

2022.09.30

2022년도 한국정보보호학회 호남지부 추계학술대회

# RF를 활용한 트래픽 기반

# IoT 봇넷 공격 탐지 모듈 개발

전북대학교

대학생 김 강 민, 우 자 영

교수 장 재 우, 홍 득 조

# CONTENTS

## I. 서론

## II. 제안하는 시스템

1. 봇넷 공격 탐지 보안 시스템 구축
2. 공격 탐지 보안 모듈 구성
3. Feature 선정

## III. 결과

1. Mirai 탐지 및 악성 트래픽 전송
2. Mozi 탐지 확인
3. 시그니처 기반 탐지 도구(Snort)와 비교
4. 인터넷 성능 확인

## IV. 결론

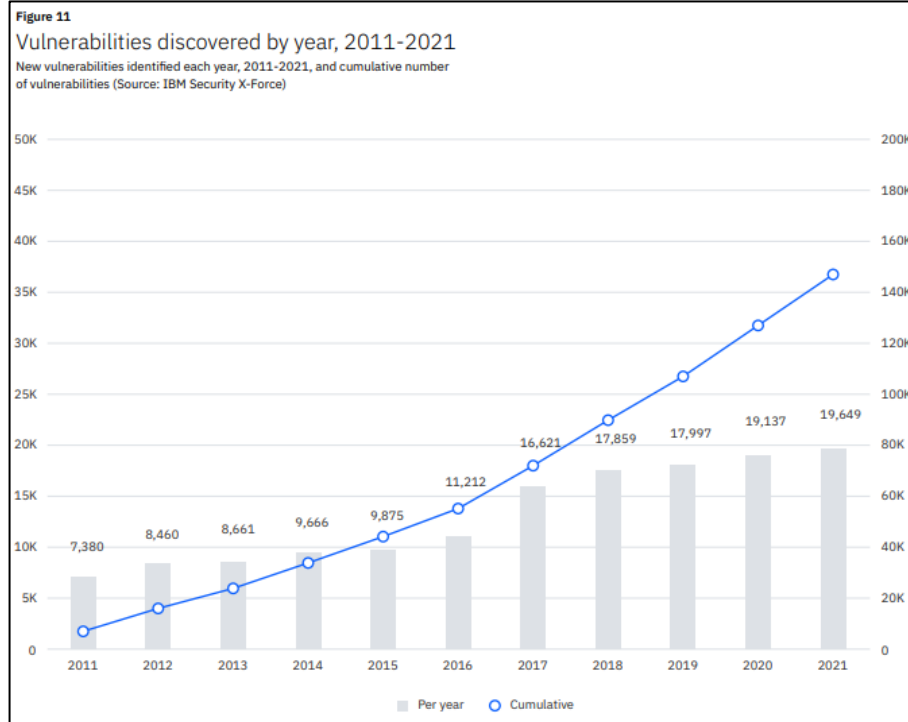
# 1. 서론

# I. 서론

2022년도 한국정보보호학회 호남지부 추계학술대회  
RF를 활용한 트래픽 기반 IoT 봇넷 공격 탐지 모듈 개발

## 1. 연구 필요성

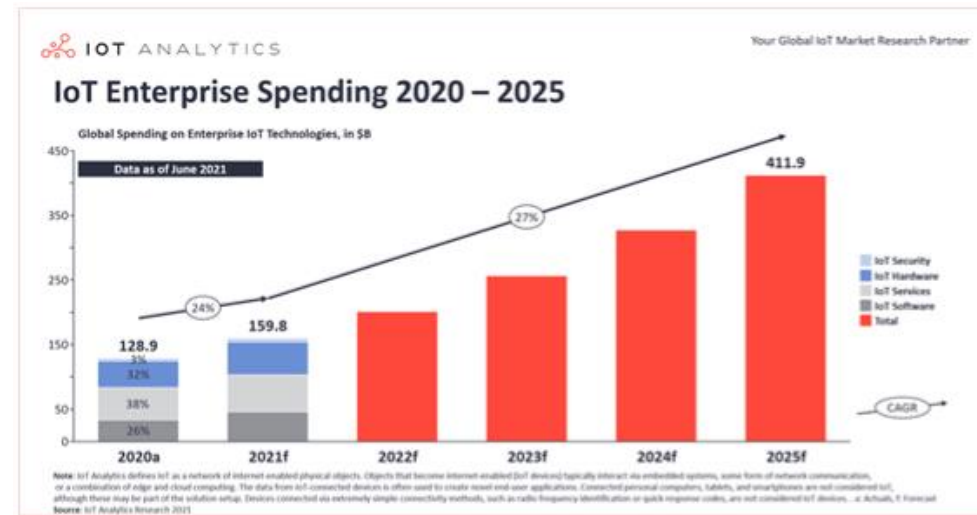
### IoT 시장의 급성장, 그에 따른 IoT 위협 증가



74%

Share of IoT attacks originating from Mozi botnet

In 2021, attacks against IoT devices originated from the Mozi botnet 74% of the time.



