DU-도전학기 결과보고서

과제명	AI 기반, 홈 IoT 기기를 향한 DR-DoS 공격 탐지 솔루션 개발		
참여자	성명	소속	학번
	김OO	컴퓨터공학전공	
	이OO	컴퓨터공학전공	
	박OO	컴퓨터공학전공	
	안OO	컴퓨터소프트웨어전공	
지도교수 의견	상기 학생들은 주 3회 이상 토론하면서 단계적으로 도전학기 과제를 성실히 수행하였습니다. 4대의 라즈베리파이를 이용하여 사물인터넷 구축, 공격 주입, 데이터셋 수집 에이전트 개발, 딥러닝 기반 공격 탐지 및 식별 모듈 개발, 실시간 모니터링 대시보드 개발까지 직접 수행하였으며 이는 기존 상용 솔루션에도 존재하지 않는 최신 사물인터넷 보안 기술로 평가할 수 있습니다. 또한, 도전학기 성과를 대한임베디드공학회 추계학술대회에서 구두 발표하는 등 미래의 IT 전문인력으로서 학계의 발전에도 기여하였습니다. 최고의 팀워크와 열정, 뛰어난 전공실력으로 이루어낸 결과라고 생각하며 학생들의 그동안의 노력을 칭찬하고 싶습니다. (소속) 컴퓨터공학전공 (성명) 김지연 (서명 또는 날인)		

1. 도전 과제 내용

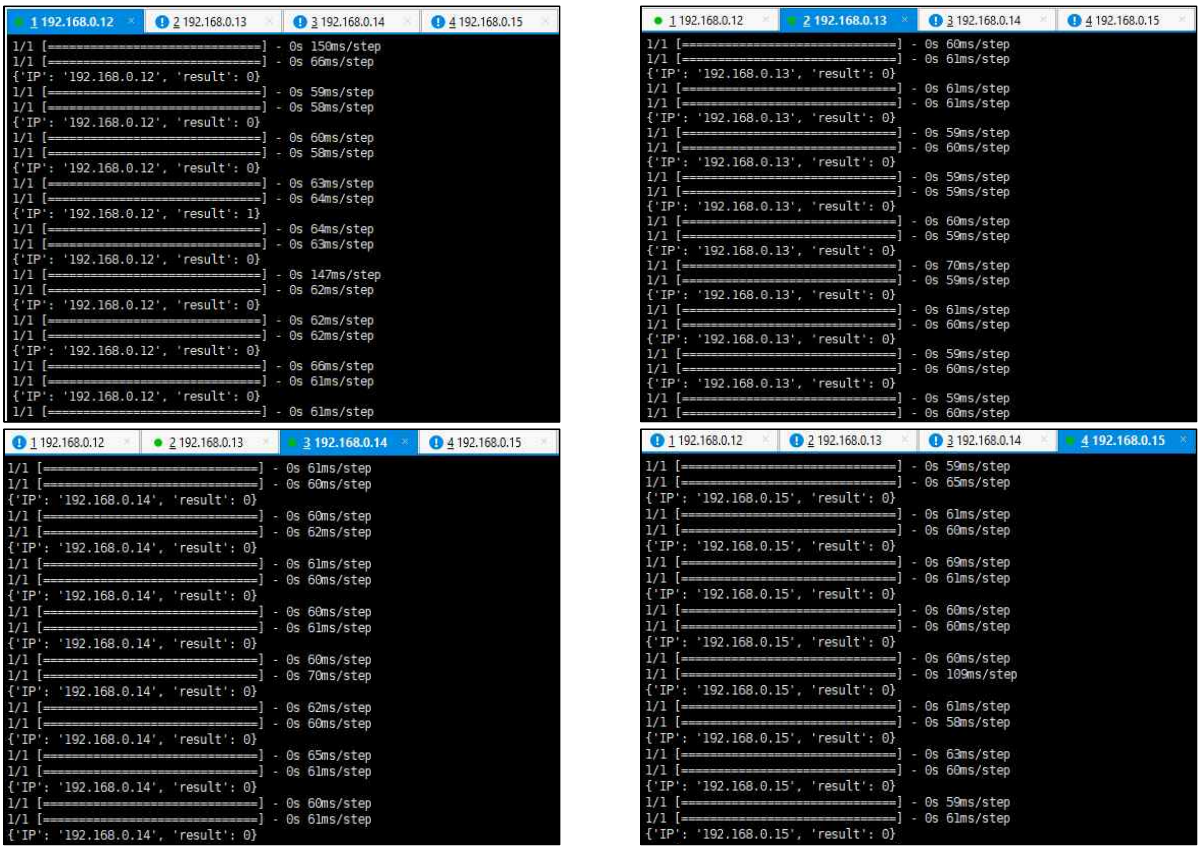
오늘날, 실생활에서 사물인터넷 기기들이 보편화되면서 개인정보유출이나 홈 캠 해킹 등 보안 취약점이 증가하고 있는 추세이다. 이러한 이유로 사물인터넷 보안의 중요성이 높아지고 있으며 보안에 대한 경각심도 중요시되고 있다. 본 팀의 주제는 AI기반, DR-DoS 공격 탐지 솔루션으로 시중에서 판매되는 상용 SW와의 차별점은 DoS 및 랜섬웨어등과 같은 공격 탐지 및 대응 기술을 가지고 있는 상용 SW의 특징은 단순히 공격을 탐지하고 대응하는 공격대응에 대한 부분만을 살린 기술이라고만 생각하였다. 본 팀은 이러한 기술들에서 학술적 가치를 탐구해보기 위해 DoS 공격의 변형인 DR-DoS 공격의 특징을 살린 탐지 솔루션을 제시하게 되었고, 다양한 연구를 찾아보았을 때, DR-DoS 공격의 특성에 맞게 연구된 내용은 연구가 미비하다는 것을 확인하였다. 따라서, 본팀은 '**DR-DoS 공격에 특화된 공격 탐지 솔루션**'을 제시한다는 점에서 학술적 가치가 있다고 판단되었기에 이러한 내용을 기반해 의의를 두고 도전학기 프로젝트를 진행했다.

