 가속센서나 자이로센서, 터치 위치 그리고 디바이스에 따라 감압 정보 등을 이용하여 기존의 단순 키 입력보다 더 많은 특징들을 기반으로 다양한 환경에서의 입력 상황을 가정하여 위조 인증을 판별할 수 있다[8].

음성 인식은 인공지능과 자연어 처리 기술의 발전으로 인해 애플의 시리나 마이크로소프트의 코타나, 구글 나우가 보여주는 것처럼 많은 발전을 보이고 있지만, 아직까지 음성 인식을 넘어서는 화자 인증의 단계에서는 상용기술로 사용되지 않고 있다. 이는 음성 녹음을 이용한 리플레이 공격이나 주변 노이즈

에 민감한 것이 취약점으로 작용하기 때문이며 이를 극복하기 위해 많은 연구가 진행되고 있다.

현재 핀테크 보안에서 실제로 사용되는 행위기반 인증 기술들은 대부분이 키 입력 기반의 부정행위 패턴 감지로써 기존에 학습된 사용자의 입력패턴과 다른 패턴이 들어올 시 인증에 실패한다. 이러한 키 입력 패턴의 특징으로는 키 입력 시간, 간격, 터치 포인트와 같이 일반적인 특징 외에 왼손잡이 및 오른손잡이, 터치스크린과의 입력 각도, 입력하는 사용자의 물리 위치 등 여러가지 정보를 활용하는 연구가 진행되고 있다.

4. 스테그아날리시스

본 절에서는 스테가노그래피를 검출하는 스테그아날리시스 기술에서 딥러닝을 이용한 범용적 모델 구성에 대해 살펴본다.

스테가노그래피는 원본 파일을 크게 훼손하지 않으면서 암호화된 메시지를 삽입하는 기법이다. 원본 파일로는 이미지, 텍스트, 영상, 음성 등 여러가지가 있을 수 있으며 주로 이미지에 암호화 메시지를 넣는 기법이 많이 연구되고 있다. 스테가노그래피는 원본 파일의 헤더나 EOF 뒤에 자료를 삽입하는 삽입기법과 각 이미지 픽셀들의 LSB값만 변형시켜 사람의 육안으로는 변형을 확인하기 힘들게 하는 수정기법이 있다. 삽입기법은 원본 파일의 변형이 없고 삽입한 내용도 그대로 드러나서 발견 및 분석이 쉽지만 수정기법은 발견이 쉽지 않으며 발견하더라도 수정 내용에 대해 분석이 필요하다. 이러한 수정기법에는 HUGO(Highly Undetectable steGO), UNIWARD(UNIversal Wavelet Relative Distortion), WOW(Wavelet Obtained Weights) 등이 있다.

이런 스테가노그래피를 사용하여 인터넷에서 사용자들이 쉽게 받을 수 있는 자료에 악성코드를 숨겨놓는 보안 위협도 증가하고 있다. 지난 2015년 7월에는 스테가노그래피를 사용한 해머토스라는 악성코드가 보고되었으며 평범한 이미지 파일에 암호화된 명령을 숨긴 후, 필요 시 복호화 하여 피해자의 컴퓨터에 연결된 클라우드 저장소에 접근하는 툴이었다.

스테그아날리시스는 이러한 스테가노그래피 기법에 대응하여 데이터에서 스테가노그래피를 검출하는 기법이다. 스테그아날리시스도 여러 방면으로 연구되고 있는데, 2015년 Qian은 특징 추출과 분류과정을 딥러닝을 이용하여 스테그아날리시스를 수행하였다[9]. 그리고 2016년 Pibre는 여러가지 신경망을 사용한 스테그아날리시스를 분석하였고 CNN에서 가장 좋은 결과를 보임을 확인하였다[10].