# I. 서론

## 1. 연구 필요성

## ■ AI를 활용한 악성 트래픽 분석 연구 현황

2022년도 한국정보보호학회 호남지부 추계학술대회

## RF를 활용한 트래픽 기반 IoT 봇넷 공격 탐지 모듈 개발

Journal of Digital Convergence  
Vol. 19, No. 5, pp. 462-468, 2022

ISSN 2713-6434 / eISSN 2713-6442  
https://doi.org/10.14400/JDC.2022.19.5.462

### IoT 네트워크에서 악성 트래픽을 탐지하기 위한 머신러닝 알고리즘의 성능 비교연구

현미진

경남대학교 교정융합대학 MSC교과부 교수

A comparative study of the performance of machine learning algorithms to detect malicious traffic in IoT networks

Mi-Jin Hyun

Professor, Division of Mathematics, Science, and Computers, Kyungnam University

**요약** IoT는 기술의 발전과 IoT 기기의 보급 및 서비스의 활성화로 폭발적인 증가세를 보이고 있지만, 최근 다양한 봇넷의 활동에 의해 심각한 보안 위험과 재정적 피해가 발생하고 있다. 따라서 이러한 봇넷의 활동을 정확하고 빠르게 탐지하는 것이 중요하다고 할 수 있다. IoT 환경에서의 보안은 최소한의 프로세스 성능과 메모리 운영을 해야 하는 특성이 있는 만큼, 본 논문에서는 탐지를 위한 최소한의 특징을 선택하고, KNN(K-Nearest Neighbor), Naive Bayes, Decision Tree, Random Forest와 같은 머신러닝 알고리즘이 봇넷의 활동을 탐지하는 성능을 비교연구 하였다. Bot-IoT 데이터셋을 사용한 실험 결과는 저명한 머신러닝 알고리즘 중 KNN이 DDoS, DoS, Reconnaissance 공격을 가장 효과적이고 효율적으로 탐지할 수 있음을 보여주었다.

**주제어** : 사물인터넷, 봇넷, 머신러닝, 보안, 데이터넷

**Abstract** Although the IoT is showing explosive growth due to the development of technology and the spread of IoT devices and activation of services, serious security risks and financial damage are occurring due to the activities of various botnets. Therefore, it is important to accurately and quickly detect the activities of these botnets. As security in the IoT environment has characteristics that require operation with minimum processing performance and memory, in this paper, the minimum characteristics for detection are selected, and KNN (K-Nearest Neighbor), Naive Bayes, Decision Tree, Random Forest and other machine learning algorithms such as Forest to detect botnet activity. Experimental results using the Bot-IoT dataset showed that KNN can detect DDoS, DoS, and Reconnaissance attacks most effectively and efficiently among the applied machine learning algorithms.

**Key Words** : IoT, Botnet, Machine Learning, Security, Data Sets

\*This work was supported by Kyungnam University Foundation Grant in 2020.

\*Corresponding Author : Mi-Jin Hyun(mjhyun@kyungnam.ac.kr)  
Received August 31, 2021  
Accepted September 20, 2021  
Revised September 20, 2021  
Published September 20, 2021

한국정보과학회

2020년 한국컴퓨터종합학술대회 논문집

ERIC  
교육연구정보원

### GRU와 LSTM을 이용한 Mirai 봇넷 공격 탐지 연구

홍정훈<sup>1)</sup> 정성민<sup>2)</sup>

<sup>1)</sup>성균관대학교 공학대학원  
<sup>2)</sup>성균관대학교 소프트웨어대학

hongjinhun@gmail.com, tchongshin@skku.edu

### Research on Mirai Botnet Attack Detection Using GRU and LSTM

Kyungul Bae<sup>1)</sup> Taemyeong Chung<sup>2)</sup>

<sup>1)</sup>Department of Computer Science and Engineering, Sungkyunkwan University

<sup>2)</sup>College of Computing, Sungkyunkwan University

### 요약

5세대 통신 기술의 발전으로 많은 IoT 기기가 초고속 네트워크로 연결되는 특성을 가지고 다각도로 있으며 이에 따라 IoT 및 관련 사물에 대한 수요가 증가할 것으로 많은 전문가들이 예측한다. 대규모 분산 악성 IoT 기기는 네트워크의 정보 수송 및 네트워크 연결 정도의 영향을 유발 할 것으로 치명적 지능 네트워크 설계와 암호화 등의 정보보호 솔루션을 탐지하기 어렵다. 본 논문에서는 악성 IoT 기기의 보안 솔루션의 도입은 매우 필요하다. 본 연구에서는 최근 사물에 큰 영향을 미친 악성 IoT 기기의 Mirai 봇넷의 공격에 대한 탐지를 위한 GRU와 LSTM의 특징 분석(feature selection)을 통한 공격 탐지 모듈을 제시하고, 순환신경망 (RNN) 계열인 Gate Recurrent Unit (GRU)과 Long Short-Term Memory(LSTM) 기법을 통한 공격 탐지 성능을 제안한다.

