The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 20, No. 4, pp.81-86, Aug. 31, 2020. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2020.20.4.81
JIIBC 2020-4-11

자율주행 자동차의 시스템 보안 향상을 위한 새로운 데이터처리 기능 제안

Proposal of New Data Processing Function to Improve the Security of Self-driving Cars' Systems

장은진*, 신승중**

Eun-Jin Jang*, Seung-Jung Shin**

요 약 사물인터넷 IoT를 넘어선 지능형사물인터넷 AIoT의 발달로 산업 분야가 전반적으로 변해가고 있다. 또한, 4차 산업 혁명 시대가 도래함 에 따라 자동차 산업 분야에서도 획기적인 변화와 발전이 이루어지고 있는데, 그 대표적인 예시가 바로 "자율주행자동차"라고 할 수 있다. 자율주행자동차에 대한 국내외적 관심이 높아짐에 따라 유관기관들의 관련 연구 또한 활발히 진행되고 있고, 실제로 많은 발전을 이루었으며 제한적이나마 상용화 단계로 까지 발전하였다. 하지만, 운전자가 아닌 자동차에 장착된 다양한 센서 들을 활용하여 데이터를 수집, 분석하여 제어하는 자율주행 자동차의 구조 상 보안에 대한 다중화 된 장치가 미흡하여 해킹에 고스란히 노출되는 경우가 많다. 이 경우, 운전자뿐만 아니라 주변 환경에도 위협이 될 수 있기 때문에 본 논문에서는 자율주행 자동차의 시스템 보안 향상을 위한 새로운 데이터처리 기능을 제안하고자 한다.

Abstract With the development of the intelligent Internet of Things AIoT that goes beyond the IoT of the Internet of Things, the industry is changing overall. In addition, with the advent of the 4th Industrial Revolution, revolutionary changes and developments are also taking place in the automobile industry. A representative example is "autonomous driving vehicle". Because the domestic and foreign interests in autonomous vehicles have increased, many developments have been made, and although limited, they have developed into the commercialization stage. However, the structure of the autonomous vehicle that collects, analyzes, and controls data using various sensors installed in the vehicle, not the driver, is often insufficiently exposed to hacking due to the lack of multiplexed devices for security. In this case, as this can be a threat not only to the driver, but also to the surrounding environment, this paper proposes a new data processing function to improve the system security of autonomous vehicles.

Key Words : Self-driving Car, Data processing, Security system, AIoT, intrusion detection

*정회원, 한세대학교 IT융합학과(교신저자)
**정회원, 한세대학교 IT융합학과
접수일자 2020년 7월 15일, 수정완료 2020년 8월 6일
게재확정일자 2020년 8월 7일

Received: 15 July, 2020 / Revised: 6 August, 2020 / Accepted: 7 August, 2020
*Corresponding Author: dmswls1061@naver.com
Dept of IT Convergence, Hansei University, Korea

Ⅰ. 서 론

1. 자율주행 자동차의 정의

자율주행 자동차는 "운전자가 조작을 하지 않고, 센서로 수집된 정보를 기반으로 운행되는 자동차"로 정의할 수 있다.

현재와 같은 개념의 자율주행 자동차는 1977년 일본 쓰쿠바 기계공학 연구소에서 시속 30km의 자율주행 자동차의 개발을 시작으로 그 역사가 시작된다. 그 이후 독일과 미국에서 자율주행 자동차의 연구가 진행되었고, 2010년 구글에서 자율주행 자동차인 Self driving car를 개발하면서 자율주행 자동차의 발전이 급격하게 이루어졌다. 2010년을 기점으로 벤츠와, 테슬라, 현대, 포드 등 대규모의 자동차 회사들이 자율주행 자동차를 연구개발하고 있고, 현재 실제로 사용자가 사용이 가능한 단계로까지 발전이 이루어졌다.