본 팀은 초기 도전학기 계획서 내용과 같이 실제 홈 IoT에서 사용되는 센서환경 구현을 위해 라즈베리파이 4대를 사용하여 IoT 환경을 구현했으며, 이를 기반으로 구현된 센서들의 정상 상태와 DR-DoS 공격이 주입되었을 때의 비정상 상태의 메트릭 294종을 프로메테우스&NodeExpoter를 사용하여 수집하였다. 다음으로는 수집한 데이터 셋으로 IoT 기기의 정상/비정상 상태를 탐지하면서 **DR-DoS 공격의 특성**에 따라 **신속하게 공격자/반사체/희생자를 식별**할 수 있도록 RNN 학습 모델 코드를 구현하였다. 이러한 학습모델은 각각의 라즈베리파이에 에이전트로 장착하여 공격이 발생했을 경우 공격을 탐지해내는 역할을 한다. 즉, DR-DoS 공격을 받았을 경우 각각의 에이전트들이 신호를 출력하게 되면 이 신호를 소켓을 통해 통신하면서 구축한 DR-DoS 실시간 탐지 시스템으로 전송하게 되어 공격자/반사체/희생자 기기를 시공간적으로 공격 상태 및 정상 상태를 식별할 수 있도록 구현을 진행하였다.