### 1. 서론

DDoS 공격은 공격자가 다수의 기기를 감염시킨 뒤에 이들에게 명령을 내려 공격 대상 서버에 일제히 접속을 명령해 대대적으로 공격하기는 공격이다. 다수의 기기가 존재하며 보안에 취약한 IoT 기기들은 공격자들의 표적이 되기 쉬우며 IoT 기기가 증가하는 현재 사회에 더욱 위험적이다. Static의 조사에 따르면 2025년까지 약 750대의 IoT 기기가 서로 네트워크상 연결 될 것으로 예상된다. [1] 이에 DDoS 공격의 위험은 더욱 커질 것으로 보인다.

최근에 등장한 비파괴 분석은 IoT 기기를 주 공격 대상으로 삼고 있으며 해당 기기를 좀비로 만들어 공격자가 자유롭게 제어할 수 있도록 하는 봇넷의 활용이다. 공격자는 봇넷을 통해 DDoS 공격을 감행하게 된다. 2016년 10월 다수의 DNS 기기를 관리하는 Dyn 사의 대규모 공격이 감행되었다. 이로 인해 트위터(twitter), 가디언(The Guardian), 넷플릭스(Netflix), 레딧(Reddit), CNN 등 미국과 유럽 여러 기업들의 서비스가 마비되었다. 비파괴 분석은 오키우, 예코보(EchoBot) 등 새로운 형태로 진화하며 발전된 형태의 공격을 진행하고 있다. 이에 비파괴 분석의 공격에 대한 대비가 필요하다고 보인다.

현재 IoT 기기의 보안은 취약하다. 저전력, 저성능으로 설계된 IoT 기기는 많은 에너지, 메모리 제한을 가지므로 현재 개발된 고전력·고성능 연산계

적합한 보안 알고리즘은 IoT 기기들에 적합하지 않다. [2] 이로 인해 이에 따라 현재 다수의 IoT 기기들이 비파괴 분석의 공격 위험에 노출된 상태로 인 터넷상에 연결되어 있다. 이러한 여러 이유로 본 연구에서는 비파괴 분석의 공격 탐지 방안 제안을 제안한다. 본 논문에서는 각 특징들을 선택한 타당성 근거에 대해 제시하고 순환 신경망(RNN) 계열인 기법을 통한 공격 탐지 방안을 제안한다. 장기적으로 누적되는 패킷 데이터의 학습을 위한 Long Short-Term Memory (LSTM) 기법과 실시간으로 빠른 분석 결과물 얻기 위한 Gate Recurrent Unit (GRU) 기법을 사용하여 공격 탐지를 진행하였다.

### 2. 관련연구

#### 2.1. LSTM

기존의 RNN 모델은 그라디언트 소실 및 폭주(Vanishing and exploding gradient)의 문제가 크며 장기적인 패턴에 대해 학습이 어렵다는 문제점을 가지고 있다. RNN의 계열 중 최근 LSTM은 셀레 게이트들을 추가함으로써 전 순차적인 정보를 저장하도록 개선되었다. [3] 데이터가 계속해서 누적되는 패킷 데이터의 특성상 장기적인 패턴의 학습은

한국정보보호학회 하계학술대회 논문집 Vol.32, No. 1

### 이종 IoT 데이터셋에 대한 기계 학습 기반 악성 트래픽 탐지 성능 분석

박지훈<sup>1)</sup>, 박수현<sup>2)</sup>, 홍해민<sup>3)</sup>, 김성민<sup>4)</sup>

<sup>1)</sup>성신여자대학교(학부생), 성신여자대학교(학부생), 성신여자대학교(학부생), 성신여자대학교(학부생), \*성신여자대학교(교수)

Machine Learning-Based Malicious Traffic Detection Performance Analysis for Heterogeneous IoT Datasets

Ji-Eun Park<sup>1)</sup> Su-Hyun Park<sup>2)</sup> Hye-Min Hong<sup>3)</sup> Hae-Dam Kim<sup>4)</sup> Seong-Min Kim<sup>5)</sup>

\*Sungshin Women's University(Undergraduate student), Sungshin Women's University(Undergraduate student), Sungshin Women's University(Undergraduate student), Sungshin Women's University(Undergraduate student), \*Sungshin Women's University(Professor)

### 요약

병적 클라우드의 등장과 5G 네트워크의 보편화에 따라 IoT 기기의 수는 폭발적으로 증가하고 있으며, IoT 기기의 보안 취약점을 이용한 공격 또한 증가하고 있다. 이에 대응 기술 IoT 기기를 대상으로 한 공격에 대한 학습 기반 악성 트래픽 탐지 기술이 주목을 받고 있다. 그러나 일반 네트워크 기반 학습 탐지와 달리 IoT 환경은 홈 네트워크, 스마트 공장 등 다양한 데이터 시리오는 일제적인 침입과 사물 등의 데이터 존재한다. 본 논문에서는 이종 IoT 데이터가 포함된 TCP, UDP 프로토콜에서 공통된 패킷 속성을 통해 IoT 기기를 대상으로 한 학습 기반 악성 트래픽 탐지 성능을 분석하였다. 랜덤 포레스트, 커널결정 트리, 서포트 벡터 머신 등 기계 학습 알고리즘의 성능을 비교 분석한 결과, IoT 기기의 제각각인 환경을 고려하여 이종 데이터셋으로부터 일부 피해에 대한 추측만으로도 효과적인 악성 트래픽 탐지가 가능함을 확인하였다.

