DU-도전학기 결과보고서

과제명	주요기반시설의 IoT 취약점 분석 및 보안 솔루션 개발		
참여자	성명	소속	학번
	조	컴퓨터공학전공	
	김	컴퓨터공학전공	
	박	컴퓨터공학전공	
	이	컴퓨터공학전공	
지도교수 의견	상기 학생들은 도전학기 목표를 달성하고자 주 3-4회씩 모여서 실험하였고, 그 결과 의미있는 결과가 도출되어 학술대회 논문으로도 2편을 발표하였습니다. 두 편 모두 연구 내용의 우수성을 인정받아서 우수논문상을 수상하였으며 그 중, 한 편은 한국연구재단등재지 급의 논문지 게재를 추천받아 현재 확장 연구를 수행하고 있습니다. 참가 학생들의 최고의 팀워크와 열정으로 이루어낸 성과라고 생각하며 실험환경 구축 비용, 학술대회 참가비 및 교통비 등을 지원해주시고, 좋은 성과낼 수 있도록 기회를 제공해주신 대학혁신지원사업단에도 감사드립니다. (소속) 컴퓨터공학전공 (성명) (서명 또는 날인)		

1. 도전 과제 내용

주요 기반시설(Critical Infrastructure)은 외부 공격으로 인해 점령, 파괴 또는 기능이 마비될 시 국가 경제와 안보에 큰 영향을 미치는 중요한 시설이다. 이러한 주요 기반시설을 목적으로 하는 악의적인 사이버 공격의 횟수가 증가하고 있다. 최근 발생하는 사이버 공격의 경우 기존의 공격 탐지방식으로는 탐지하는 데 있어 어려움이 존재한다. 본 팀은 주요 기반시설에 포함되는 도로 시설 중에서 어린이 보호 구역에 초점을 두어 어린이 보호 구역 환경에서 발생하는 사이버 공격에 대한 조사 및 공격이 발생했을 경우 시설에 대한 공격 데이터 및 정상 데이터를 수집하였다. 수집한 공격 및 정상 데이터를 기반으로 사이버 공격의 탐지 방법에 대해 제안하는 것을 주제로 도전 학기를 진행하였다.

2. 도전 과제 수행 결과 및 성과

이번 도전 학기의 주제는 주요 기반시설의 IoT 취약점 분석 및 보안 솔루션 개발이었다. 다음과 같은 주제를 진행하기 위해서 크게 7가지의 분야로 나누어 진행하였다.

<표 1> 도전 학기 진행 분야

	내용
진행 분야	IoT의 취약점 조사
	실험 환경 구축
	구축 환경 테스트
	공격 선정 및 공격 시나리오 제작
	구축 환경에 실시간 공격 주입 및 공격 데이터 수집
	수집한 데이터 비교 및 분석
	논문 작성 및 학회 참여

각 진행 분야는 팀원끼리 적절히 나누어 진행하였다.

o IoT의 취약점 조사

IoT의 취약점 조사는 팀원 전체가 진행하였다. IoT 취약점의 경우에는 다양한 논문 및 저널에서 찾아보았으며 IoT에서 발생할 수 있는 공격의 종류 및 공격 방식은 <표2> 와 같다.

<표 2> IoT에서 발생할 수 있는 공격의 종류 및 공격 방식

공격 종류	방식
봇넷 멀웨어를 통한 공격	o Mirai, Mozi, Satory 등의 악성코드를 통해 IoT기기들을 감염시켜 사진 및 동영상이 임의로 유출하거나 제어하거나 DDoS같은 공격들을 실행
무선신호 교란	o IoT 서비스는 ZigBee, WIFI, Z-Wave와 같은 무선통신 기술을 통해 데이터를 전송하는데 공격자는 Noise, 동일 주파수 사용, 주파수 위변조를 통해 실제 신호의 정상적인 송수신을 방해
DoS, DDoS	o 주변 node에 지속적이고 반복적으로 광고 패킷 송신, 메시지 반복 전송으로 시스템 부하 가중시킴, 주파수 Jamming으로 서비스 방해
데이터 변조	o 엔드 포인트 간 송수신 데이터를 변조하거나, 암호화되지 않는 node와 Gateway 간의 정보를 도청
가짜 디바이스 접속	o 인가되지 않는 가짜 사물 인터넷 기기를 네트워크에 접속시켜 노드 간 데이터를 스푸핑 하여 도청하거나 과도한 트래픽을 발생시킴
평문메시지 분석	o 한정된 리소스로 통합된 암호화 기술의 적용이 어렵다는 취약점을 노린 방법으로, 암호화되지 않은 패킷을 찾아내어 공격함
리소스 소모	o 저속의 CPU나 한정된 메모리 그리고 소형배터리 등의 리소스를 소모하는 방법으로 과도한 패킷의 전송이나 연산을 유도하여 IoT 기기가 정상 동작하지 않도록 공격

또한, 실제 IoT를 목적으로 한 공격 사례에 대해서도 조사를 진행하였으며 IoT 공격 사례와 보안 위협의 경우는 <표3>에서 확인할 수 있다.

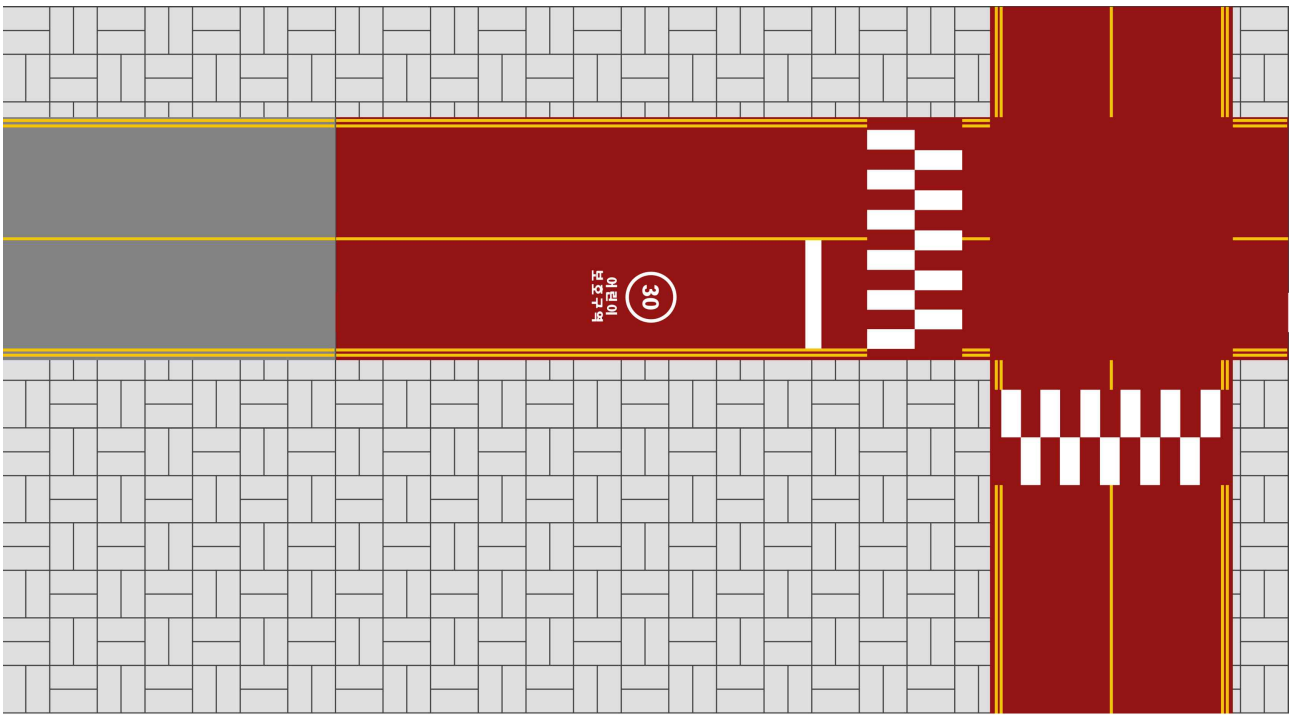
<표 3> IoT 공격 사례 및 보안 위협

종류	보안 위협
홈캠, 네트워크 카메라 등	o 공격자에 의해 사진 및 동영상이 임의로 유출하거나 제어 당하는 등의 사생활 침해 위험
IoT 빅데이터 해킹	o IoT에 저장된 많은 데이터가 있는 데이터 저장소가 공격받을 시 이에 저장된 여러 민감한 개인정보 유출 위험
IoT를 통한 홈네트워크 침입	o 홈네트워크 침입을 통해서 장치를 사용하는 개인의 신상과 금융 정보를 훔치거나 다른 장치, 전화 또는 컴퓨터를 제어당함
Mozi같은 악성코드를 통한 공격	o CCTV, 영상 녹화 장비 등을 통해 악성코드가 자가 증식 o HTTP 공중 납치와 MITM등의 방식으로 넷기어, D-Link, 화웨이 같은 라우터에 취약한 지점에 침투 o 이를 통해 인터넷 서버를 무력화시키는 DDoS 공격까지도 가능함

o 실험 환경 구축

IoT의 취약점을 조사함과 동시에 팀원 전체가 실험 환경 구축을 진행하였다. 실험 환경 구축을 위해서는 팀원끼리 나누어 진행하였으며 각 팀원의 역할 분담은 다음과 같다.