자율주행자동차의 자동화 단계는 미국 자동차기술회(SAE)에 따르면 총 6단계로 나뉘게 된다. level 0 단계는 자율주행의 기능이 전혀 없는 단계이고, level 1 단계는 운전자가 자동차를 운전하는 상태에서 핸들조향 및 가속 또는 감속의 기능을 지원하는 단계이다. level 2 단계는 부분 자동화 단계로 핸들조향 및 속도 조절 등 하나 이상의 자동화 기능이 포함된 단계를 말하며, level 3 단계는 조건부 자동화 단계로 자율주행이 가능하지만 특수한 상황에서 운전자의 조작이 필요한 경우를 말한다. level 4 단계는 일반 도로 등의 주행 환경에서 자율주행이 가능한 단계를 말하며, level 5 단계는 모든 도로 상황에서도 자율주행이 가능한 완전한 자율주행 단계를 나타낸다. 아래의 그림 1. 은 자율주행자동차의 자동화 단계를 나타낸다.

현재 자율주행 자동차의 개발 정도는 level 4 단계로까지 발전해 있으나 센서 기반 자율주행자동차의 특성상 보안 취약점이 존재한다.

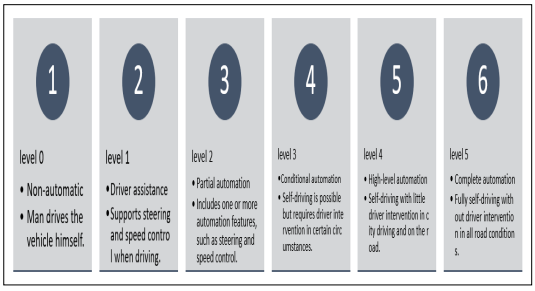

그림 1. 자율주행 자동차의 자동화 단계
Fig. 1. Automation level of self-driving cars

2. 자율주행 자동차의 해킹 사례

2016년 9월 중국의 인터넷기업 텐센트의 한 부서인 '킨보안연구소'가 테슬라의 S모델 시리즈를 원격조종하는 모습을 유튜브에 올렸다[1]. 킨 보안 연구소의 연구원들은 원격조종으로 운행 중인 자동차를 급제동시키고, 썬루프와 운전석을 임의로 조정하는 등의 장면을 공개했고, 이 영상으로 인해 많은 사람들이 자율주행 자동차의 시스템 해킹위험성에 대해 우려를 표했다.

그림 2. 는 해당 공개된 영상에서 보여 지는 해킹된 테슬라 자동차의 주행 중 모습으로 임의로 조작되어 트렁크가 열린 모습이다.

그림 2. 자율 주행 중 해킹된 테슬라 자동차의 모습[2]
Fig. 2. Tesla car hacked during autonomous driving

Ⅱ. 자율주행 자동차의 보안시스템 기술 및 보안 취약점

1. 자율주행 자동차 보안 시스템 기술

국내에서 사용되는 자율주행 자동차 보안 시스템 기술에는 'ECU 보안검증', '지능형 원격검침', 'V2X 보안인증체계', 등이 있다.

ECU는 Electronic Control Unit의 약자로 전자 제어 장치를 뜻한다. 'ECU 보안검증'은 이더넷 기반의 보안 기술로서 자동차의 결점을 자동으로 해석해주는 차량용 방화벽이라고 할 수 있다. '지능형 원격검침'은 키 분배 기술로서 해커가 키(메시지)를 탈취해도 암호화 되어 있기 때문에 내용을 확인할 수 없는 기술이라고 할 수 있다. 'V2X 보안인증체계'에서 V2X란 Vehicle to Everything의 약자로서 자동차와 사물 사이의 통신을 말한다. 'V2X 보안인증체계'란 자율주행이 가능하게하기 위해서 자동차와 주변 기기들 간의 통신이 필수적으로

수반되어야 하는데, 이 때 인증된 기기들 간의 통신만을 가능하도록 하여 보안성을 향상시키는 시스템이라고 할 수 있다.

2. 자율주행 자동차의 시스템 보안 취약점

현재 사용되는 자율주행 자동차의 보안 시스템은 온보드 형식의 OBD2의 블루투스 통신을 통한 ECU코드 변경 등 제한된 환경에서 구현된다고 할 수 있다.