주제어 : 사물인터넷(IoT), 보안, 네트워크, 적정 트래픽 탐지, 데이터셋, 기계 학습 알고리즘

### I. 서론

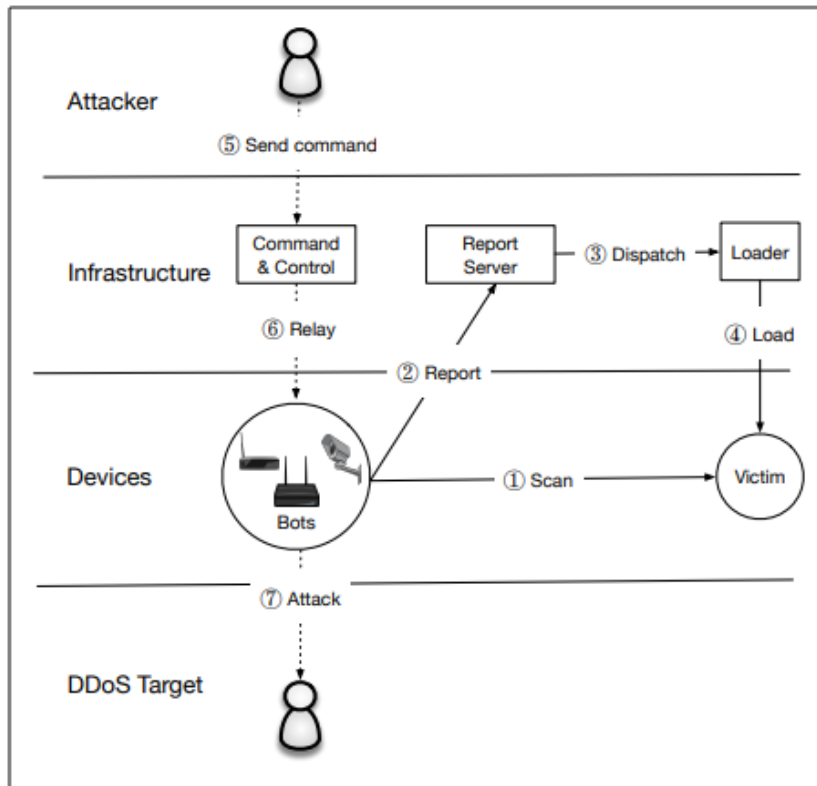
사물인터넷(IoT) 기기의 사용자가 증가함에 따라 IoT 기기의 보안 취약점으로 인해 주목받기 시작했다. IoT 기기의 경우 홈 네트워크와 같이 사용자 및 일반 환경에서 구동됨에 따라, 기기 사용자들의 생활에 유출될 수 있다는 문제가 존재한다. 대표적인 사례로, 2011년 11월 밤에 70여 개 아파트 단지 백엔드가 당도되는 침묵으로 연구가 수행되었다. 그러나 일반 네트워크 기반 학습 탐지와 달리 IoT 환경은 홈 네트워크, 스마트 공장 등 다양한 데이터 시리오는 일제적인 침입

보 및 사생활과 더욱 밀접한 데이터들은 다루기에 대한 취약점을 탐지하는 것은 시급한 문제이며, 이를 위해 네트워크 단에서 IoT 기기를 대상으로 한 공격에 대한 학습 기반 악성 트래픽 탐지 기술이 주목을 받고 있다. 일제적인 데이터는 기계 학습으로 모든 측면에서 성능을 어떻게 한 것인지, 알고리즘 자체를 어떻게 개선할지에 대한 분석을 많은 방향으로 연구가 수행되었다. 그러나 일반 네트워크 기반 학습 탐지와 달리 IoT 환경은 홈 네트워크, 스마트 공장 등 다양한 데이터 시리오는 일제적인 침입

# I. 서론

## 1. 연구 필요성

### ■ 기존 연구의 이분법적 분류



#### ① 취약한 기기 Scan

Master Bot이 취약한 IoT 기기를 Scan 한다.

#### ② Loader로 정보 전달

Master Bot이 취약한 기기에 접속하고 Loader로 해당 정보를 전달한다.

#### ③ 악성코드 다운로드 및 실행

Loader에서 wget 명령어를 통해 C&C 서버에서 취약한 기기로 악성코드 다운 및 실행한다.

#### ④ C&C 서버와 통신

감염된 기기는 C&C 서버의 명령을 대기한다.