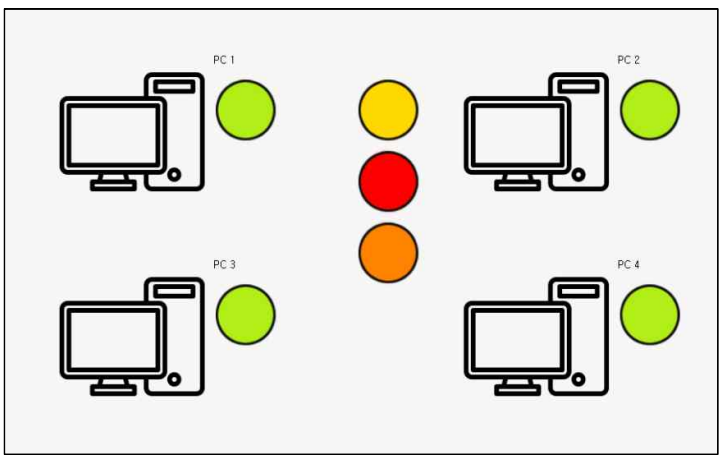
2. 도전 과제 수행 결과 및 성과

- 팀 공통 과제 수행 결과

본 팀은 도전학기 초기 계획대로 공격 선정 및 시나리오 구상을 통해 성공적으로 공격을 진행하였고 정상 및 DR-DoS 공격 데이터 수집에 성공했다. 이를 기반으로, 수집된 데이터들을 Grafana를 통해 시각화하여 분석을 진행할 수 있도록 구현했다. 수집된 데이터 셋의 특성에 맞게 학습 모델을 RNN으로 선정하여 진행하였고, 총 2,400개의 데이터 셋으로 정상/공격 상태를 식별할 수 있도록 학습을 진행했다. 다음으로는 학습된 모델을 각각의 4개의 라즈베리파이에 공격 탐지 에이전트로 장착하여 탐지할 수 있도록 진행했고, 에이전트에서 전송되는 신호를 기반으로 소켓을 통해 실시간 공격 탐지 시스템으로 전송시켜서 DR-DoS 공격이 이뤄졌을 때, 에이전트가 장착된 기기들의 상태를 시공간적으로 모니터링 할 수 있도록 하는 시스템 개발을 성공적으로 구현했다.



<그림 1> 4개의 라즈베리파이에 에이전트를 장착해 공격 탐지 진행



<그림 2> 실시간 공격 시공간 모니터링 UI 설계

3. 자기 평가

- 팀원 개별 과제 수행 결과

- 김OO : 도전 학기 초기에 계획했던대로 DR-DoS 공격 선정 및 공격 시나리오를 구성하여 hping3를 사용한 공격 Shell Script 작성을 진행했다. 또한, 11월에 개최된 대한 임베디드 공학회에 논문을 팀원들과 함께 투고하며 구두 발표를 진행하며 성공적으로 최종 결과물 달성에 나아가고 있다. 마지막으로 논문 투고 후 후속 연구로 진행한다고 예정했던 DR-DoS 공격 실시간 탐지 시스템 UI 설계를 팀원들과 함께하며 맡은 역할을 성공적으로 진행했다.

- 이OO : 팀원이 선정한 공격 시나리오를 기반으로 정상 및 DR-DoS 공격 학습데이터를 프로메테우스를 통해 성공적으로 수집하였으며, 이를 기반으로 RNN 기반의 DR-DoS 공격 탐지 모델 코딩을 진행했다. 학습을 진행하기위해 학습 데이터셋이나 학습 횟수 등과 같은 파라미터들을 설정하며 효과적인 공격탐지를 진행하기 위해 노력했다. 마지막으로 팀원과 함께 수집한 데이터 기반으로 Grafana 대시보드 구현을 진행하며 맡은 역할을 성공적으로 진행했다.

- 박OO : 실험 환경 구축 진행을 위해 라즈베리파이 4대를 직접 연결하여 IoT 환경 구축에 노력했으며, Grafana 및 NodeExpoter를 설치하는 등의 환경 구축을 성공적으로 해냈다. 이를 기반으로 팀원과 함께 정상 및 DR-DoS 공격 데이터인 294종의 메트릭 수집을 진행하였다. 이를 기반으로 Grafana를 대시보드 구현을 진행하여 정상 상태와 비정상 상태의 메트릭 분석을 진행하며 맡은 역할을 성공적으로 진행했다.