o 조 : 실험 환경인 어린이 보호 구역의 제작을 위해 어린이 보호 구역에 대해 조사를 진행하였으며 조사한 내용을 기반으로 어린이 보호 구역 초안을 제작하였음.

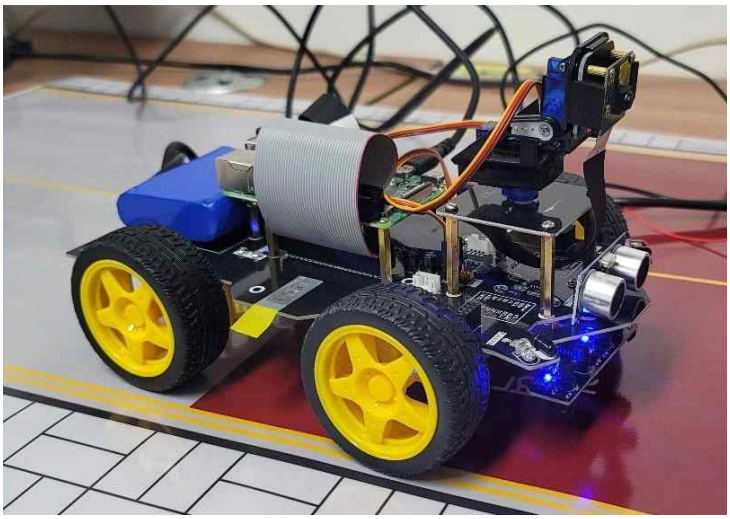


[그림 1] 어린이 보호 구역 제작을 위한 도로 초안

제작한 초안을 기반으로 어린이 보호 구역을 제작하였음.

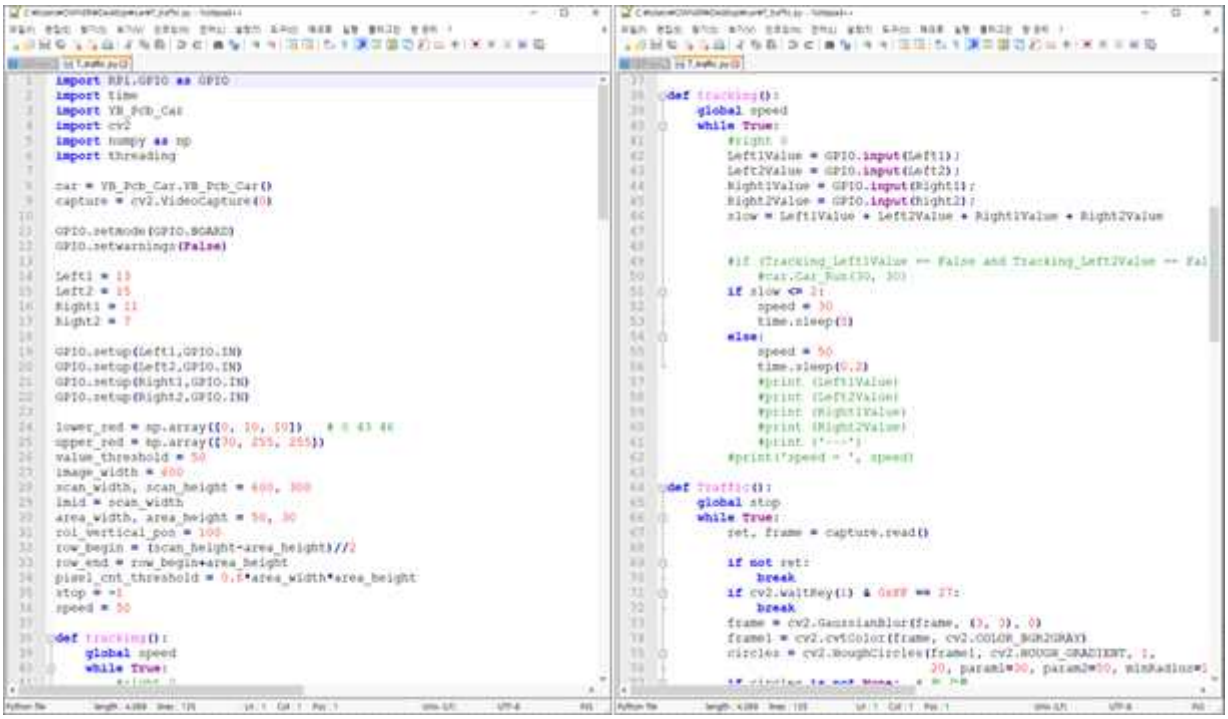
[그림 2] 실제 제작한 어린이 보호 구역 이미지

o 김 : 어린이 보호 구역에서 작동하는 자율 주행차의 제작을 진행하였으며, 이 팀원을 도와 자율 주행차 코드 작성을 진행하였음.



[그림 3] 제작한 자율 주행 자동차

o 이 : 어린이 보호 구역에서 동작할 수 있는 자율 주행차의 코드를 작성하였음. 자율 주행차의 기능으로는 신호등 인식 및 장애물 감지와 어린이 보호 구역 감지 기능으로 구성하였음. [그림 4]는 자율 주행차를 위한 코드 일부를 확인할 수 있음