하지만, 스마트폰과 자율주행 자동차가 블루투스를 통해 연결되고, 해커가 사용자의 핸드폰을 통해 자율주행 자동차에 접근하려할 경우 이를 감지하고 차단할 수 있는 기술이 현재로서는 없는 상태이다. 현대인의 필수품이 된 스마트폰을 통한 자율주행 자동차의 해킹을 막을 수 있는 기술적 장치가 부재하다는 것은 자율주행 자동차의 보안 안전성을 위협할 수 있는 요인이 될 수 있다는 것을 뜻한다.

따라서 본 논문은 보다 다양한 환경에서 관리자가 불량 패킷을 분석하여 차단하고, 사용자에게 침입 탐지 알림을 제공하는 새로운 데이터 처리 기능을 제안한다.

Ⅲ. 자율주행자동차 관련 정책 및 새로운 데이터 처리 기능 제안

1. 자율주행자동차 관련 정책

현재 자율주행자동차에 대한 법제도는 「자동차관리법」이 시험 목적의 임시운행을 위하여 자율주행자동차의 정의규정을 마련하고, 임시운행의 관련절차를 규정하고 있을 뿐 상용화를 전제로 한 자율주행자동차 관련 규정을 두고 있지 않다. 또한, 사이버보안이나 개인정보보호 문제에 대하여는 아직 입법 움직임은 없으나 UN 산하 유럽경제위원회 자동차 안전기준포럼(UNECE/WP29)과 공동으로 사이버보안 기준 가이드라인 설정에 참여하고 있다고 한다[3].

자율주행자동차 산업은 빠르게 발전하고 있고, 현실적 상용화를 위해 국내 관련 정책 및 법규 마련이 필수적이라는 전문가들의 조언이 이어지고 있지만 관련 정책은 사실상 부재한 상황이다.

2. 새로운 데이터 처리 시스템 제안

본 논문에서 제안되는 자율주행 자동차 보안성 향상을 위한 새로운 데이터 처리 기능은 차량과 연결되어있는 사용자의 스마트폰 또는 차량정보수집이 가능한 OBD2를 통해 차량 정보를 스캐닝하고, 자동차 조향장치, 변속, 브레이크 등에서 불량 패킷의 시도가 감지되었을 경우 시스템이 적용된 라즈베리파이에서 해당 IP를 차단하는 "침입탐지 시스템" 이라고 할 수 있다. 그림 3. 은 본 논문에서 제안되는 침입탐지 시스템의 기술 구현도이다.

라즈베리파이와 차량 연결은 라즈베리 OBD2 모듈을 사용한다. 테스트 구현을 위해 OBD2모듈을 VM웨어로 대체한다.

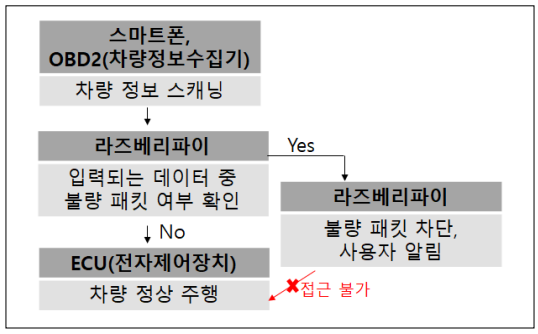

그림 3. 침입탐지 시스템 기술 구현도
Fig. 3. Intrusion Detection System Technology Implementation image

3. 개발환경

본 논문에서 제안되는 새로운 침입탐지 시스템을 구현하기 위해 다음과 같은 개발환경을 사용하였다.

OS 환경은 라즈비안 32bit이고, 개발도구는 eclipse를 사용하였으며, 개발 언어는 JavaScript를 통해 구현하였고, 사용된 보안 오픈 소스는 Suricata이다. 웹서버는 Node.Js를 사용하였다. 또한 라즈비안을 설치하기 위한 기기는 라즈베리파이를 사용하였다.