그러나 아직까지 스테그아날리시스는 특정 스테가노그래피 기법에 대해 학습을 하면 해당 기법의 스테고 데이터에 대해서만 검출이 가능하다는 단점이 존재한다. 이 때문에 범용적인 스테그아날리시스 모델에 대한 연구가 진행되고 있다. 국내의 연구에서는 UNIWARD와 HUGO로 만들어진 스테고 데이터를 CNN으로 학습하여 범용적 스테그아날리시스 기법에 대한 가능성을 확인하였다[11]. 학습 모델은 총 3개로 모델1은 UNIWARD 스테고 데이터 셋만 학습시킨 모델, 모델2는 HUGO 스테고 데이터 셋만 학습시킨 모델, 모델3은 UNIWARD와 HUGO 스테고 데이터들이 섞여있는 데이터 셋을 학습시켰다.

표 2. 모델별 HUGO, UNIWARD 데이터의 분류 결과

Embedded dataset	Model1 (UNI)			Model2 (HUGO)			Model3 (UNI+HUGO)		
	Acc	Pre	Rec	Acc	Pre	Rec	Acc	Pre	Rec
HUGO	0.50	0.13	0.01	0.69	0.67	0.79	0.69	0.67	0.75
UNIWARD	0.97	0.97	0.97	0.66	0.65	0.74	0.88	0.75	0.91

〈표 2〉에서 보듯이 단일 스테가노그래피 기법을 학습시킨 모델 1, 2에 비해 두가지 기법을 학습시킨 모델3의 성능은 약간 낮거나 때론 더 좋은 결과를 보였다.

Ⅲ. 사물인터넷 기술 동향

1. 사물인터넷 개요

본 절에서는 사물인터넷에 대해서 살펴본다. 사물인터넷이란 사물(thing)들이 하나의 인터넷(Internet)망을 구축한다는 의미이다. 즉, 모든 디바이스가 인터넷에 접속이 된다는 의미이다.

사물인터넷은 기본적으로 4개의 계층으로 구성된다. 〈그림 2〉는 사물인터넷의 4계층을 보여주고 있다. 사물인터넷은 디바이스, 통신, 플랫폼, 응용서비스 계층으로 구성된다.

디바이스 계층은 사물인터넷 디바이스들이 동작하는 계층을 의미하며, 주로 사물인터넷 데이터를 수집하는 역할을 수행한다. 사물인터넷 디바이스란 스마트폰과 같은 실생활에 사용되는 고사양 디바이스부터 4비트급의 초경량 디바이스를 포함한다. 또한 사물인터넷 디바이스는 WiFi, ZigBee, 블루투스 등 다양한 유무선 통신을 사용할 수 있다.

통신 계층은 사물인터넷 디바이스가 수집한 데이터를 사물인터넷 플랫폼에 전송해줄 수 있도록 하는 계층이다. 즉 사물인터넷 환경을 구축을 위한 연결성 이슈를 위해 존재한다. 일반적으로 통신 계층에는 사물인터넷 게이트웨이가 포함되며, 멀티프로토콜과 같은 연결성을 위한 기능과 경량프로세싱 기능을 수행한다.

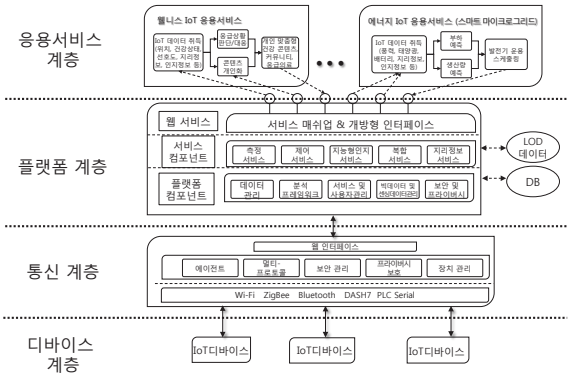

그림 2. 사물인터넷 전체 구성도

플랫폼 계층은 사물인터넷의 디바이스, 사용자, 서비스 등을 관리하고, 사물인터넷 데이터에 대한 분석을 수행한다. 또한 분석된 데이터를 기반으로 응용서비스 계층에 메쉬업 API(application program interface)를 제공해준다.

응용서비스 계층은 플랫폼에서 제공된 메쉬업 API를 기반으로 사용자 중심의 서비스를 제공한다. 사물인터넷 응용서비스는 사물인터넷 빅데이터를 통해서 사용자의 상황 및 의도에 맞는 서비스를 지능적으로 제공해주는 서비스라고 할 수 있다.