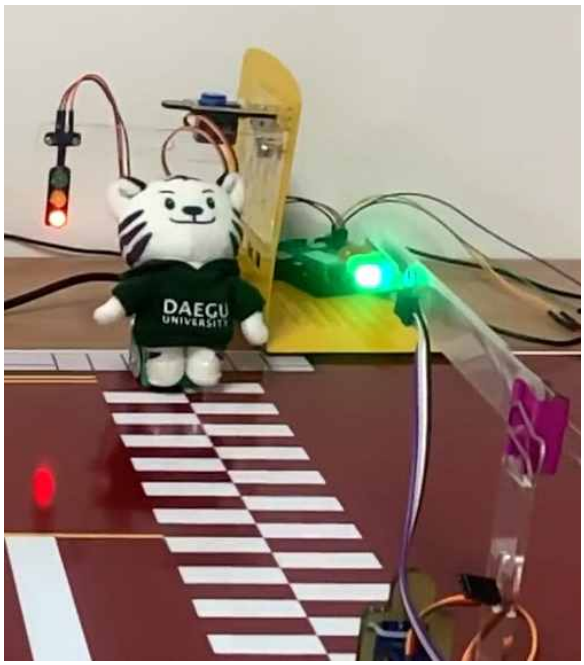


[그림 4] 자율 주행차의 동작을 위해 작성한 코드

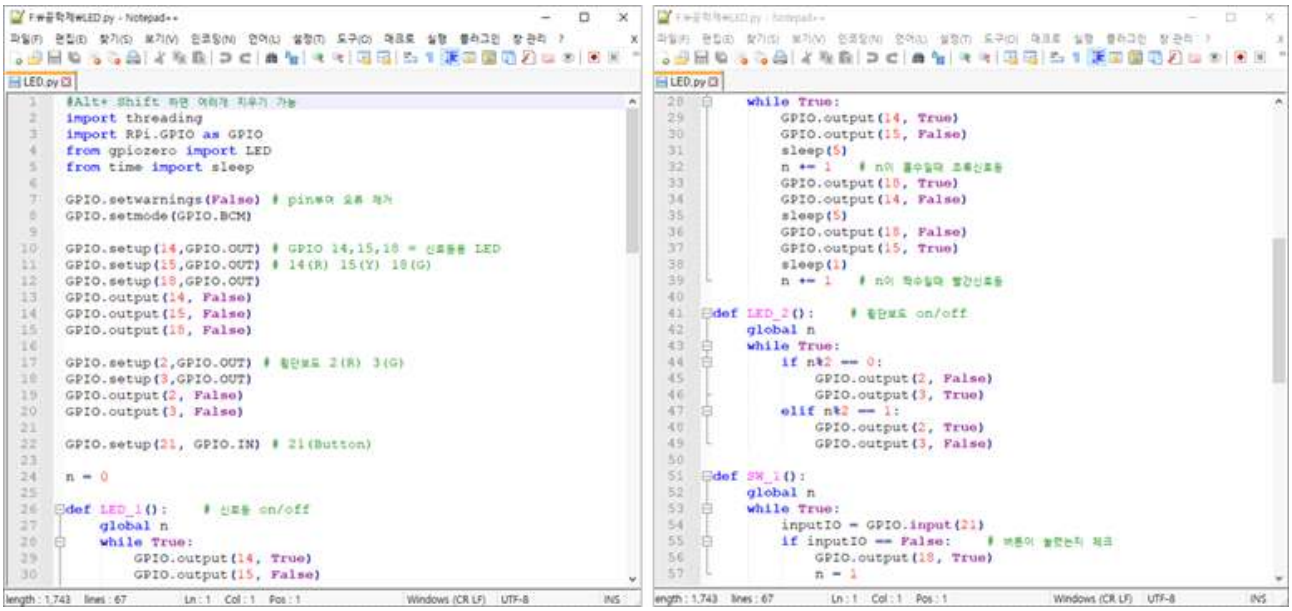
<표 4> 자율 주행차 제작에 사용한 언어 및 라이브러리

Python 3	Open CV

o 박 : 어린이 보호 구역의 신호 체계를 위해 라즈베리 파이를 이용하여 횡단보도 신호등과 도로 신호등의 제작을 진행하였으며, 나아가 신호 체계를 위해 코드를 작성하였음.



[그림 5] 제작한 신호등



```
#Alt+ Shift 하면 여러개 지우기 가능
import threading
import RPi.GPIO as GPIO
from gpiozero import LED
from time import sleep

GPIO.setwarnings(False) # pin부터 오류 제거
GPIO.setmode(GPIO.BCM)

GPIO.setup(14,GPIO.OUT) # GPIO 14,15,18 = 신호등용 LED
GPIO.setup(15,GPIO.OUT) # 14(R) 15(Y) 18(G)
GPIO.setup(18,GPIO.OUT)
GPIO.output(14, False)
GPIO.output(15, False)
GPIO.output(18, False)

GPIO.setup(2,GPIO.OUT) # 횡단보도 2(R) 3(G)
GPIO.setup(3,GPIO.OUT)
GPIO.output(2, False)
GPIO.output(3, False)

GPIO.setup(21, GPIO.IN) # 21(Button)

n = 0

def LED_1():    # 신호등 on/off
    global n
    while True:
        GPIO.output(14, True)
        GPIO.output(15, False)
        sleep(5)
        n += 1    # n이 홀수일때 초록신호등
        GPIO.output(18, True)
        GPIO.output(14, False)
        sleep(5)
        GPIO.output(18, False)
        GPIO.output(15, True)
        sleep(1)
        n += 1    # n이 짝수일때 빨간신호등

def LED_2():    # 횡단보도 on/off
    global n
    while True:
        if n%2 == 0:
            GPIO.output(2, False)
            GPIO.output(3, True)
        elif n%2 == 1:
            GPIO.output(2, True)
            GPIO.output(3, False)

def SW_1():
    global n
    while True:
        inputIO = GPIO.input(21)
        if inputIO == False:    # 버튼이 눌렸는지 체크
            GPIO.output(18, True)
            n = 1
```

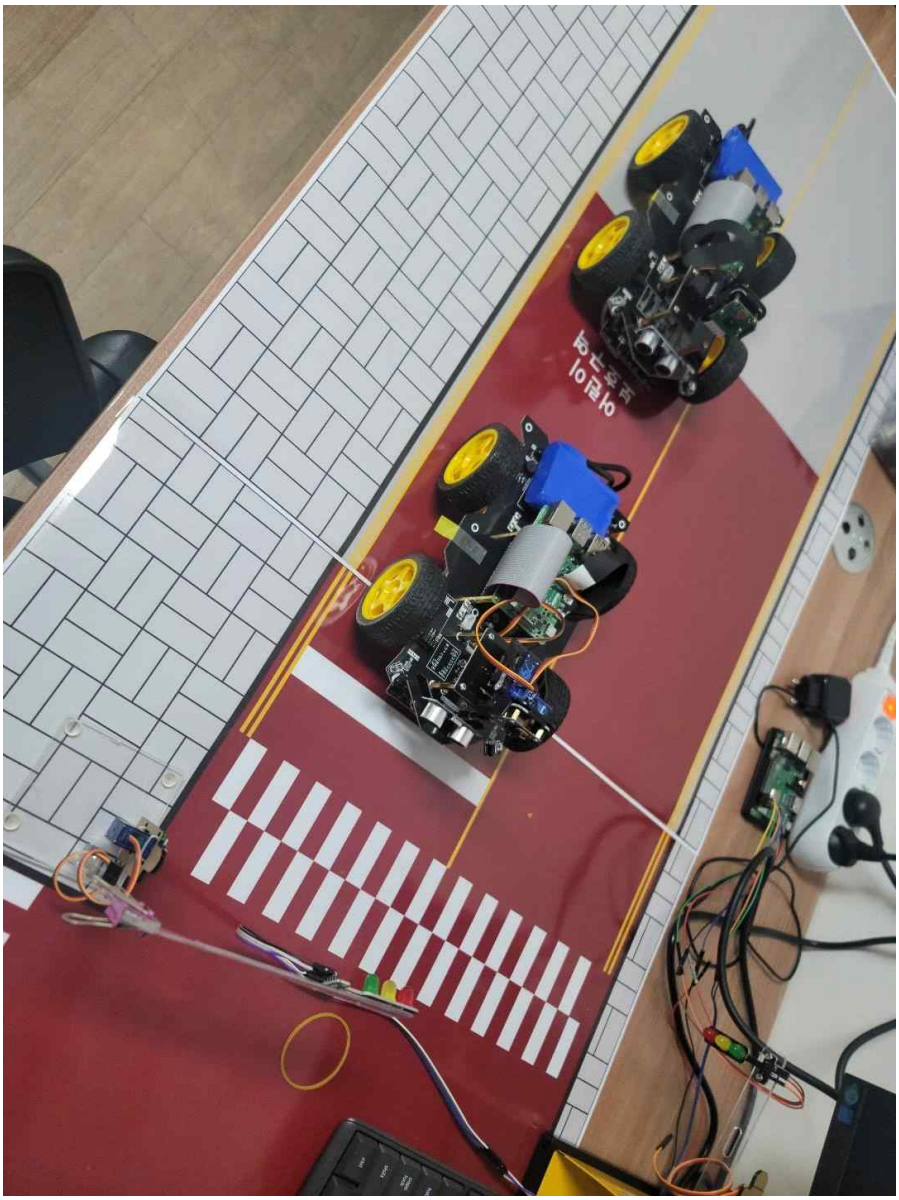
[그림 6] 어린이 보호 구역 신호 체계를 위해 작성한 코드

o 구축 환경 테스트

각 팀원끼리 역할을 나누어 구축한 실험 환경의 테스트를 진행하기 위해 [그림 7]과 같은 환경에서 구축 환경 테스트를 진행하였다. 환경 테스트 중 자율 주행차에 대한 문제점을 발견하였다.

본 팀은 자율 주행차를 제작하기 위해 라즈베리 파이와 다양한 센서를 사용하였다. 자율 주행차의 기능을 위해 신호 인식 및 장애물 탐지를 위해 여러 개의 코드를 Thread로 작성하였다. 이때 라즈베리 파이의 Memory가 부족하여 신호 인식이 잘 진행되지 않는 문제점이 발생하였다.

이러한 문제점은 Thread로 돌리는 기능을 따로 실행시키는 방법으로 바꾸어 해결한 후 구축 환경에 대한 테스트를 완료하였다.