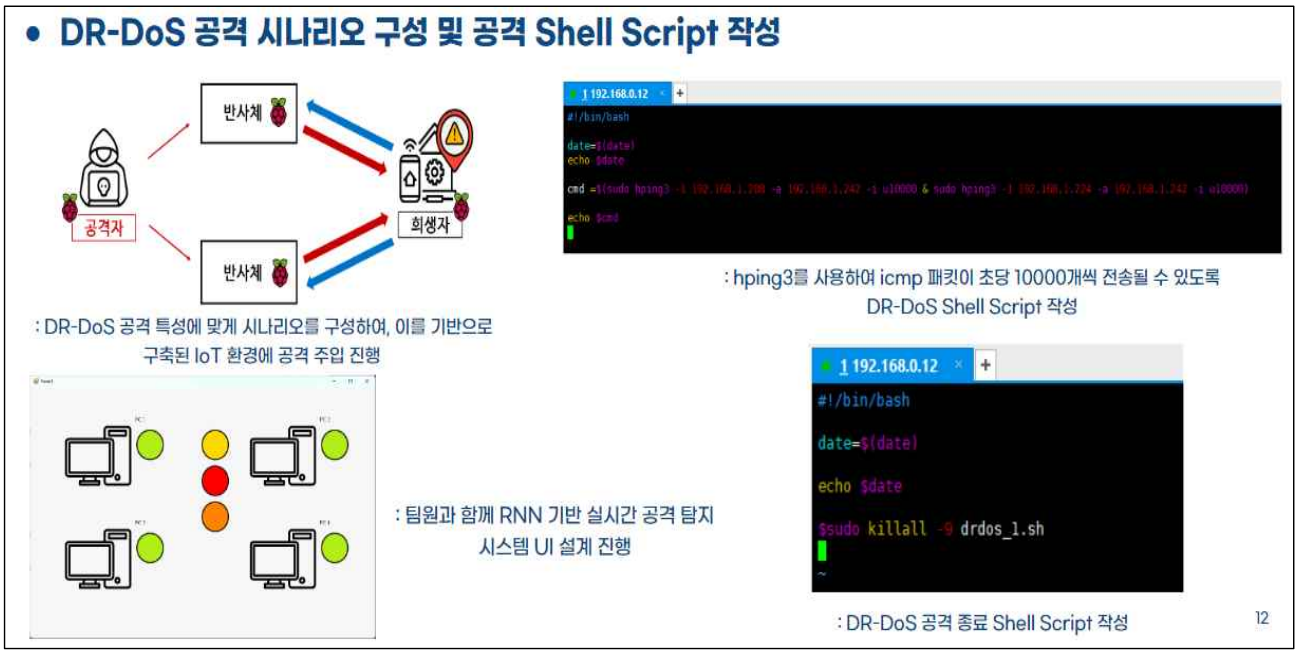
- 안OO : 자신의 관심 분야를 살려 DR-DoS 공격 실시간 팀지 시스템 구축을 진행했다. 팀원과 함께 공격자/반사체/희생자를 신속히 식별할 수 있도록 하는 공격 탐지 시스템 UI 설계를 진행했다. 이를 기반으로 소켓을 통해 전송받을 신호를 가지고 설계에서 더 나아가 .Net Framework와 C#을 사용하여 개체를 신속히 식별할 수 있도록 실시간 공격 탐지 시스템 개발을 성공적으로 진행했다.

▶ 팀원 모두 자신이 맡은 개인 과제를 도전 학기 초반에 세운 계획대로 잘 진행했기에 **AI 기반, DR-DoS 공격 탐지 시스템 개발** 프로젝트 진행을 성공적으로 진행할 수 있었다.