2. 사물인터넷 지능형 프레임워크

본 절에서는 사물인터넷 환경에서 지능형 프레임워크가 상호동작하는 방법에 대해서 살펴본다. 지능형 인지프레임워크란 SVM, KNN 등과 같은 기계학습 기법과 CNN, RNN 등과 같은 딥러닝 기법에 기반하는 프레임워크로, 데이터로부터 상황이나 데이터의 의미를 추론할 수 있는 프레임워크이다.

상황과 데이터간의 연관성이 있다면, 데이터로부터 상황을 추론하는 것은 어렵지 않다. 그러나, 문제는 상황과 데이터간의 직관적으로 연관성이 있지만, 그것을 모델링하는 것은 쉽지 않은 일이다.

기존의 기계학습에 기반하는 알고리즘은 데이터로부터 특징(feature)를 추출하여, 추출된 특징을 이용하여 학습과 분류 및 예측을 수행한다. 이러한 경우에는 의미있는 특징을 선택하고 추출해야만 한다.

하지만 CNN이나 RNN과 같은 딥러닝 기반은 특징을 학습하기 보다는 데이터를 학습하고, 학습된 데이터에 대한 모델링을 한다. 그리고 특정 데이터가 주어졌을 때, 학습된 모델을 이용하여 특정 데이터를 분류 또는 예측한다.

최근에는 개인당 사용 디바이스 수가 100개를 넘어가고 있는 실정이다. 이러한 환경에서 사물인터넷 데이터는 초당 테라급의 데이터가 생성될 수 있다. 그러나 이러한 빅데이터를 모두 분석하여 특정 사건에 대해 데이터의 특징점을 분석하는 것은 현실적으로 어렵다.

따라서 데이터에 대해 사건을 라벨링한 데이터를 학습하고, 모델링할 수 있는 딥러닝 기반 프레임워크는 사물인터넷의 지능화에 핵심알고리즘이라고 볼 수 있다. 그러나 딥러닝 기법은 학습하는데, 많은 시간을 요구한다.

다시 말해 딥러닝 학습알고리즘을 사물인터넷 플랫폼에서 수행하면, 플랫폼에 엄청난 과부하를 초래할 수 있다. 따라서 지능형 인지프레임워크를 독립적으로 분리하여 학습에 대한 과부하를 분산할 필요가 있다.

〈그림 3〉은 사물인터넷 환경에서 지능형 인지프레임워크와 사물인터넷의 각 계층와 연결되는 상호동작 구성도를 보여준다. 사물인터넷 게이트웨이, 플랫폼, 서비스에서 각 개체가 보유한 데이터를 이용하여 지능화를 수행하려고 할 때, 지능형 인지프레임워크를 통해서 API형태로 수행할 수 있다.

실제 응용서비스를 위해서 각 서비스마다 지능형 인지프레임워크를 해당 서비스에 특정하여 운영할 수도 있다. 이러한 경우 인지프레임워크에서 학습알고리즘을 수행하고 모델링한 정보를 서비스 단말에 저장하여, 서비스 단말에서 분류 또는 예측을 수행하는 방법도 고려할 수 있다.

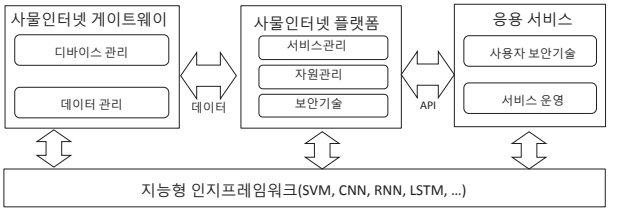

그림 3. 지능형 인지프레임워크 상호동작 구조도

3. oneM2M 보안기술

oneM2M[12]의 보안아키텍쳐는 보안기능계층 (Security Function Layer), 보안환경추상계층 (Secure Environment Abstraction Layer), 보안환경계층(Secure Environments Laye)으로 구성된다. 보안기능계층은 oneM2M의 실직적은 보안기능을 제공해주는 계층으로 식별 (Identifiction) 및 인증 (Authentication), 인가(Authorization), 식별자 관리(Identity Management), 보안 연관(Security Association), 민감데이터 관리(Sensitive Data Handling), 보안 관리(Security Administration)기능들을 제공한다. 보안환경추상계층은 보안환경계층의 요소를 이용하여, 실질적으로 보안기능에서 사용할

암호알고리즘 등을 제공해준다. 보안환경계층은 민감데이터 등에 접근하기 위해서 물리적으로 필요한 요소를 정의하며, 스마트카드, 유심(USIM)카드 등이 해당 계층에 포함된다.