[그림 7] 구축 환경 테스트 장면

o 공격 선정 및 공격 시나리오 제작

테스트를 완료한 실험 환경에서 실시간으로 공격 데이터를 수집하기 위해 자율 주행차 및 신호 체계에 주입할 공격에 대한 선정 및 공격 시나리오 제작을 진행하였다. 처음 제작한 시나리오의 경우 시나리오의 개발 및 검증에 관한 내용으로 학회에 참가하였으며, 이후 시나리오의 개선 및 내용을 추가하여 한국산업정보 학회에 참가하였다. 따라서 본 팀은 시나리오를 크게 2개로 제작하였으며, 각각의 내용은 다음과 같다.

- **멀티미디어 학회**

주요 기반시설 중 하나인 도로 중 어린이 보호 구역에는 다양한 IoT가 존재한다. 다양한 IoT 기기 중 공격 시나리오를 위해 사용한 IoT 기기는 자율 주행차와 신호 체계를 위한 신호등이다. 자율 주행차와 신호등에는 각각 공격이 발생할 수 있으므로 다양한 환경에서 공격 데이터를 수집하기 위해 크게 4가지의 환경으로 나누어 시나리오를 제작하였다.

<표 5> 멀티미디어 학회 시나리오

시나리오	공격 대상	공격 기법	
1	신호등	포맷 스트링 취약점 악용을 통한 신호등 제어 변수 조작	
2	자율 주행차	가용성	128MB 스트레스를 1개 프로세스로 실행
3			1,024MB 스트레스를 2개 프로세스로 실행
4			1,024MB 스트레스를 3개 프로세스로 실행

신호등에 주입할 공격으로는 포맷 스트링 공격으로 선정하였으며, 자율 주행차에 주입한 공격으로는 가용성 공격을 사용하였다. 포맷 스트링 공격의 경우 공격 강도가 없으므로 공격이 주입된 하나의 상황만 시나리오로 제작하였으며, 공격 강도가 다양한 가용성 공격의 경우에는 공격의 강도를 강함, 중간, 약함으로 나누어 자율 주행차에는 3가지의 시나리오를 제작하였다.

- **한국산업정보 학회**

앞선 4가지의 시나리오는 도로 신호 및 자율 주행차에 대한 전반적인 시나리오였으면, 이후에 제작한 시나리오의 경우에는 자율 주행차에 초점을 두어 시나리오를 제작하였다.

<표 6> 한국산업정보 학회 시나리오

상태	시나리오	
정상 (Normal)	N1	정속 주행
	N2	어린이 보호 구역 내 정지
	N3	어린이 보호 구역 외 정지
공격 (Attack)	V1	정속 주행 시, 비정상 동작
	V2	어린이 보호 구역 내 충돌
	V3	어린이 보호 구역 외 충돌

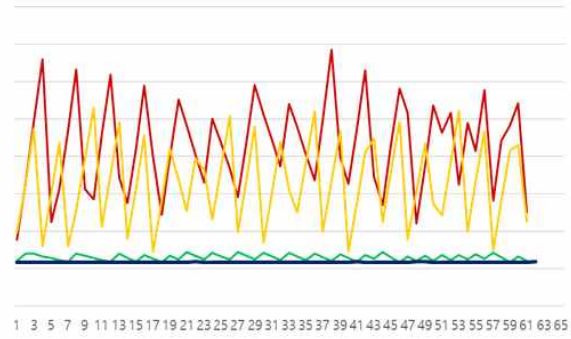
자율 주행차는 어린이 보호 구역에서 정속 주행 및 어린이 보호 구역에 진입하는 상황과 어린이 보호 구역에 진입하지 않은 상황으로 나누어 볼 수 있다. 따라서 본 팀은 정상 상태에서의 데이터 수집을 위해 정속 주행, 어린이 보호 구역 내 정지, 어린이 보호 구역 외 정지 총 3가지로 정상 시나리오를 제작하였다. 추가로 공격 시나리오의 경우에는 정상 상태의 데이터와 비교를 진행하기 위해서 정상 시나리오와 같은 환경에서 자율 주행차에 가용성 공격을 주입하는 3가지의 공격 시나리오를 제작하였다.

o 구축 환경에 실시간 공격 주입 및 공격 데이터 수집 및 수집한 데이터 비교 분석

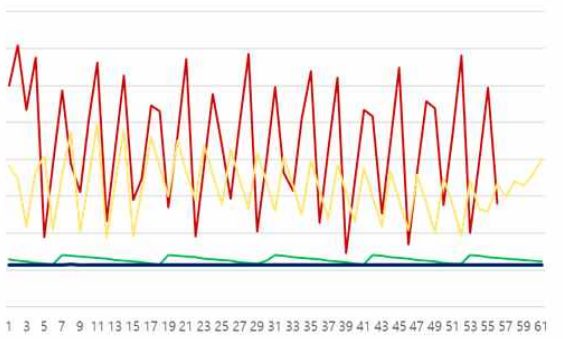
사이버 공격의 탐지를 하기 위해서는 공격 데이터가 필요하다. 따라서 제작한 시나리오 환경에서 실시간으로 공격을 주입하여 공격 데이터를 수집하였으며, 공격 데이터와 비교를 위한 정상 데이터의 수집을 정상 환경에서 진행하였다. 공격 및 정상 데이터 수집은 두 번에 나누어 진행하였다. 수집한 데이터는 공격 탐지를 위해 수집한 데이터로, 정상 데이터와 공격 데이터의 비교를 통해 데이터의 검증까지 진행하였다. 각각 수집한 공격 데이터와 데이터의 비교 분석 결과는 다음과 같다.

- **멀티미디어 학회 공격 데이터 수집 및 비교 분석**

앞선 첫 번째로 제작한 시나리오에서 공격 데이터 및 정상 데이터의 수집을 진행하였다. 데이터의 경우에는 Web cam, 초음파 센서, 적외선 센서의 성능 데이터를 수집하였다. 정상 데이터의 경우 제작한 4가지의 시나리오 모두에 대해서 수집을 진행하였으며, 공격 데이터는 자율 주행차에 가용성 공격을 실시간으로 주입하며 공격 데이터를 수집하였다.



[그림 8] Web Cam 메모리 사용량



[그림 9] 초음파 센서 메모리 사용량

[그림 8]과 [그림 9]는 가용성 공격 강도에 따른 Web cam 및 초음파 센서의 성능 데이터이다. 가용성 공격의 경우에는 3가지의 강도로 주입하였다. 빨간색 그래프의 경우에는 가장 강한 강도의 가용성 공격이며, 각 프로세스 당 1024M(1G) 크기의 스트레스를 3개의 프로세스로 실행시켰을 때의 공격 데이터이다. 노란색 그래프는 각 프로세스 당 1024M(1G) 크기의 스트레스를 2개의 프로세스로 실행시킨 후 수집한 데이터이다. 마지막으로 가장 약한 강도의 공격 데이터인 초록색 그래프는 1개의 프로세스에 128M 크기의 스트레스가 부하된 상황에서 수집을 진행한 데이터이다. 추가로 파란색 그래프는 공격이 주입되지 않은 상황에서 수집을 진행한 정상 데이터이다.

정상 데이터와 공격 데이터의 수집 이후 비교를 진행한 결과, 정상과 공격 데이터는 명확하게 차이가 났으며, 나아가 공격 강도에 따라서도 구분할 수 있었다. 이와 같은 결과로 수집한 정상 및 공격 데이터가 잘 수집되었음을 검증하였고, 데이터를 사용하여 공격을 탐지할 수 있다는 것을 확인하였다.

- **한국산업정보 학회 공격 데이터 수집 및 비교 분석**

이후 자율 주행차에 초점을 두어 공격 데이터를 수집하기 위해 새로운 수집 환경을 제작하였다.