➔ 다양한 행동을 하나의 유형으로 분류하는 것은 트래픽의 특징을 모호하게 만들 수 있음

# I. 서론

2022년도 한국정보보호학회 호남지부 추계학술대회

## RF를 활용한 트래픽 기반 IoT 봇넷 공격 탐지 모듈 개발

### 1. 연구 필요성

#### ■ 데이터셋에서의 학습 및 검증

##### 3.1 BoT-IoT 데이터셋

본 논문에서 IoT 네트워크에서 악성 트래픽의 탐지 성능을 측정하기 위하여 BoT-IoT 데이터셋[18]을 사용하였다. IoT에서 봇넷 탐지를 위하여 필요한 IoT trace에 대한 충분한 정보가 포함된 데이터셋이다.

##### 3.1.1 IoT-23

IoT-23 데이터셋[2]은 Philips HUE 스마트 LED 램프, Amazon Echo 홈 지능형 개인 비서 및 Somfy 스마트 도어록의 세 가지 IoT 장치에서 네트워크 트래픽을 캡처하였고 DDoS, Mirai, Okiru, C&C 서버, 포트 스캔 공격을 포함하고 있다.

##### 3.1.2 Bot-IoT

Bot-IoT 데이터셋[3]은 일반 트래픽과 봇넷 트래픽의 조합을 통한 환경에서 수집되었다. DDoS, DoS, OS 및 서비스 스캔, 키로깅 및 데이터 유출 공격이 포함되며 사용된 프로토콜을 바탕으로 DDoS 및 DoS 공격이 수행되었다.

##### 3.2. 데이터셋

본 연구에 사용되는 데이터는 공개되어있는 미라이 봇넷 공격 데이터를 사용한다. [6] 본 데이터는 SKT NUGU (NU 100) 와 EZVIZ Wi-Fi Camera (C2C Mini O Plus 1080P)에서 취합된 패킷 데이터이다. 모두 무선 네트워크 환경에서 전달받은 패킷이며 노트북, 스마트폰이 같은 무선 네트워크 환경에 접속하여 데이터를 수집되었다. 총 1,748,870개의 패킷으로 이루어져 있으며 이 중 공격자가 송신한 패킷은 1,035,380개로 이루어져 있다.

➔ 기존의 데이터셋 뿐만 아니라 실제 환경에서의 검증, 봇넷 특징에 맞는 feature 선정 필요

# I . 서론

2022년도 한국정보보호학회 호남지부 추계학술대회  
RF를 활용한 트래픽 기반 IoT 봇넷 공격 탐지 모듈 개발

## 2. 본 논문의 특징

### ■ Scan 행위 초점에 맞춘 트래픽 검증

- Scan은 감염 되기 전/후로 발생
- 봇넷의 특성 상 Scan을 하는 행위는 지속적으로 발생
- 외부에서 AP로 들어오는 Scan/감염 후, 내부에서 외부로 나가는 Scan 분리

➔ Scan이라는 행위에 초점을 맞춰 특징을 명확히 함으로써 탐지율을 높이하고자 함



# I . 서론

2022년도 한국정보보호학회 호남지부 추계학술대회  
RF를 활용한 트래픽 기반 IoT 봇넷 공격 탐지 모듈 개발

## 2. 본 논문의 특징

### ■ 실제 네트워크 트래픽 환경에서의 학습 및 검증

- 폐쇄망에서 Github에 공개된 Mirai 악성코드를 기반으로 컴파일해 데이터 수집
- 정상 트래픽은 실제 사용중인 환경의 트래픽을 수집
- Mirai 악성코드를 분석해 Feature를 선정
- Mirai 악성코드 뿐만 아닌 변종인 Mozi 악성코드의 탐지도 검증