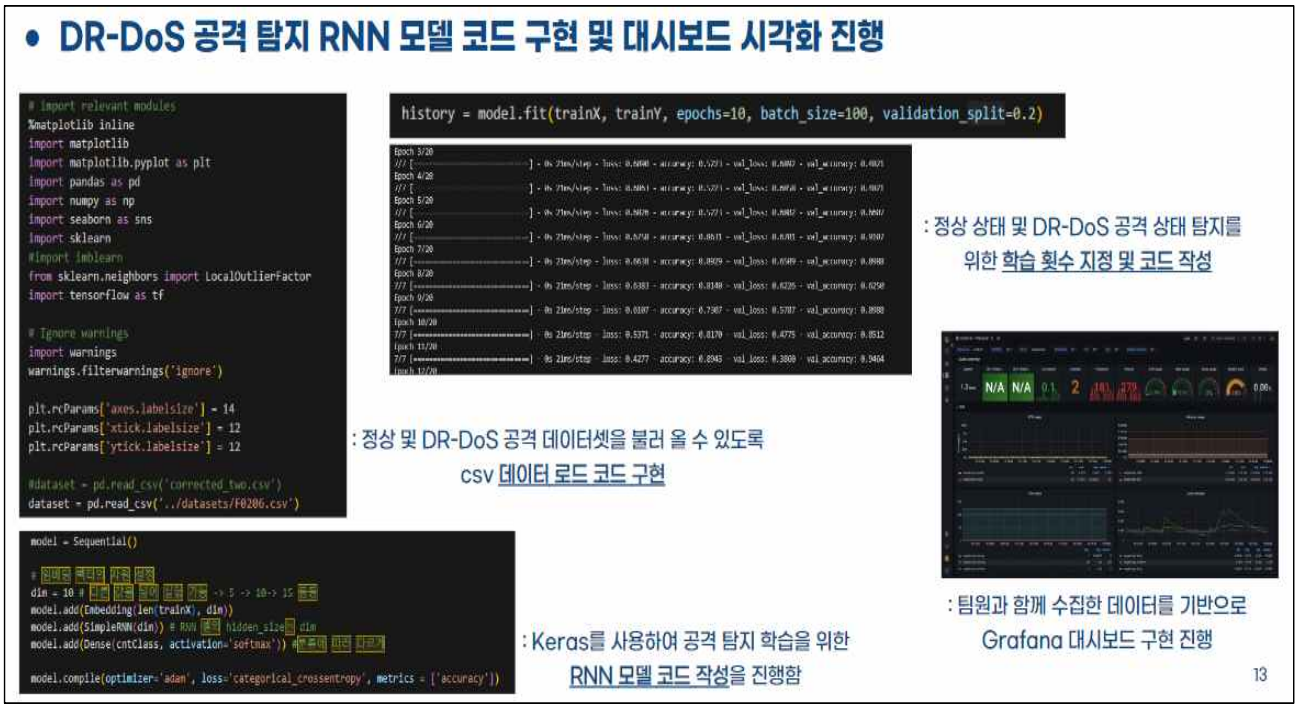
4. 최종 결과물

- 개인(팀원별) 결과물

- 김OO : DR-DoS 공격 시나리오 구성 및 공격 Shell Script 작성, 팀원과 함께 RNN기반 실시간 공격탐지 시스템 UI 설계 진행



- 이OO : DR-DoS 공격 탐지 RNN 모델 코드 구현 & 유지보수 및 팀원과 함께 데이터 수집 및 Grafana 대시보드 구현



- 박OO : 라즈베리를 통한 IoT 환경 구축과 정상 및 DR-DoS 공격 데이터 수집 진행, 팀원과 함께 Grafana 대시보드 구현

- 안OO : DR-DoS 실시간 공격 탐지 시스템 UI 설계 진행과 함께 설계한 UI를 기반으로 .NET Framework를 통한 DR-DoS 실시간 공격 탐지 시스템 구현

- **팀 공통 결과물 :** 홈 IoT 기기들이 사이버 공격을 받았을 경우 정상/비정상 상태를 탐지할 수 있는 딥러닝 모델(RNN 기반), DR-DoS 공격 탐지 실시간 시스템, 학술대회 논문

```python
#정상 1 공격 0

my_ip = "192.168.0.15"                          #설정
send_ip = ""                                    #설정
prometheus_url = "http://192.168.0.15:9090"   #설정

plt.rcParams['axes.labelsize'] = 14
plt.rcParams['xtick.labelsize'] = 12
plt.rcParams['ytick.labelsize'] = 12

test = pd.read_csv('192_168_0_15_total.csv')   #설정
test = test.drop(['timestamp'], axis=1)
test = test.drop(['Label'], axis=1)
test.head()

model = keras.models.load_model('192_168_0_15_RNN.h5')   #설정
scaler = MinMaxScaler(feature_range=(0, 10))
```

```python
#인공지능 탐지
def detection(test):
    #마지막 행의 데이터 갱신
    test.iloc[-1] = metric_request(metric_list.metrics_list)

    #데이터 전처리
    test = test.apply(pd.to_numeric, errors='coerce')
    cols = test.select_dtypes(include=['float64','int64']).columns
    sc_test = scaler.fit_transform(test.select_dtypes(include=['float64','int64']))
    testX = pd.DataFrame(sc_test, columns = cols)
    testX.head()

    #마지막 행만 추출
    testX = testX.iloc[-1:]

    Y_pred = model.predict(testX)

    y_pred = np.argmax(Y_pred, axis=1)

    y_pred = model.predict(testX)

    predict_classes=np.argmax(y_pred,axis=1)[0]
```