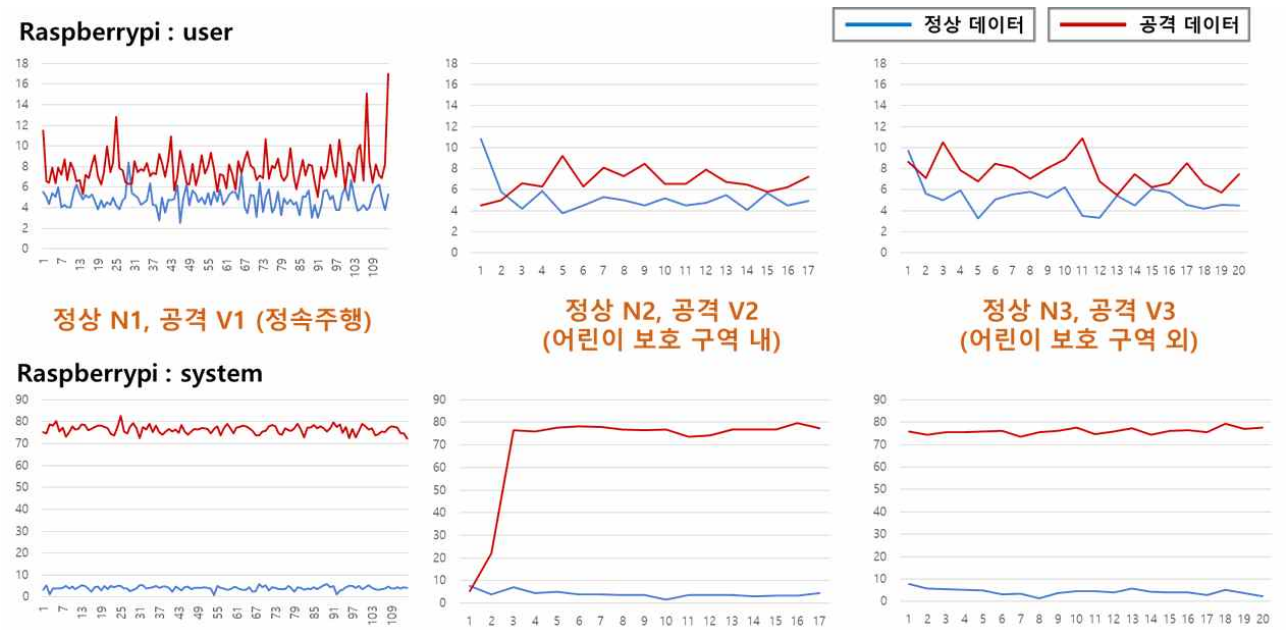
[그림 10] 공격 데이터 수집을 위한 그라파나 수집 환경

추가적인 데이터를 수집하기 위해 그라파나 웹 애플리케이션을 사용하였다. 그라파나 환경에서는 라즈베리 파이의 CPU, Memory, Network, GPU 등의 다양한 성능 데이터를 수집할 수 있으며, 이를 사용하여 CPU, Memory, Process 메트릭을 수집하였다. 3가지의 메트릭은 총 22종(CPU 9종, Memory 6종, Process 7종)으로 구성되어 있었으며, 상세한 메트릭은 <표 7>과 같다.

<표 7> 그라파나를 사용하여 수집한 데이터 메트릭

CPU	Memory	Process
Respberrypi : User	Respberrypi : total	Respberrypi : running
Respberrypi : system	Respberrypi : used	Respberrypi : blocked
Respberrypi : softirq	Respberrypi : cached	Respberrypi : sleeping
Respberrypi : steal	Respberrypi : free	Respberrypi : stopped
Respberrypi : nice	Respberrypi : buffered	Respberrypi : zombies
Respberrypi : irq	Mem.last	Respberrypi : paging
Respberrypi : iowait		Respberrypi : unknown
Respberrypi : guest		
Respberrypi : guest_nice		

본 팀은 수집을 진행한 22종의 메트릭 모두에 대해서 공격 데이터와 정상 데이터의 비교를 진행하였다. 비교를 진행한 후 정상과 공격의 차이가 명확한 4가지의 메트릭을 공격 탐지를 위한 메트릭으로 사용하였다. 4가지의 메트릭은 CPU에서 Respberrypi : User, Respberrypi : system 두 가지. Memory에서 Respberrypi : used, Process에서 Respberrypi : running이다. [그림 11]은 공격 탐지를 위해 사용한 4가지의 메트릭 중 CPU 메트릭에 대한 비교 그래프이다.



[그림 11] 4종의 메트릭 중 2종의 메트릭에 대해 정상 및 공격 데이터 비교 그래프

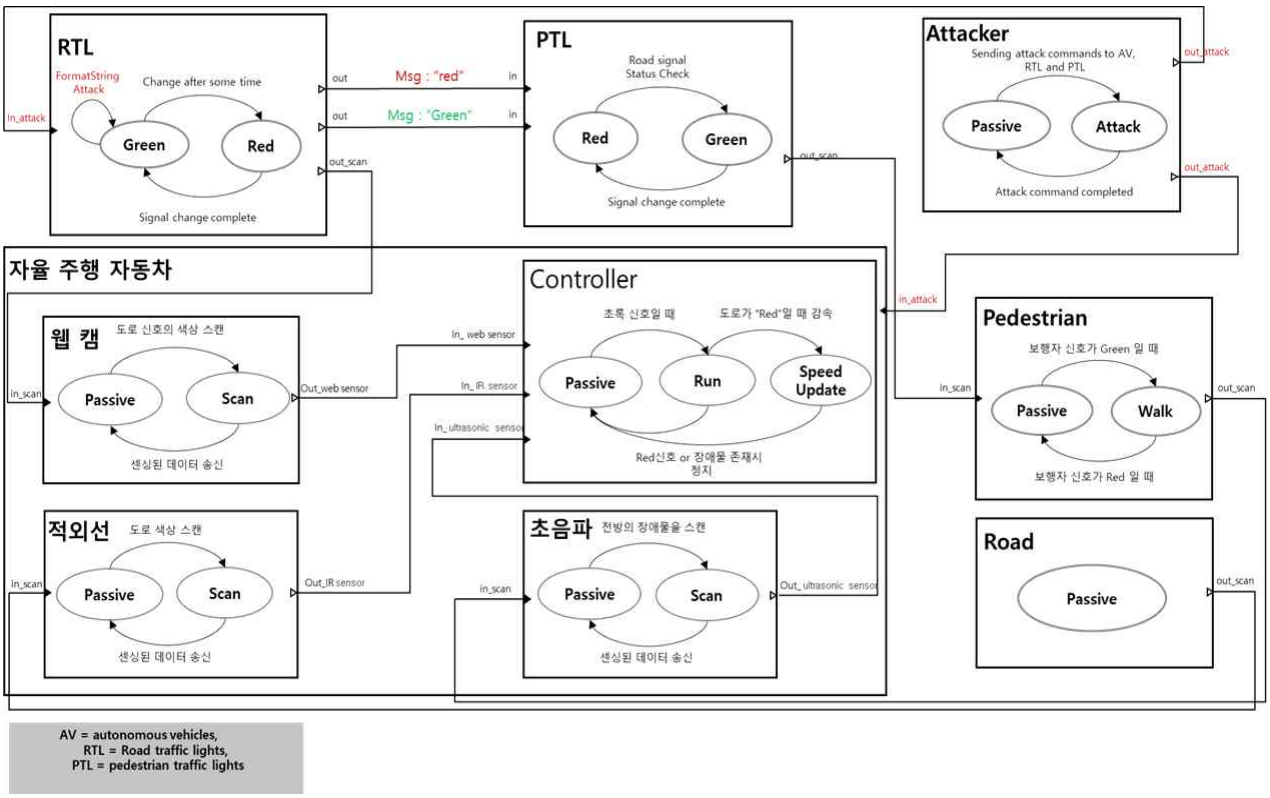
파란색 그래프는 공격이 들어가지 않은 정상 데이터이며, 빨간색 그래프는 공격을 주입한 후 수집한 공격 데이터이다. 비교 결과 모든 시나리오에서 공격 데이터와 정상 데이터의 차이가 명확한 것을 확인할 수 있었다. 따라서 4가지의 메트릭 모두 공격 탐지를 위해 사용 가능하다는 것을 검증하였다.

o 가상 데이터 생성 및 Devs 모델링 제작

본 팀은 주요 기반시설에서 발생하는 공격의 보안 솔루션을 제안하기 위해서 디지털 트윈을 활용하였다. 디지털 트윈은 물리적인 공간을 디지털 공간에 그대로 구현하는 방식이다. 주요 기반시설의 경우 사이버 공격으로 시설이 마비되거나 손상이 되면 국가에 큰 피해를 입힌다. 이러한 주요 기반시설에 대한