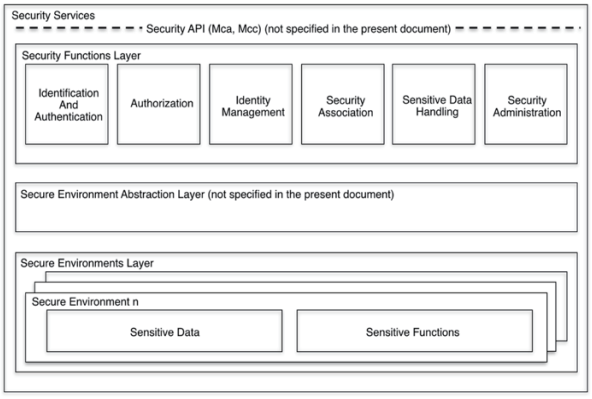

그림 4. oneM2M 보안아키텍쳐

oneM2M은 각 디바이스를 노드(Node)라고 지칭하며, 하나의 노드는 응용개체(Application Entity), 공통서비스개체(Common Service Entity)로 구성한다.

식별 및 인증을 위해 노드 내의 각 개체에 대한 식별자를 부여하고, 이는 각각의 사용용도와 특성에 따라서 글로벌 또는 로컬 유일성(Uniqueness)을 가진다.

원격 보안 준비 프레임워크(Remote Security Provisioning Framework)는 oneM2M 엔터티간의 식별 및 인증을 위한 사전 보안 정보를 원격으로 배포하기 위한 프레임워크로 대칭키, 인증서, GBA기반의 3가지 준비 프레임워크를 제공한다. 보안 연관 성립 구조(Security Association Establishment Framework)는 원격 보안 준비 프레임워크를 통해서 분배된 키 또는 인증서를 이용하여 두 개체간의 상호 인증을 수행한다.

보안 연관 성립 구조는 자격 증명 설정(Credential Configuration), 연관 설정(Association Configuration), 연관 보안 핸드쉐이크(AssociationSecurity Handshake) 단계로 구성된다. 자격 증명 설정 단계는 각 구조에 맞는 자격 증명 요소를 설정하고, 자격 증명 요소로는 사전분배된 대칭키, 인증서, 마스터 자격 증명(Master Credential)이 존재하며 이를 통해 개체간의 상호 인증을 수행한다. 연관 설정 단계는 식별 및 상호 인증에 필요한 엔터티의 식별자를 설정하고, 인증서 기반의 보안 연관 성립 구조에서는 검증과정에서 필요한 인증서 이름, RoT(Root of Trust)의 정보가 설정한다. 연관 보안 핸드쉐이크는 개체간의 식별 및 인증하고, 보안 채널을 성립한다.

인가 기능은 인증된 개체(Entity)가 리소스에 접근할 때, PEP, PDP, PRP, PIP 간의 요청 및 응답을 통해 접근 여부를 결정한다. PEP(Policy Enforcement Point)는 oneM2M 리소스에 대한 접근 요청을 받고, 접근 결정에 따라 리소스에 연결하도록 하는 역할을 수행한다. PDP(PolicyDecision Point)는 PRP, PIP와의 요청/응답을 통해 접근 요청에 해당되는 인가 정책들과 속성들을 가져오고, 접근 제어 리스트(Access Control List), 역할 기반 접근 제어(Role-Based Access Control), 속성 기반 접근 제어(Attribute-Based Access Control)등의 접근 제어정책을 이용하여 리소스에 대한 접근 여부를 결정하는 역할을 수행하며, 접근 결정 결과를 PEP에게 전송한다. PRP(PolicyRetrieval Point)는 접근 제어 정책을 관리하며 PDP의 접근 제어 정책요청에 대한 응답(Policy Response)를 전달하고, PIP(PolicyInformation Point)는 인가 정책을 평가하는데 필요한 속성들을 관리하며, PDP의 요청에 따른 응답을 전송한다.