<그림 3> DR-DoS 탐지 딥러닝(RNN 기반) 모델 코드 구현

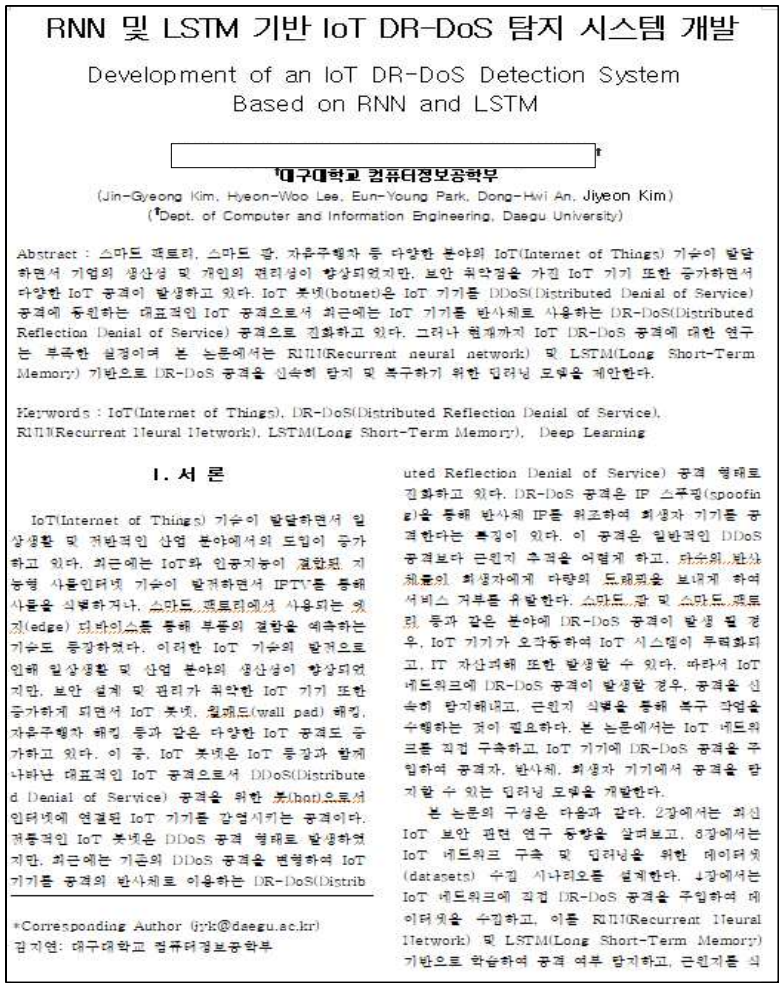
```python
public void Socket_Server()
{
    Socket server = new Socket(AddressFamily.InterNetwork, SocketType.Stream, ProtocolType.Tcp);
    // 내 pc IP
    IPEndPoint endPoint = new IPEndPoint(IPAddress.Parse("1.251.137.105"), 9999);
    // 내 IP로 소켓 생성
    server.Bind(endPoint);
    // 생성한 소켓 수신대기
    server.Listen(20);
    // 데이터를 무한히 받고 색깔도 바꿈
    while (true)
    {
        Socket client = server.Accept();
        IPAddress clientIP = ((IPEndPoint)client.RemoteEndPoint).Address;
        int clientPort = ((IPEndPoint)client.RemoteEndPoint).Port;

        byte[] receiverBuff = new byte[8192];
        int recvBytes = client.Receive(receiverBuff);
        string recvData = Encoding.UTF8.GetString(receiverBuff, 0, recvBytes);

        Console.WriteLine(recvData);

        client.Close();
        change_color(recvData);
    }
}
public Form1()
{
    InitializeComponent();
    // 쓰레드로 json 파일 수신 동시에 처리
    Thread thread = new Thread(() => Socket_Server());
    thread.Start();
}
```

<그림 4> DR-DoS 실시간 공격 탐지 시스템 코드 구현



RNN 및 LSTM 기반 IoT DR-DoS 탐지 시스템 개발

Development of an IoT DR-DoS Detection System Based on RNN and LSTM

[redacted]†

†대구대학교 컴퓨터정보공학부

(Jin-Gyeong Kim, Hyeon-Woo Lee, Eun-Young Park, Dong-Hwi An, Jiyeon Kim)

(†Dept. of Computer and Information Engineering, Daegu University)