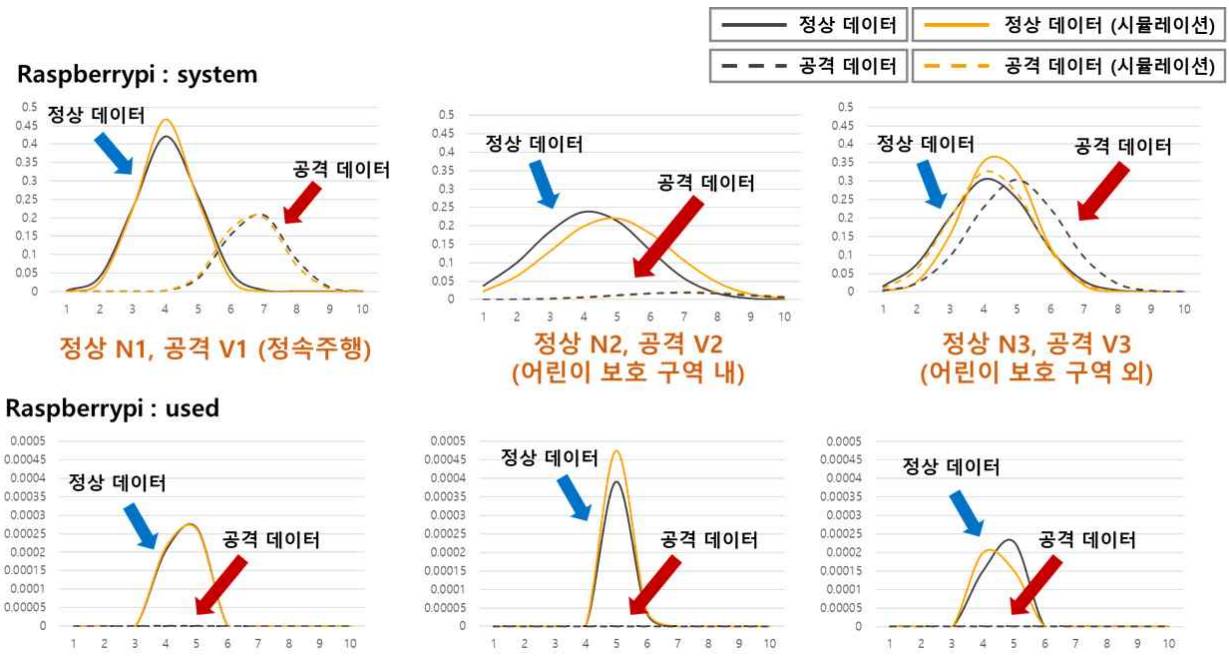
사이버 공격 탐지 방법을 제시하기 위해서는 주요 기반시설에 직접 공격을 주입한 후 공격 데이터를 수집하는 과정이 필요하다. 하지만 주요 기반시설의 특성으로 인하여 실제 공격을 주입하여 공격 데이터를 수집하는데에는 어려움이 있다, 따라서 주요 기반시설에 대한 사이버 공격 탐지 솔루션을 위해 디지털 트윈 방법을 사용하였다. 디지털 트윈은 물리 공간과 물리 공간을 그대로 재현한 사이버 공간을 만든다. 그 후 물리 공간과 사이버 공간 사이에 데이터를 주고받으며 피드백을 주는 것이 가능하다.

본 팀은 사이버 공격 탐지를 위한 디지털 트윈 모델을 제안하기 위해서 이산사건 시뮬레이션(Discrete Event System Specification, 이하 Devs) 모델링을 진행하였다.



[그림 12] 디지털 트윈 모델 제안을 위한 이산 사건 시뮬레이션 모델링

다음의 모델링은 자율 주행차와 신호 체계를 이산 사건 시뮬레이션으로 구현한 모델이다. 제작한 모델에는 파라미터로 사용한 데이터가 필요하며, 이후 시뮬레이션에 사용할 가상 데이터의 제작을 진행하였다. 가상의 데이터는 앞서 공격 탐지를 위해 검증이 끝난 수집 데이터를 기반으로 제작하였다.

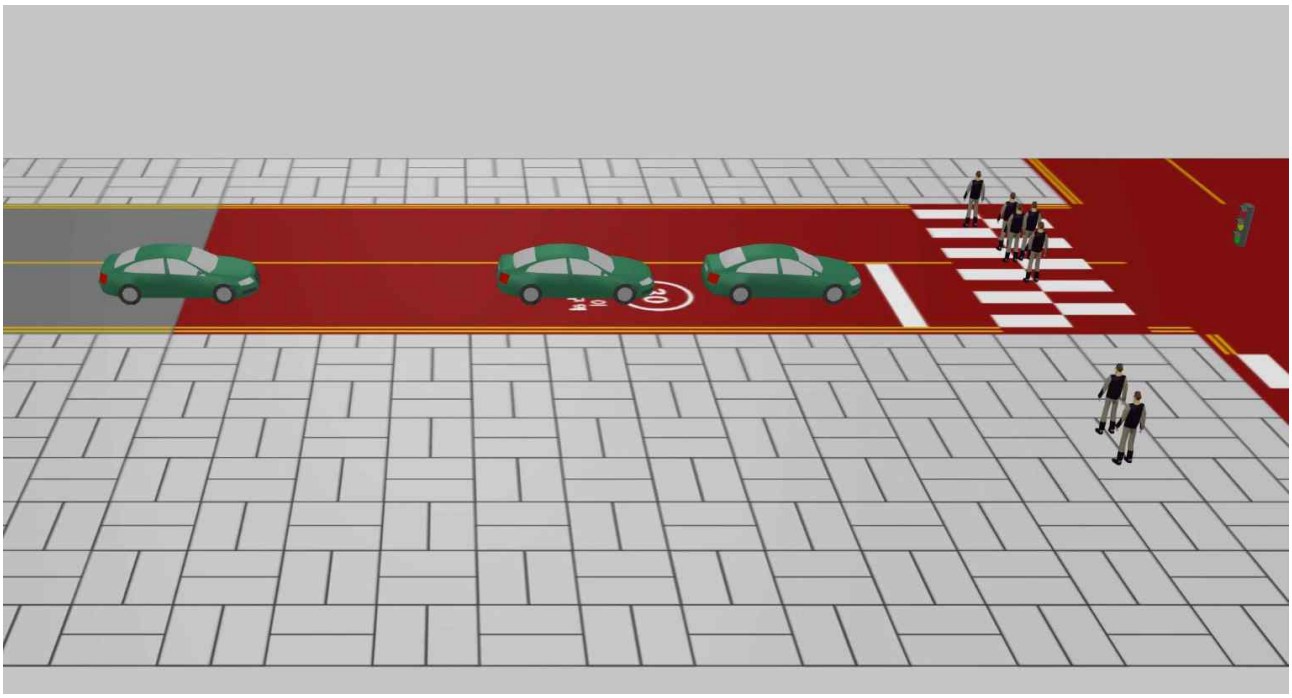


[그림 13] 시뮬레이션에 주입하기 위해 생성한 가상 데이터 비교 그래프

가상 데이터의 경우에는 수집한 데이터의 표준 편차와 데이터 셋의 수, 평균 값을 사용하여 생성하였다. 생성한 가상 데이터의 검증을 위해 가상 데이터와 직접 수집한 데이터를 정규 분포표로 만들었으며, 비교를 진행하였다. [그림 13]에서는 생성한 가상 데이터와 수집한 데이터의 비교 결과를 확인할 수 있다. 주황색 선은 생성한 가상 데이터이며 검은 선은 수집한 데이터이다. 또한, 실선은 정상 데이터이며, 파선은 공격 데이터이다. 각각의 정규 분포표를 비교해 본 결과 생성한 정상 데이터와 수집한 정상 데이터, 생성한 공격 데이터와 수집한 공격 데이터가 유사한 형태를 띠는 것을 확인할 수 있으며. 이는 생성한 가상 데이터가 수집한 데이터를 잘 반영하였다는 것을 의미한다.

o 도전 학기 결과

본 팀은 주요 기반시설의 IoT 취약점 분석 및 보안 솔루션 개발이라는 주제로 도전 학기를 진행하면서 다양한 IoT 기기의 취약점 조사와 실제 주요 기반시설에서 발생하는 공격에 대한 데이터를 수집하기 위해 어린이 보호 구역을 제작하였다. 이후 어린이 보호 구역에서 운행할 수 있는 자율 주행차와 신호체계를 제작하였다. 이후 공격이 발생할 수 있는 다양한 공격 시나리오를 제작하였으며, 제작한 시나리오에 맞추어 실시간으로 공격 데이터 수집을 진행하였다. 수집한 데이터는 검증을 위해 그래프화 하여 비교 및 분석을 진행하였으며, 최종적으로 보안 솔루션을 제안하기 위해 실제 Devs 모델링과 모델링에 사용한 가상 데이터 생성을 진행하였다. 이후 얻은 결과 및 데이터를 기반으로 자율 주행차 데이터 분석을 통한 사이버 공격 디지털 트윈 모델 연구라는 논문을 작성하였으며, 나아가 제작한 Devs 모델링 중 정상 상태에 대해서 그래픽화까지 진행하였다.