4. IoTivity 보안기술

IoTivity[13] 디바이스는 서비스를 사용하는 OIC Client, 서비스를 제공하는 OIC Server, 서비스 중계 역할을 수행하는 OIC Intermediaries로 구성된다. 각각의 디바이스는 응용 리소스(Application Resources)을 가지고 있으며, 각 애플리케이션에 대한 응용 프로파일(Application profiles)이 정의된다. 이 때, 응용 프로파일에는 접근제어를 수행하는 SRM(Secure Resource Manager)과 보안 리소스(Security Resources) 가 있으며, 보안 채널을 형성하기 위한 Session Protection 등이 포함될 수 있는데, 이는 각각의 애플리케이션 특성마다 특화된 응용 프로파일로 정의된다.

OIC Client는 OIC Resource에 대한 접근 요청 Action을 수행하며, Resource 에 대한 접근 제어는 OIC Server의 접근 제어 모델에 따라 수행된다. OIC Client는 Resource를 소유하고 있는 OIC Server와 네트워크 연결을 성립하고, 연결성 추상 계층은 추상화를 통해 다양한 연결 옵션을 제공한다. OIC 디바이스를 식별하기 위해서 IoTivity에서는 Device ID를 사용한다. 네트워크 주소는 DeviceID로 맵핑되며 네트워크 주소를 통해 연결이 성립한다.

IoTivity에서 보안 정책은 Device ID를 이용하여 기술되는데, (D)TLS를 이용하여 보안 채널을 생성하고, 로컬플랫폼에 저장되어 있는 암호키를 이용하여 상호 인증 및 보안 통신을 수행한다. OIC Client가 리소스에 접근하기 위해서 OIC Server는 OIC Client에 대한 식별 및 인증을 수행하고, SRM은 접근제어모델에 따라 접근 제어를 수행한다. SRM이 접근제어를 수행하기 위해서 보안 리소스에 정의된 모델을 참조하는데, 보

안 리소스를 정의하기 위해서 ACL, 서비스(Service), 자격증명(Credential)에 대한 각각의 오브젝트를 정의한다.

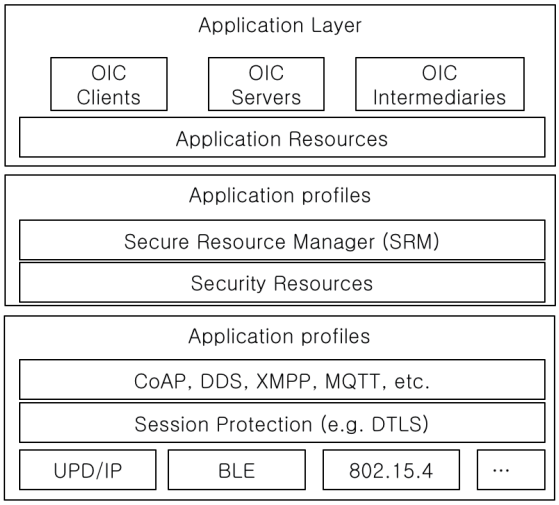

그림 5. IoTivity 보안아키텍쳐

5. LWM2M 보안기술

LWM2M[14]기반의 리소스에 대한 접근제어는 접근제어객체(Access Control Object)에 의해서 결정된다. 접근제어객체는 LWM2M 서버가 LWM2M 클라이언트의 객체(Object)에 접근할 때, 적절한 권한을 가졌는지를 확인하기 위해서 사용하며, LWM2M에서 접근제어객체를 기술하기 위해서 XML 스키마를 이용한다. 접근제어객체의 상위 스키마는 Resource 스키마로 구성되며 Operations 태그는 Read/Write/Execution에 대한 권한설정을 할 수 있고, RangeEnumeration을 통해서 설정 가능한 범위를 기술한다.