4. 시스템 기능 구현

본 시스템은 패킷 패턴에 따른 규칙인 rule 옵션을 만들어서 사용자가 정해둔 일정 규칙에 맞지 않는 패킷 접근이 발생한 경우 외부로부터의 비정상적인 접근이라고 간주하여 차단시키는 시스템이다. 아래의 표 1은 rule 옵션이 적용된 코드이고, 표 2는 rule옵션을 불러오는 코드이다.

표 1. Rule 옵션 적용 코드
Table 1. Rule Option Code

```
// IPS룰 적용하기
function loadrule() {
return new Promise(function(resolve, reject) {
var data = [];

//  패턴(룰) 정보 조회 부분
var sqlite = require('sqlite3');
var db = new
 sqlite.Database('/home/rule.db');
var query =
"select
sid,action,proto,direction,src_ip,src_port,dst_ip,dst_port,options
from rule";
db.serialize(function() {
db.all(query, function(err, rows) {
if (err) {
reject('err');
}
if (rows.length > 0) {
var cnt = 0;
rows.forEach((row) => {
data.push(row);
cnt++;
if (cnt == rows.length) {
resolve(data);
}
});
} else {
resolve(data);
}
});
});
db.close();
});
}
```

표 2. Rule 옵션 호출 코드
Table 2. Rule Option Call Code

```
source=sys.argv[1]
    f = open(source, 'r')
    lines = f.readlines()
    sid=0
    for line in lines:
        if len(line) > 0:
            idx = line.find(" ")
            if (line[0] != "#") & (idx > 0):
                # action proto src_ip src_port direction,
dst_ip, dst_port
                dst_ip=line[0:idx].strip()
                idx2 = dst_ip.find(":")
                if(idx2 < 0):
                    sid=sid+1
                    action=2
                    direction=1
                    src_ip="any"
                    src_port="any"
                    dst_port="any"
                    proto="ip"
                    service=""
                    udate=rdate
                    position=1
                    try:
                        cur_rule.execute(sql_fw,
(sid,action,yn_used,direction,src_ip,src_port,dst_ip,dst_port,prot
o,service,rdate,udate,position))
                    except Exception as ex:
                        print('Error : ', ex, line)
    f.close()
            conn_rule.commit()
    conn_rule.close()
```

표 3.은 사용자가 지정한 rule 옵션으로 외부의 비정상적인 접근에 대한 패킷 차단 rule옵션을 나타낸다. 그림 4.는 수리카타에 적용된 rule을 나타내고, 그림 5.는 수리카타로 차단 된 침입 현황을 보여준다. 그림 6.은 Node.Js를 이용한 UI로 사용자가 실시간으로 확인할 수 있는 차단 결과를 나타낸다.

그림 6.의 {ICMP}10.0.2.15:8->8.8.8.8:0은 ICMP 프로토콜 방식으로 해킹 시도자의 IP(10.0.2.15:8)가 해킹 대상 자동차의 IP(8.8.8.8:0)로 접근을 시도 하였다는 것을 의미한다.

표 3. 패킷 차단 rule 옵션
Table 3. Packet blocking rule option

```
#alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"외
부 네트워크 접속 차단";
content:"외부에서 접속하는 접속을 차단하였습니다."; sid:1; rev:1;)

$EXTERNAL_NET <- 외부의  any <- 모든 출발지

$HOME_NET <- 내부가 목적지인 any 모든 목적지 //외부에서 내부로
접근하는 모든 ip차단

//가속 룰
drop http any 881228 -> $HOME_NET any (msg:"Accel Block";
flow:established,to_client;                content:"flag";
pcre:"/.*\"flag\":[1],\"time\":[1-9]{1,}[0-9]/";   sid:0001;   rev:1;
classtype:automotive;)

//브레이크
drop http any 881228 -> $HOME_NET any (msg:"Break Block";
flow:established,to_client;                content:"flag";
pcre:"/.*\"flag\":[2],\"time\":[1-9]{1,}[0-9]/";   sid:0001;   rev:1;
classtype:automotive;)
```