[그림 14] Devs 모델링을 기반으로 제작한 정상 상태의 모델링

이후 본 팀은 수집한 가상 데이터를 기반으로 디지털 트윈 모델을 제작하여, 물리 공간에서 공격이 발생할 때 실시간으로 사이버 공격의 탐지 및 예방을 할 수 있도록 제작할 예정이며, 나아가 공격 상황에 대한 그래픽화까지 진행해보려고 한다.

3. 자기 평가

조 : 이번 도전 학기를 진행하면서 주요 기반시설을 주제로 조사하며 많은 정보를 얻을 수 있었다. 이번 도전 학기를 진행하면서 크게 어린이 보호 구역 제작 및 신호 체계에서 발생할 수 있는 공격인 포맷 스트링 공격을 제작하였다. 이 중 포맷 스트링 공격의 구현에 있어 Python 언어의 구조상 메모리 주소를 얻어 공격을 주입하기에 어려움이 있었다. 이러한 문제점은 C 언어로 신호 체계 코드를 작성하여 해결하였다. 이러한 문제점으로 인하여 모르는 지식을 알 수 있는 계기가 되었다. 또한, 멀티미디어 학회와 한국산업정보 학회에 참가하면서 논문을 작성하면서 다양한 정보를 얻을 수 있었다. 최종적으로 팀장으로서 팀원들과 원만한 협업을 통해 좋은 성과를 도출할 수 있어서 도전 학기 중 맡은 역할에 대해 잘 수행한 거 같다.

박 : 먼저 기반 시설에서 발생할 수 있는 공격 취약점을 조사하고 위험도 분석을 진행했고 신호 체계에 사용되는 라즈베리파이의 기본 설치와 Thread Code를 사용하여 신호등의 역할을 할 수 있도록 코딩을 진행하였는데 Tread 함수를 사용해본 적이 없어서 응용하는 데에 있어 어려움이 존재했지만, 검색과 교수님들께 질문해서 해결하였다. 그리고 한국산업정보학회에 제출할 논문에 필요한 정상 데이터와 공격 데이터들을 수집하고 분석할 때 사용한 Grafana도 사용법이 익숙지 않아 해결하는 데 많은 시간이 걸렸다. 도전 학기를 진행하면서 여러 학회 참여와 어려웠던 점들의 해결함으로써 좋은 경험을 쌓을 수 있었고 어려웠지만 노력해서 스스로 맡은 부분을 잘 수행했던 것 같다.

김 : 도전 학기를 진행하면서 자율 주행 자동차에 가용성 공격 주입을 위해 공격에 사용하기 위한 tool을 검색하고 이를 기반으로 연구를 수행하기 위해 사용되는 자율 주행 자동차에 적합한 공격을 선택하여 가용성 공격을 주입하여 차량의 성능 저하를 확인하고 이를 시각화하여 더욱

세부적으로 공격의 강도를 조절하며 그래프화 하였다. 공격을 탐색함에 있어 적절한 공격 탐색에 어려움과 공격의 강도를 설정하기 위한 과정에서 다소 어려운 부분이 있었으나 적합한 강도를 찾으므로 실제 자율 주행 자동차의 성능 저하를 확인 함으로써 성취감을 느끼며 이번 과제를 통해 다양한 환경에서 시용할 수 있는 공격의 종류를 배울 수 있었다.

이 : 도전 학기 초반에는 크게 자율 주행 자동차 제작과 주요 기능들인 신호등 인식과 센서 감지를 코딩하였으며 중간 보고서 이후 후반에는 자율 주행 자동차에 대한 공격데이터의 수치화를 위한 그라파나 및 텔레그래프를 이용한 데이터 수집환경을 구축하고 수집하였다. 도전 학기를 진행하면서 많은 문제와 어려움이 존재했다. 크게 2가지를 고르자면 원래 파이토치와 YOLO를 이용한 딥러닝 학습을 하여 신호등을 인식시킬 예정이었지만 자동차가 지원하는 라즈베리 파이 OS와 YOLO가 사용 가능한 라즈베리파이 OS가 달라 사용하지 못하고 opencv만을 이용한 원 검출 및 색 검출로 신호등을 인식하여 문제를 극복했다. 그리고 그라파나 및 텔레그래프를 이용한 데이터 수집환경을 구축할 때도 라즈베리 파이 OS의 호환성 문제가 있어 많은 어려움이 있었다. 이처럼 자율 주행 자동차 제작 및 코딩과 수집환경구축을 하면서 다른 사소한 문제들이 발생하면서 그것을 해결할 때마다 성취감을 느끼며 학교 강의에서는 배우지 못하는 점들이 많아서 학습에 많은 도움이 되었다.

4. 최종 결과물

이번 도전 학기를 주요 기반시설의 IoT 취약점 분석 및 보안 솔루션 개발에 대한 주제로 진행하였다. 주요 기반시설의 취약점 및 보안 솔루션을 위해 직접 어린이 보호 구역을 제작하였으며, 제작한 환경에서 실시간으로 공격을 주입하여 공격 데이터 수집을 진행하였다. 이후 공격 데이터의 비교, 분석 및 가상 데이터를 제작하여 자율 주행차 데이터 분석을 통한 사이버 공격 보안을 위한 디지털 트윈 모델에 대해 제안하였다. 다음과 같은 과정에서 멀티미디어 학회와 한국산업정보 학회에 논문을 투고하였으며, 포스터 세션과 구두 발표 세션에 참여하였다.

본 팀의 최종 결과물은 멀티미디어 학회와 한국산업정보 학회에 투고한 논문과 각 학회에서 수상한 상장을 최종 결과물로 제출한다.

o 멀티미디어 학회

멀티미디어 학회에는 사물 인터넷 기반 도로교통 시설에 대한 사이버 공격 시나리오 개발 및 검증이라는 주제로 논문을 투고하였으며, 다음과 같은 내용으로 포스터 세션에 참가하여 우수 논문 발표 상을 수상하였다.

· 사물인터넷 기반 도로교통 시설에 대한 사이버 공격 시나리오 개발 및 검증

사물인터넷 기반 도로교통시설에 대한 사이버 공격 시나리오 개발 및 검증

Development and Verification of Cyberattack Scenarios against IoT-based Road Transport Infrastructure

* Dept of Computer Engineering, Daegu University

요 약

사물인터넷 기술이 발달하면서 국가 주요기반시설 운영에 사물인터넷 기기를 도입하는 사례가 증가하고 있다. 본 연구에서는 다양한 주요기반시설 중, 교통시설에 초점을 두어 신호체계와 같은 도로 교통시설에 존재하는 취약점 및 자율주행차 취약점을 분석하여 보행자의 안전을 위협할 수 있는 사이버 공격 시나리오를 개발한다. 본 연구에서는 교통사고의 위험성이 높은 어린이 보호구역을 사물인터넷 환경으로 구축하고, 신호체계 및 자율주행차에 직접 공격을 주입함으로써 개발된 공격 시나리오의 실현 가능성 및 위험성을 검증한다.

• 개인 역할

본 논문에 작성을 위해 팀원들의 역할은 다음과 같다.