LWM2M기반의 리소스에서 접근제어객체를 작성할 때, 그 외에도 ObjectID, ItemID 등을 포함하고 Resources 스키마에 다수의 ItemID를 포함하여 하나의 Object 밑에 있는 Item을 생성한다. 실질적으로, LWM2M 서버가 LWM2M 클라이언트에게 LWM2M 기반의 리소스를 요청하면, 정의된 접근제어객체에서 LWM2M 서버가 Object/Item에 대한 권한이 있는 지를 확인하고 기술된 접근제어객체의 Operation이 R/W/RW/E 인지에 따라서 LWM2M 서버에 접근권한을 할당한다.

```
<xs:element name="Resources">
  <xs:element name="Name" type="xs:string"/>
  <xs:element name="Operations"/>
  <xs:element name="MultipleInstances"/>
  <xs:element name="Mandatory"/>
  <xs:element name="Type"/>
  <xs:element name="RangeEnumeration" type="xs:string"/>
  <xs:element name="Units" type="xs:string"/>
  <xs:element name="Description" type="xs:string"/>
</xs:element>
```

그림 6. LWM2M의 접근제어객체 스키마

Ⅳ. 지능형 사물인터넷 보안 기술 연구방안

본 장에서는 사물인터넷 환경에서 딥러닝 알고리즘 기반의 보안 기술을 적용하기 위한 방안을 제시한다.

사물인터넷 환경은 다수의 디바이스에서 생성되는 빅데이터를 분석 및 사용하여 다양한 사용자 중심의 서비스를 제공하는 것을 목표로 한다. 즉, 다수의 디바이스와 서비스들의 하나의 플랫폼에서 망을 구축하고 있다는 것이다.

이로 인해서 해당 플랫폼에서는 대량의 데이터와 서비스를 분석하여 사용자의 상황이나 의도를 추론 및 예측하는 성능을 높일 수 있다. 반면에 모든 서비스와 디바이스가 연결되어 있다는 것은 플랫폼뿐만 아니라, 사용자와 서비스까지 모든 구간의 보안이 밀접하게 연결되어 있다는 의미이다.

따라서 사물인터넷 환경에 적합한 보안 기술을 개발하기 위해 oneM2M, IoTivity, LWM2M 등과 같은 주요 사물인터넷 플랫폼에서는 보안아키텍쳐를 적립하기 위한 많은 노력을 해왔다. 그러나, 여전히 추출 특징 분석을 기반으로 하는 기법에 기반하고 있다.

반면에 사물인터넷 환경에서 디바이스 및 서비스에 대한 공격기법은 다양한 계층에서 융합된 형태의 공격기술에 등장하고 있다. 이러한 고도화된 공격기술을 탐지하기 위해서는, 해당 공격기술에 대한 지식습득과 탐지를 위한 특징을 추출하는 과정이 요구된다. 이러한 과정은 급속하게 변하고 있는 사물인터넷 환경에서 그에 따른 보안 기술을 제공하기에는 한계가 생길 수 밖에 없다.

따라서 본고에서는 능동적 사물인터넷 보안기술을 위한 연구방안으로 딥러닝 기법과 보안기법의 융합연구 방법을 제시한다. 기존의 딥러닝 기반 기법은 하나의 개체에서만 독립적으로 수행되는 구조를 가졌다. 하지만, 사물인터넷에서는 사물인터넷 디바이스들이 개별로 지능형 알고리즘을 수행할 수 있는 능력을 모두 보유하고 있지 않은 환경이다.

이 때문에 사물인터넷 게이트웨이가 연결된 사물인터넷 디바이스들에 대한 보안성 검토를 수행을 한다. 또한, 플랫폼에서는 사물인터넷 게이트웨이와 서비스를 위한 데이터에 대한 보안성 검토를 수행한다.