➔ 데이터 셋이라는 제한적인 환경을 극복하고자 함

## 2. 제안하는 시스템

2.1. 봇넷 공격 탐지 보안 시스템 구축

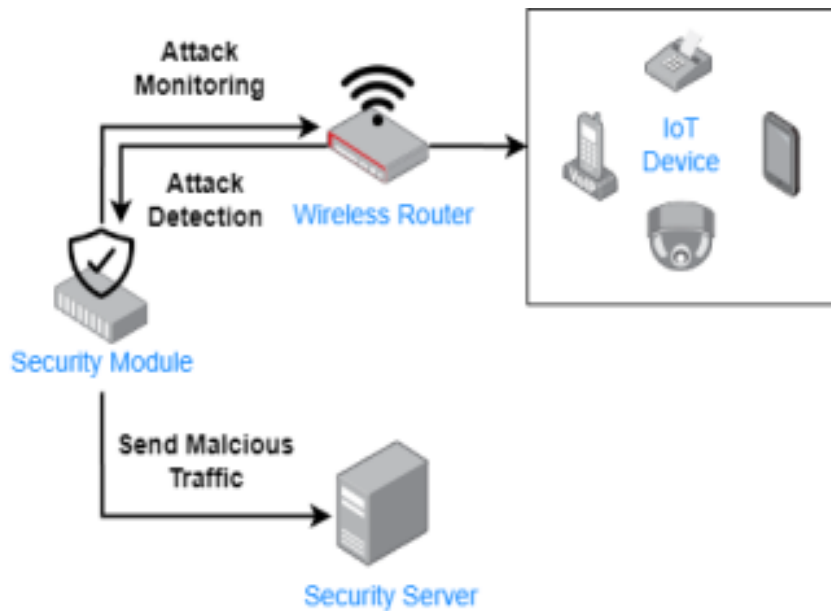
2.2. 공격 탐지 보안 모듈 구성

2.3. Feature 선정

# II. 제안하는 시스템

2022년도 한국정보보호학회 호남지부 추계학술대회  
RF를 활용한 트래픽 기반 IoT 봇넷 공격 탐지 모듈 개발

## 1. 봇넷 공격 탐지 보안 시스템 구축



### ■ System Configuration Diagram

- 무선 환경을 고려해 트래픽을 수집할 수 있게 Router 앞 단에 Bridge 형태 구축
- 10분마다 지속적으로 트래픽을 모델에게 전송
- 모델이 악성 트래픽을 탐지할 경우 보안 서버로 해당 트래픽을 전달하여 이를 분석
- 차단이 아닌 탐지에 초점을 두어 네트워크 속도 저하 방지

# II. 제안하는 시스템

## 2. 모듈 내의 학습 모델 선정

Journal of Digital Convergence  
Vol. 19. No. 9, pp. 463-468, 2021

ISSN 2713-6434 / eISSN 2713-6442  
<https://doi.org/10.14400/JDC.2021.19.9.463>

### IoT 네트워크에서 악성 트래픽을 탐지하기 위한 머신러닝 알고리즘의 성능 비교연구

현미진  
경남대학교 교양융합대학 MSC교육부 교수

2022년도 한국정보보호학회 호남지부 추계학술대회

RF를 활용한 트래픽 기반 IoT 봇넷 공격 탐지 모듈 개발

## ■ Random Forest

- 속도를 고려해 딥러닝 모델대신 머신러닝 모델을 선정
- 머신러닝 알고리즘의 봇넷 탐지 성능을 비교한 연구 존재  
=> KNN, Random Forest가 성능이 좋은 것으로 연구
- Random Forest는 Feature 중요도 확인 가능

## II. 제안하는 시스템

2022년도 한국정보보호학회 호남지부 추계학술대회  
RF를 활용한 트래픽 기반 IoT 봇넷 공격 탐지 모듈 개발

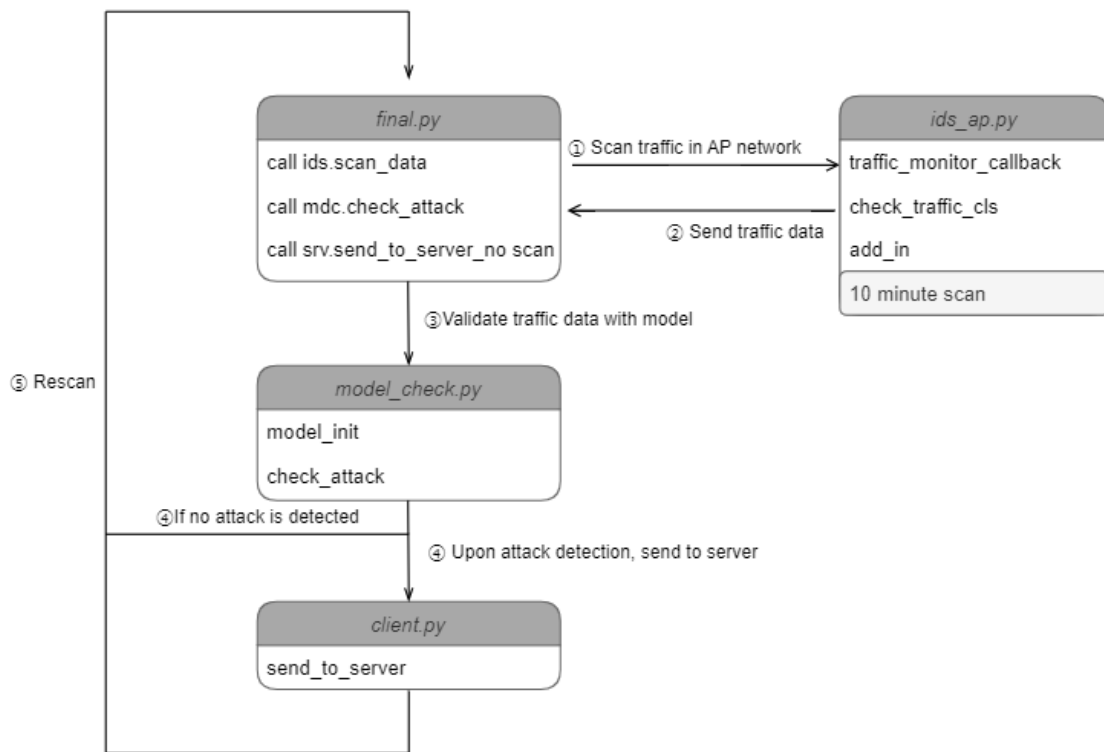
### 3. Feature 선정

Feature	Description
weak_port	공격이 접근하는 취약한 port
proto	Protocol 종류
length	패킷의 길이
flag	패킷의 TCP 플래그
total_length	특정 IP의 전체 패킷의 길이
time	동일한 목적의 패킷 전송 시간
datarate	동일한 목적의 패킷 전송 속도
cnt	Host로의 접근 횟수