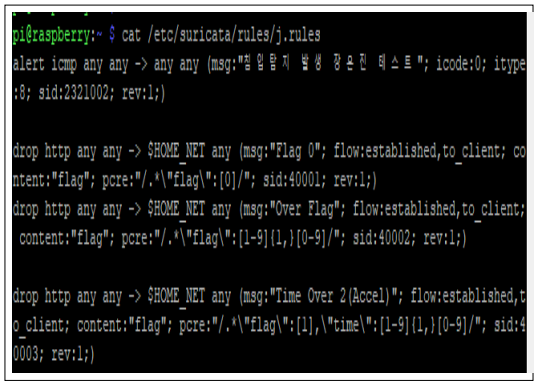

그림 4. 수리카타에 적용된 Rule
Fig. 4. Rule applied to Suricata

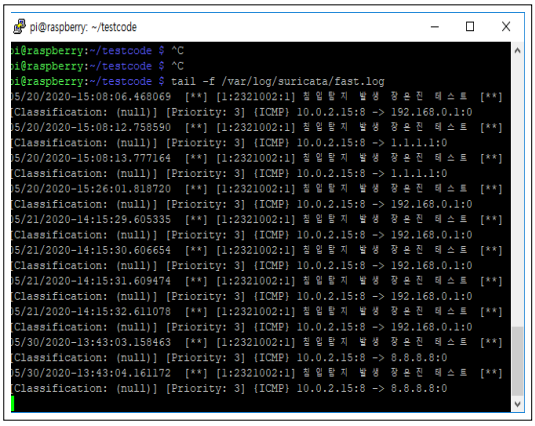

그림 5. 수리카타로 차단 된 침입 현황
Fig. 5. Intrusion status blocked by Suricata

내용
05/20/2020-15:07:45.488985 [**] [1:2321002:1] 침입탐지 발생 장은진 테스트 [**] [Classification: (null)] [Priority: 3] {ICMP} 10.0.2.15:8 -> 8.8.8.8:0
05/20/2020-15:07:46.520178 [**] [1:2321002:1] 침입탐지 발생 장은진 테스트 [**] [Classification: (null)] [Priority: 3] {ICMP} 10.0.2.15:8 -> 8.8.8.8:0
05/20/2020-15:07:47.524132 [**] [1:2321002:1] 침입탐지 발생 장은진 테스트 [**] [Classification: (null)] [Priority: 3] {ICMP} 10.0.2.15:8 -> 8.8.8.8:0
05/20/2020-15:07:48.528042 [**] [1:2321002:1] 침입탐지 발생 장은진 테스트 [**] [Classification: (null)] [Priority: 3] {ICMP} 10.0.2.15:8 -> 8.8.8.8:0

그림 6. 사용자가 실시간으로 확인할 수 있는 차단 결과
Fig. 6. Blocking results that users can check in real time

Ⅳ. 결 론

본 논문에서는 실시간 데이터 수집 및 처리가 필수적인 자율주행 자동차의 시스템 특성 상 외부의 해킹 위험에 노출될 확률이 높다는 것을 인지하고, 이에 대한 보안 안전성을 향상 시킬 수 있는 새로운 침입탐지시스템을 제안했다.

침입탐지 시스템은 사용자가 지정해둔 rule옵션의 기준치에 맞지 않는 비정상적인 접근이 발생할 경우 이를 차단시키는 새로운 데이터 처리 시스템이다.

이는 다양한 센서를 기반으로 작동되는 자율주행 자동차의 특성상 외부로 부터의 해킹이 발생할 경우 운전자 뿐만 아니라 주변 환경의 위험도 또한 높아질 것을 우려한 것으로 본 시스템을 적용하지 않았을 때보다 패킷 접근성의 안전성이 향상될 것으로 기대할 수 있다.