Abstract : 스마트 팩토리, 스마트 팜, 자율주행차 등 다양한 분야의 IoT(Internet of Things) 기술이 발달하면서 기업의 생산성 및 개인의 편리성이 향상되었지만, 보안 취약점을 가진 IoT 기기 또한 증가하면서 다양한 IoT 공격이 발생하고 있다. IoT 봇넷(botnet)은 IoT 기기를 DDoS(Distributed Denial of Service) 공격에 동원하는 대표적인 IoT 공격으로서 최근에는 IoT 기기를 반사체로 사용하는 DR-DoS(Distributed Reflection Denial of Service) 공격으로 진화하고 있다. 그러나 현재까지 IoT DR-DoS 공격에 대한 연구는 부족한 실정이며 본 논문에서는 RNN(Recurrent neural network) 및 LSTM(Long Short-Term Memory) 기반으로 DR-DoS 공격을 신속히 탐지 및 복구하기 위한 딥러닝 모델을 제안한다.

Keywords : IoT(Internet of Things), DR-DoS(Distributed Reflection Denial of Service), RNN(Recurrent Neural Network), LSTM(Long Short-Term Memory), Deep Learning

I. 서 론

IoT(Internet of Things) 기술이 발달하면서 일상생활 및 거반적인 산업 분야에서의 도입이 증가하고 있다. 최근에는 IoT와 인공지능이 결합된 지능형 사물인터넷 기술이 발전하면서 IPTV를 통해 사물을 식별하거나, 스마트 팩토리에서 사용되는 엣지(edge) 데이터를 통해 부품의 결함을 예측하는 기술도 등장하였다. 이러한 IoT 기술의 발전으로 인해 일상생활 및 산업 분야의 생산성이 향상되었지만, 보안 설계 및 관리가 취약한 IoT 기기 또한 증가하게 되면서 IoT 봇넷, 월패드(wall pad) 해킹, 자율주행차 해킹 등과 같은 다양한 IoT 공격도 증가하고 있다. 이 중, IoT 봇넷은 IoT 등장과 함께 나타난 대표적인 IoT 공격으로서 DDoS(Distributed Denial of Service) 공격을 위한 봇(bot)으로써 인터넷에 연결된 IoT 기기를 감염시키는 공격이다. 전통적인 IoT 봇넷은 DDoS 공격 형태로 발생하였지만, 최근에는 기존의 DDoS 공격을 변형하여 IoT 기기를 공격의 반사체로 이용하는 DR-DoS(Distributed Reflection Denial of Service) 공격 형태로 진화하고 있다. DR-DoS 공격은 IP 스푸핑(spoofing)을 통해 반사체 IP를 위조하여 희생자 기기를 공격한다는 특징이 있다. 이 공격은 일반적인 DDoS 공격보다 근원지 추적을 어렵게 하고, 다수의 반사체들이 희생자에게 다량의 트래픽을 보내게 하여 서비스 거부를 유발한다. 스마트 팜 및 스마트 팩토리 등과 같은 분야에 DR-DoS 공격이 발생 될 경우, IoT 기기가 오작동하여 IoT 시스템이 무력화되고, IT 자산피해 또한 발생할 수 있다. 따라서 IoT 네트워크에 DR-DoS 공격이 발생할 경우, 공격을 신속히 탐지해내고, 근원지 식별을 통해 복구 작업을 수행하는 것이 필요하다. 본 논문에서는 IoT 네트워크를 직접 구축하고, IoT 기기에 DR-DoS 공격을 주입하여 공격자, 반사체, 희생자 기기에서 공격을 탐지할 수 있는 딥러닝 모델을 개발한다.

본 논문의 구성은 다음과 같다. 2장에서는 최신 IoT 보안 관련 연구 동향을 살펴보고, 3장에서는 IoT 네트워크 구축 및 딥러닝을 위한 데이터셋(datasets) 수집 시나리오를 설계한다. 4장에서는 IoT 네트워크에 직접 DR-DoS 공격을 주입하여 데이터셋을 수집하고, 이를 RNN(Recurrent Neural Network) 및 LSTM(Long Short-Term Memory) 기반으로 학습하여 공격 여부 탐지하고, 근원지를 식

*Corresponding Author (jyk@daegu.ac.kr)

김지연: 대구대학교 컴퓨터정보공학부

<그림 5> 대한 임베디드 공학회 논문 투고