## II. 제안하는 시스템

2022년도 한국정보보호학회 호남지부 추계학술대회  
RF를 활용한 트래픽 기반 IoT 봇넷 공격 탐지 모듈 개발

### 4. 공격 탐지 보안 모듈 구성



### ■ Security Module

- python의 scapy 패키지를 활용해 트래픽 수집
- 무선 네트워크 트래픽 패킷을 10분 단위로 수집
- 수집된 트래픽은 자식 프로세스로 모델에서 검증  
=> 자식 프로세스를 통해 트래픽 수집의 딜레이를 줄임
- 악성 트래픽이 특정 수 이상 검증이 되면 서버로 전송

## 3. 결과

- 3.1. Mirai 탐지 및 악성 트래픽 전송
- 3.2. Mozi 탐지 확인
- 3.3. 시그니처 기반 탐지 도구(Snort)와 비교
- 3.4. 인터넷 성능 확인

# III. 결과

## 1. Mirai 탐지 및 악성 트래픽 전송

### ■ 모델의 트래픽 분류 방법

1. Attack 0 (Normal) : 정상적인 트래픽을 의미
2. Attack 1 (Scan IN): 호스트 AP로 들어오는 Scan 트래픽
3. Attack 2 (Scan OUT): 이미 감염된 네트워크 내부의 기기가 호스트 AP 외부로 Scan 하는 경우

```
[*]Finish Botnet Attack Detection  
Attack 0 (Normal): 46  
Attack 1 (Scan IN): 871  
Attack 2 (Scan OUT): 7
```

- scan IN

```
[*]Finish Botnet Attack Detection  
Attack 0 (Normal): 313  
Attack 1 (Scan IN): 13  
Attack 2 (Scan OUT): 21023
```

- scan OUT

➔ 폐쇄망에서 Mirai Scan만 확인했을 때, IN의 F1 점수는 0.96, Scan OUT의 F1 점수는 0.97로 측정



# III. 결과

2022년도 한국정보보호학회 호남지부 추계학술대회  
RF를 활용한 트래픽 기반 IoT 봇넷 공격 탐지 모듈 개발

## 2. 시그니처 기반 탐지 도구(Snort)와 비교

### ■ Signature for Snort

- IIR에서 제시한 snort 룰을 사용하여 탐지 여부를 비교
- 룰은 Bot 등록, Bot Download, Bot을 통한 명령어 실행 등 다양
- Mirai 봇넷 공격 과정 중 Loader의 wget을 이용한 Download만이 탐지

➔ 현재 이루어지는 시그니처 기반 탐지는 변화 대응이 힘들

#### 1. Infrastructure Security

#### Mirai Botnet Detection and Countermeasures

```
- Bot registration and heartbeat
alert tcp any any -> any 23 (msg:"Mirai Botnet: Register Bot with C&C"; flow:to_server,established; content:"j00 00 00 01"; depth:4; sid:1000000; rev:1)
alert tcp any any -> any 23 (msg:"Mirai Botnet: Send Heartbeat from Bot to C&C"; flow:to_server,established; content:"j00 00"; depth:2; pcre:"/^x00x00$/m";
sid:1000001; rev:1)
alert tcp any 23 -> any any (msg:"Mirai Botnet: Reply Heartbeat from C&C to Bot"; flow:from_server,established; content:"j00 00"; depth:2; pcre:"/^x00x00$/m";
sid:1000002; rev:1)

- Bot downloader download
alert tcp any any -> any [23,2323] (msg:"Mirai Botnet: Download Bot Downloader via Telnet (echo)"; flow:to_server,established; content:"echo-ne "; content:" " > upnp[3b]
/bin/busybox ECCHI"; sid:1000060; rev:1)

- Bot binary download command execution
alert tcp any any -> any [23,2323] (msg:"Mirai Botnet: Download Bot binary via Telnet (wget)"; flow:to_server,established; content:"/bin/busybox wget http://";
content:"/bins/mirai."; content:"-O -> dvrHelper[3b] /bin/busybox chmod 777 dvrHelper[3b] /bin/busybox ECCHI"; sid:1000070; rev:1)
alert tcp any any -> any [23,2323] (msg:"Mirai Botnet: Download Bot binary via Telnet (tftp)"; flow:to_server,established; content:"/bin/busybox tftp "; content:"-g -l
dvrHelper -r mirai."; content:"/bin/busybox chmod 777 dvrHelper[3b] /bin/busybox ECCHI"; sid:1000071; rev:1)

- Bot binary download communications
alert tcp any any -> any 80 (msg:"Mirai Botnet: Download Bot binary via HTTP"; flow:to_server,established; content:"GET /bins/mirai."; pcre:"/^GET
/bins/mirai\.(arm|arm7|m68k|mps|mpsl|ppc|sh4|spc|x86) HTTP/1\.[01][0d 0a]$/mi"; sid:1000080; rev:1)
alert udp any any -> any 69 (msg:"Mirai Botnet: Download Bot binary via TFTP"; flow:to_server; content:"j00 01|mirai."; pcre:"/^x00x01mirai\.(arm|arm7|m68k|mps|mpsl|ppc|sh4|spc|x86)x00.+$/mi"; sid:1000081; rev:1)

- Bot execution
alert tcp any any -> any [23,2323] (msg:"Mirai Botnet: Run Bot binary (upnp & dvrHelper)"; flow:to_server,established; content:"/upnp[3b] /dvrHelper telnet.";
content:"/bin/busybox IHCE"; pcre:"/^\\Vupnp; \\VdvrHelper telnet\.(arm|arm7|m68k|mps|mpsl|ppc|sh4|spc|x86); \\Vbin/busybox IHCE$/m"; sid:1000090; rev:1)
alert tcp any any -> any [23,2323] (msg:"Mirai Botnet: Run Bot binary (dvrHelper)"; flow:to_server,established; content:"/dvrHelper telnet\.(arm|arm7|m68k|mps|mpsl|ppc|sh4|spc|x86); \\Vbin/busybox IHCE$/m";
pcre:"/^\\VdvrHelper telnet\.(arm|arm7|m68k|mps|mpsl|ppc|sh4|spc|x86); \\Vbin/busybox IHCE$/m"; sid:1000091; rev:1)
```