향후 본 시스템에서 보안 기능을 확대하여 패킷 접근에 대한 통제뿐만 아니라 센서 간의 데이터 통신을 방해하는 접근에 대한 보안 장치 및 보다 다중적인 보안 시스템에 대한 추가적인 연구가 진행되어야 할 것이다.

References

[1] http://news.khan.co.kr/kh_news/khan_art_view.html?art_id=201609211731001

[2] https://www.youtube.com/watch?v=AiP_CbPl64g

[3] Chang-Geun Hwang, Choong-Kee Lee, "An experimental study on improvement of administrative regulations in driving of autonomous vehicle", The Journal of The Law Reasearch institutute of Hongik Univ. Vol.17, No. 2, pp.27-59, 2016
DOI: https://doi.org/10.16960/jhlr.17.2.201606.27

[4] Min-Hwan Ok,"A Simulator Implementation of Highway Driving Guidance System for Longitudinal Autonomous Driving of ADAS-Driving Vehicles",Journal of KIIT. Vol. 17, No. 11, pp. 27-35, Nov. 30, 2019.
DOI:http://dx.doi.org/10.14801/jkiit.2019.17.11.27

[5] Hong Min, Jinman Jung, Taesik Kim,"A Decision Scheme of Dynamic Task Size for Cloud Server composed of Connected Cars",The Journal of The Institute of Internet, Broadcasting and Communication (IIBC) Vol. 20, No. 3, pp.83-88, Jun. 30, 2020.
DOI:https://doi.org/10.7236/JIIBC.2020.20.3.83

[6] Jin-mo Kim, Eun-jin Jang, Chang-Sik Jeong, Seung-Jung Shin, "Mixed reality health management model using smart phone", The Journal of the Convergence on Culture Technology (JCCT), Vol.4, No.2, pp. 185-189, May 2018.
DOI: https://doi.org/10.17703/JCCT.2018.4.2.185

[7] Kyung-Ah Yang, Dong-Woo Shin, Jong-Kyu Kim, Byung-Chul Bae, "Trend and Prospect of Security System Technology for Network", The Journal of The Institute of Internet, Broadcasting and Communication, Vol.18, No5, pp. 1-8, Oct 2018.
DOI:https://doi.org/10.7236/JIIBC.2018.18.5.1

[8] Jeong-A Kim, Jongpil Jeong, "Smart Warehouse Management System Utilizing IoT-based Autonomous Mobile Robot for SME Manufacturing Factory", The Journal of The Institute of Internet Broadcasting and Communication, Vol.18, No52, pp. 237-244, Oct 2018.
DOI:https://doi.org/10.7236/JIIBC.2018.18.5.237

[9] Md Foysal Haque, Hye-Youn Lim, and Dae-Seong Kang,"Real Time Object Detection Based on YOLO with Feature Filter Bank",Journal of KIIT. Vol. 17, No. 5, pp. 91-97, May 31, 2019.
DOI:http://dx.doi.org/10.14801/jkiit.2019.17.5.91

[10] Joon-Kyu Park, Keun-Wang Lee,"Analysis of Data

Characteristics by UAV LiDAR Sensor", Journal of the Korea Academia-Industrial cooperation Society Vol. 21, No. 5 pp. 1-6, 2020.
DOI:https://doi.org/10.5762/KAIS.2020.21.5.1

저 자 소 개

장 은 진(정회원, 교신저자)

•2012년 2월 : 단국대학교(학사) 식량생명공학과, 중국어학과
•2019년 2월 : 한세대 대학원 IT융합학과 (공학석사)

신 승 중(종신회원)

• 1988년도 세종대학교 대학원 경영학과 졸업(석사)
• 1994년도 건국대학교 대학원 전자계산학과 졸업(석사)
• 1999년도 국민대학교 대학원 정보관리학과 졸업(박사)
• 1995년~2003 중부대학교 정보보호학과 교수
• 2003~현재 한세대학교 ICT융합학과 교수
• 주관심분야 : 정보보호, 이동통신, 통신공학

※ 본 논문은 한국산업단지공단의 학술연구비를 지원받아 작성되었음.