- 조 : 논문 작성을 위해 필요한 주요 기반시설 중 하나인 어린이 보호 구역의 제작을 진행하였으며, 제작된 신호 체계에 주입할 포맷 스트링 코드를 제작하여 주입하였다. 추가로 공격을 주입한 환경에서 공격 데이터 수집을 진행하였다.
- 김 : 논문 작성을 위해 자율 주행차의 제작을 진행하였으며, 자율 주행차에 발생할 수 있는 가용성 공격의 주입을 진행하였다. 수집한 공격 데이터와 시나리오를 통해 논문 작성을 진행하였다.
- 이 : 논문의 관련연구 챕터를 작성하기 위해 사물인터넷 기반 도로 교통시설에 대해 발생한 사이버 공격에 관한 관련 연구를 조사하였으며, 이를 기반으로 관련 연구 챕터를 작성하였다. 또한, 실험을 위한 자율 주행차의 신호 인지 및 초음파 센서에 대한 코드 작성을 진행하였다.
- 박 : 논문 작성에 필요한 어린이 보호 구역에 있는 신호 체계의 코드 및 시설 제작을 진행하였으며, 포맷 스트링 공격 주입으로 인한 공격 데이터 수집을 진행하였다.

· 참고 문헌

[1] 이재호. (2019). AHP 기법을 활용한 주요 정보통신기반시설 웹 취약점 점검 항목 위험도 산정 방법. 예술인문사회 융합 멀티미디어 논문지, 9(6), 719-728.

[2] 김도연. (2014). 산업제어시스템의 사이버보안을 위한 취약점 분석. 한국전자통신학회논문지, 9(1), 137-142.

[3] Choi, S., & Kim, H. (2020). MITRE ATT&CK 프레임워크 기반 에너지분야 기반시설 보안 모니터링 방안. Review of KIISC, 30(5), 13-23.

[4] Cho, H., Lee, S., & Choi, W. (2021). MEMS 센서대상 오류주입 공격 및 대응방법. Review of KIISC, 31(1), 15-23.

[5] 조경현, 김지연, "주요 기반시설 보안을 위한 CVE 기반 취약점 분석(Analysis of CVE-based Vulnerabilities for Critical Infrastruction Protection)", 2022년도 한국멀티미디어학회 춘계학술발표대회 논문집 제25권 1호, 2022.05.

· 우수논문발표 상

KOREA MULTIMEDIA SOCIETY

한멀회 2022-276호

우수논문발표상

논문제목 : 사물인터넷 기반 도로교통시설에 대한
사이버 공격 시나리오 개발 및 검증

저 자 명 :
(대구대학교)

귀하께서는 본 학회의 2022년도 추계학술대회의 학부생 포스터 논문 발표 부문 에서 심사위원/좌장의 공정한 심사에 의해 우수논문발표자로 선정되었기에 이 상을 드립니다.

2022년 11월 18일

사단법인 한국멀티미디어학회

학 회 장

한국멀티미디어학회

부산광역시 해운대구 센텀동로 99 벽산 e-센텀클래스원 504호 **사업자번호** 617-82-04590 T_051.712.9601 F_051.712.9603
99, Centum Dong-ro, 5F, #504, Haeundae-gu, Busan, Korea. www.kmms.or.kr

o 한국산업정보 학회

한국산업정보 학회에는 자율 주행차 데이터 분석을 통한 사이버 공격 디지털 트윈 모델 연구라는 주제로 논문을 투고하였으며, 다음과 같은 내용으로 구두 발표 세션에 참가하여 우수 논문 상을 수상하였다.

· 자율 주행차 데이터 분석을 통한 사이버 공격 디지털 트윈 모델 연구

자율주행차 데이터 분석을 통한 사이버 공격 디지털 트윈 모델 연구

요 약 본 사물인터넷 기술이 발전하면서 센서 데이터를 기반으로 도로 상황을 실시간 파악하고, 인터넷을 통한 정보 처리 및 공유를 통해 최적의 알고리즘으로 스스로 운행하는 자율주행차가 등장하였다. 자율주행차는 안전사고에 대비하여 수많은 기능 및 안전성 평가를 거쳐 제조되지만, 해킹 등 인터넷을 통한 사이버 공격에 노출될 경우, 주행기능이 무력화되면서 심각한 인명 및 재산 피해를 초래할 수 있다. 이러한 피해를 줄이기 위해서는 자율주행차에 발생할 수 있는 다양한 사이버 공격을 사전에 예측하고 대응 기술을 마련하는 것이 필요하다. 본 논문에서는 자율주행차 공격을 안전하고 효율적으로 연구할 수 있도록 디지털 트윈 모델로 개발하는 모델링 연구를 수행한다. 디지털 트윈은 물리 공간을 디지털 공간에 재현하는 기술로서 자율주행차의 정상 및 공격 상태를 디지털 트윈 모델로 개발함으로써 공격 시나리오 예측, 패치 개발, 실시간 자율주행차 모니터링을 통한 신속한 공격 탐지 및 제어가 가능해진다. 본 논문에서는 라즈베리파이 기반의 자율주행차를 활용하여 주행 시나리오별로 정상 및 서비스 거부 공격 데이터를 수집하고, 확률분포 모델링을 통해 디지털 트윈 모델을 생성 및 검증하는 연구를 수행한다.

핵심주제어 : 자율주행차, 사이버보안, 디지털 트윈, 서비스 거부

Key Words : Autonomous Vehicle, Cybersecurity, Digital Twin, Denial of Service

• 개인 역할

본 논문에 작성을 위해 팀원들의 역할은 다음과 같다.

- 조 : 데이터 수집에 필요한 시나히오 제작을 진행하였으며, 그라파나 환경을 통해 시나리오에 맞추어 공격 및 정상 데이터의 수집을 진행하였다. 이후 관련 연구 및 데이터를 기반으로 논문을 작성하였다.
- 김 : 그라파나 환경에서 공격 데이터 수집을 진행하였으며, 수집이 끝난 후 디지털 트윈을 사용한 자율 주행차의 보안에 관한 주제로 관련 연구의 조사를 진행하였다.
- 이 : 자율 주행차의 추가 데이터 수집을 위해 새로운 공격 수집 환경인 그라파나 웹 애플리케이

1) 대구대학교 정보통신대학 컴퓨터공학과 학사과정
2) 대구대학교 정보통신대학 컴퓨터공학과 교수

션 설치를 진행하였으며, 시나리오 제작을 진행하였다.

- 박 : 그라파나 환경에서 수집한 다양한 데이터의 비교를 진행하였다. 이후 비교 결과에 대해 그래프화 하였으며, 수집한 데이터를 기반으로 시뮬레이션에 사용할 가상 데이터의 생성 및 가상 데이터와 수집한 데이터의 비교를 진행하였다.

· 참고 문헌

[1] 김상현, 안승현, 유상조. (2022). 심층강화학습을 이용한 자율주행 차량제어 및 ML-Unity 디지털 트윈 환경구현. 한국통신학회 학술대회논문집, 1721-1722.

[2] Y. Kim and J.-E. Hong, “VENTOS-Based Platoon Driving Simulations Considering Variability,” KIPS Transactions on Software and Data Engineering, vol. 10, no. 2, pp. 45-56, Feb. 2021.

[3] Ahn, D. et al. (2019) “A Study on Simulation Based Fault Injection Test Scenario and Safety Measure Time of Autonomous Vehicle Using STPA,” The Journal of The Korea Institute of Intelligent Transport Systems. The Korea Institute of Intelligent Transport Systems. doi: 10.12815/kits.2019.18.2.129.

[4] S. Almeaibed, S. Al-Rubaye, A. Tsourdos and N. P. Avdelidis, "Digital Twin Analysis to Promote Safety and Security in Autonomous Vehicles," in IEEE Communications Standards Magazine, vol. 5, no. 1, pp. 40-46, March 2021, doi: 10.1109/MCOMSTD.011.2100004.

[5] Y. Zhou, A. K. Bashir, J. Wu, Y. D. Al-Otaibi, X. Lin and H. Xu, "Secure Digital Twin Migration in Edge-based Autonomous Driving System," in IEEE Consumer Electronics Magazine, 2022, doi: 10.1109/MCE.2022.3217363.

· 우수 논문상

우 수 논 문 상

귀하께서는 본 학회의 2022년도 추계학술대회의 발표논문 중에서 학술위원의 공정한 심사에 의해 우수논문으로 선정되었기에 본 학술대회 논문상을 드립니다.

논문제목 : 자율주행차 데이터 분석을 통한 사이버 공격 디지털 트윈 모델 연구

저 자 명 :

(대구대학교)

2022년 12월 2일

사단법인 한국산업정보학회장