IIR (Internet Initiative Japan)

일본 인터넷 서비스 제공업체

# III. 결과

## 3. Mozi 탐지 확인

### ■ Detection Mozi

```
[*]Finish Botnet Attack Detection
Attack 0 (Normal): 410
Attack 1 (Scan IN): 9
Attack 2 (Scan OUT): 23038
```

Dateadded (UTC)	Malware URL	Status	Tags	Reporter
2022-09-21 08:10:05	<a href="http://81.35.202.169:39769/i">http://81.35.202.169:39769/i</a>	Online	hajime	@geenensp
2022-09-21 08:08:04	<a href="http://188.149.161.176:40941/bin.sh">http://188.149.161.176:40941/bin.sh</a>	Online	32-bit elf mips Mozi	@geenensp
2022-09-21 08:04:05	<a href="http://60.179.235.123:37738/i">http://60.179.235.123:37738/i</a>	Online	32-bit arm elf Mozi	@geenensp
2022-09-21 08:03:06	<a href="http://163.123.143.4/WW/traff.exe">http://163.123.143.4/WW/traff.exe</a>	Online	dropby PrivateLoader	@andretavare5
2022-09-21 07:59:10	<a href="http://222.241.51.27:39971/i">http://222.241.51.27:39971/i</a>	Online	hajime	@geenensp
2022-09-21 07:59:05	<a href="http://178.208.167.60:50922/i">http://178.208.167.60:50922/i</a>	Online	32-bit arm elf mirai Mozi	@geenensp
2022-09-21 07:58:16	<a href="http://106.60.35.6:47056/i">http://106.60.35.6:47056/i</a>	Online	hajime	@geenensp
2022-09-21 07:58:06	<a href="http://117.215.213.15:36035/bin.sh">http://117.215.213.15:36035/bin.sh</a>	Online	32-bit elf mips Mozi	@geenensp

- Mozi 샘플 : 분석용 악성코드 샘플 다운로드 사이트인 URLhaus에 샘플 획득
- 폐쇄망 환경에서 보안 모듈이 Mozi를 탐지하는 것 확인 완료

# III. 결과

## 4. 인터넷 성능 확인

공격 탐지 시스템의 보안 모듈이 공유기와 브리지로 연결되어 있기 때문에, KT 인터넷 속도 테스트로 인터넷 성능을 확인

- 보안 모듈을 설치한 경우
  - 10회 측정한 평균값의 다운로드 속도는 42Mbps, 업로드 속도는 49Mbps
- 모듈을 설치하지 않은 경우,
  - 다운로드 속도는 38Mbps, 업로드 속도는 57Mbps

➔ 두 경우가 유사한 결과를 보임

※ 구현코드 <https://github.com/wja0/IoT-Botnet-Attack-Detection-Module>



## 4. 결론

# IV. 결론

- Scan하는 행위에 초점을 맞춰 트래픽의 특징을 명확하게 함
- 데이터셋에만 의존한 기존 연구에서 벗어나 실제 환경에서 탐지되는 학습 모델을 개발
- Mozi 악성코드가 탐지 가능
- 모듈이 인터넷 속도에 큰 영향을 주지 않음
- 브리지 형태의 연결 방식으로 더욱 정교한 모델이 만들어질 경우, 모델 교체만으로 대응 가능

2022.09.30

# 감사합니다

발표 경청해 주셔서 감사합니다.

전북대학교

대학생 김 강 민, 우 자 영

교수 장 재 우, 홍 득 조