〈그림 7〉은 지능형 사물인터넷 보안기술을 위한 구조도를 보여준다. 사물인터넷 보안기술에 지능형 알고리즘을 적용했을 때, 야기될 수 있는 문제는 학습의 문제이다. 보안을 위한 학습을 수행할 모듈을 추가하고, 해당 보안 모듈이 게이트웨이와 플랫폼과 상호동작하면서 다양한 보안을 탐지해주는 구조를 가져야 한다.

이 때에는 보안모듈에서 학습기능만 수행하는 경우와, 학습과 분류 및 예측기능을 수행하는 두가지 모델로 구성될 수 있다. 보안 모듈에서 학습기능만 수행할 경우, 게이트웨이가 분류 기능을 수행할 수 있을 정도의 계산능력을 가져야 한다.

하지만 보안모듈이 학습 및 분류/예측 기능을 수행할 경우에는, 보안모듈 내에서 학습 기능을 위한 독립적 모듈이 요구된다. 학습 기능은 많은 부하를 야기할 수 있기 때문에, 분리된 모듈을 수행하지 않을 경우 실시간 데이터에 대한 예측 및 분류 모델을 제공하기 어렵기 때문이다.

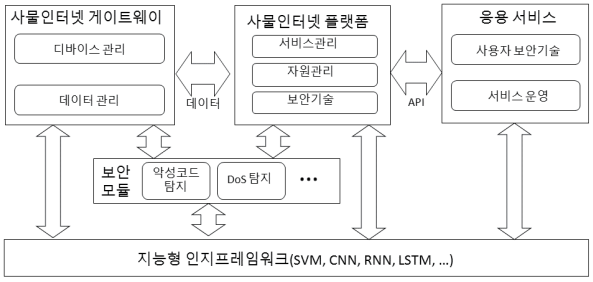

그림 7. 사물인터넷 보안과 지능형 프레임워크 구성도

V. 결론

사물인터넷이란 사물들이 하나의 인터넷을 만들어서 운영되는 환경으로, 하나의 플랫폼의 다수의 디바이스와 서비스가 연결된다. 이러한 환경에서는 초당 대량의 데이터가 생성된다. 또한, 기존의 고사양 컴퓨터 환경과 달리, 사물인터넷 디바이스는 4비트급 초경량 디바이스까지 포함하며, 이는 보안 공격에 완전히 노출되어 있을 수 밖에 없다.

사물인터넷은 서비스, 플랫폼, 통신, 디바이스의 4계층으로 구성된다. 특히, 디바이스 및 서비스 계층은 다양한 이기종 디바이스와 서비스를 포함한다. 이 때문에, 다양한 방법으로 플랫폼, 게이트웨이, 디바이스, 사용자 등 다양한 자원 및 개체를 대상으로 공격을 시도할 수 있다. 컴퓨터 또는 웹기반 서비스와 같이 특정 공격점으로 한정되는 것이 아니기 때문에, 사물인터넷 환경에서는 공격의 방법 또한 여러 계층의 하이브리드로 구성될 수 있다. 기존의 연구되었던 많은 공격 기법들은 이러한 공격을 분석하여 각 공격의 특징을 찾아낸다. 그리고, 주어진 특징에 대한 유효성 및 정당성을 검사하여 공격을 탐지 및 예측하는 방법을 주로 사용하였다.

하지만 급변하는 데이터와 서비스가 연결된 사물인터넷 환경에서는 공격 분석 및 대응을 통한 방법으로는 능동적으로 공격에 대응하기가 어렵다. 이를 해결하기 위해서, 데이터와 라벨링을 이용하여 이벤트에 대한 모델링을 할 수 있는 딥러닝 기법 기반의 보안기술이 사물인터넷 환경에 적용될 필요가 있다.

본고에서는 사물인터넷 환경에서 딥러닝 기반 보안 기술을 적용하기 위한 연구 방안을 제시한다. 딥러닝 기법을 이용한 보안기술에 대한 연구는 수차례 진행되었다. 그러나, 독립적 환경에서 적용되는 보안기술은 사물인터넷 환경에서는 디바이스나 게이트웨이 계층에서 완전히 수행하는 것이 어렵다. 이를 해결하기 위해서, 분리된 보안 모듈에 대한 연구를 수행하고, 이를 사물인터넷 지능형 프레임워크와 연계하여 딥러닝 기반 알고리즘에 기반한 보안기술을 고려하여야 한다. 또한, 보안모듈에서 학습한 모델의 안전한 공유 방법에 대한 연구를 수행함으로써, 능동적인 사물인터넷 보안환경을 구축할 필요가 있다.

딥러닝 기반의 사물인터넷 보안기술은 기존의 특징 분석 및 추출 특징 기반의 보안 기술의 한계를 넘어서, 데이터들과 이벤트의 라벨링을 통해서 발견적 해결방법을 제시할 것이다. 이는 대량의 데이터에 대한 분석 및 특징 추출에 대한 부하를 줄여줄 것으로 기대된다.

참고문헌

[1] Daniel Bilar “Opcodes as predictor for malware” Int. J. Electronic Security and Digital Forensic, 1(2), 2007.

[2] Dahl, George E., et al. “Large-scale malware classification using random projections and neural networks.” 2013 IEEE International Conference on Acoustics, Speech and Signal Processing. IEEE, 2013.

[3] R.F. Nogueira, R. de Alencar Lotufo and R.C. Machado, “Fingerprint Liveness Detection Using Convolutional Neural Networks,” IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1206-1213, 2016.

[4] 김원진, 이경수, 박은수, 김정민, 김학일 (2016). Convolutional Neural Networks 특징을 이용한 지문 이미지의 위조여부 판별 및 시각화. 정보보호학회논문지, 26(5), 1259-1267.
[5] 남승수, 서창호, 최대선 (2016). 모바일환경에서 위조서명에 강건한 딥러닝 기반의 핑거서명검증 연구. 정보보호학회논문지, 26(5), 1161-1170.
[6] 홍성은, 임우빈, 박준우, 양현승 (2016). 얼굴과 의복 정보를 활용한 딥러닝 기반 신원인식. 대한전자공학회 학술대회, 2204-2207.
[7] David Umphress and Glen Williams. Identity verification through keyboard characteristics. International Journal of Man-Machine Studies, 23(3):263. 273, 1985.
[8] Zheng, Nan, et al., You are how you touch: User verification on smartphones via tapping behaviors, Network Protocols (ICNP), 2014 IEEE 22nd International Conference on. IEEE, 2014.
[9] Yinlong Qian, et al, "Deep Learning for Steganalysis via Convolutional Neural Networks", Proceedings of SPIE Media Watermarking, Security, and Forensics, vol. 9409, 2015.
[10] Lionel Pibre et al. "Deep learning is a good steganalysis tool when embedding key is reused for different images, even if there is a cover sourcemismatch", Proceedings of Media Watermarking, Security, and Forensics, 2016.
[11] 김현재, 이재구, 김규완, 백상현, 윤성로 (2016). 딥러닝을 이용한 범용적 스테그아날리시스. 한국 정보과학회 학술발표논문집, 1004-1006.
[12] OneM2M Alliance, "Onem2m: Standards for m2m and the internet of things.", 2014.
[13] OIC, "IoTivity 1.1.1", 2016
[14] Linyi Tian, "Lightweight m2m (oma lwm2m)." OMA device management working group (OMA DM WG), Open Mobile Alliance, 2012.

약 력

최 종 석

2011년 동명대학교 공학사
2013년 부산대학교 공학석사
2013년~현재 부산대학교 박사과정
관심분야: 사물인터넷, 정보보호 및 보안, 머신러닝/딥러닝, 취약점분석

박 종 규

2014년 부산대학교 공학사
2014년~현재 부산대학교 석박통합과정
관심분야: 사물인터넷, 정보보호 및 보안, FPGA/ASIC 칩 설계

김 호 원

1993년 경북대학교 공학사
1995년 포항공과대학교 공학석사
1999년 포항공과대학교 공학박사
2004년 Ruhr University Bochum, Post Doctorial
1998년~2008년 한국전자통신연구원 팀장
사물인터넷 연구센터 센터장
2008년~현재 부산대학교 전기컴퓨터공학부 부교수
관심분야: 사물인터넷, 정보보호 및 보안, 머신러닝/딥러닝, FPGA/ASIC 칩 설계