A Study on Hacking Attacks and Vulnerabilities in Self-Driving Car with Artificial Intelligence

Se In Jung and Shin Dong Ho
Student and Professor, PAUL MATH SCHOOL
12-11, Dowontongmi-gil, Cheongcheon-myeon, Goesan-gun,
Chungcheongbuk-do, Republic of Korea
eavatar@hanmail.net

Abstract

AI-based self-driving vehicles use open networks and develop self-driving vehicles using ICT technology based on artificial intelligence on computer platforms. However, as hacking attacks on electronic control systems of self-driving vehicles have become possible, various hacking cases such as vehicle control system attacks and remote-control attacks have occurred. Cases of such hacking attacks are increasing the threat of hacking by outside attackers, and if self-driving cars become popular, the number of hacking cases will increase further. In this paper, we propose countermeasures for hacking attacks in terms of cybersecurity systems and technology to cope with hacking attacks. By separately presenting technology and institutional-centric security enhancement measures related to cybersecurity, it contributes to the construction of security for self-driving vehicles and the development of cybersecurity for unmanned defense robots. As security holes owned by self-driving technology are expected to leak personal information or cause personal injury, the need for security research on self-driving cars is increasing, and research on hacking attacks and security measures against self-driving cars is needed. As an additional research task, it is necessary to study the development of smart keys using NFC communication methods for self-driving vehicles and encryption programming methods for security authentication.

Keywords
Artificial Intelligence, Machine learning, self-driving vehicles, AI and hacking attacks

1. Introduction

In this paper, the attack scenario for this vulnerability is described after presenting the attacker's ability and hacking attack method based on the attack model for autonomous vehicles. This attack scenario uses software and networks. A miniature model in which autonomous vehicle technology is integrated can be produced and tested. Self-driving vehicles have built-in electronic control systems and specialized software for communication between internal devices, and attack scenarios and countermeasures are studied from the perspective of the internal systems of autonomous vehicles through various communication methods.

By transmitting and exchanging via Wi-Fi and RF (Radio Frequency) applied to most vehicles, the electronic devices of the vehicle's internal network are controlled, and the vehicle is driven by executing commands according to the situation. This allows cyber attackers to manipulate the internal systems of autonomous vehicles and drone bots at will through forged messages that can control the main systems if they penetrate the internal systems of autonomous vehicles. In addition, software embedded in recently released vehicles has a vulnerability that allows an attacker to take control of the vehicle. An attacker who has penetrated the internal system can take control and perform an attack that can directly affect safety, such as a brake failure of a vehicle.

An autonomous vehicle model is controlled using a smartphone or PC, and communication uses Wi-Fi, RF, and Bluetooth. Therefore, each communication step-by-step attack process is verified through an experiment. Based on the experiments and research results of this paper, we study the security measures to identify vulnerabilities that appear in attacks on autonomous vehicles and respond to them.

2. Body

2.1. Autonomous vehicle technology

This paper performs S/W vulnerability attack and network attack on autonomous vehicle with AI function. Based on the results of the cyber attack, set the security method for the discovered vulnerability, and confirm that the security against the attack is reinforced after the security measures. Introduction of AI-based autonomous vehicle technology, machine learning technology of autonomous vehicle, S/W of autonomous vehicle, and network attack method are analyzed. By analyzing S/W and network attack methods for artificial intelligence functions and cyber attacks, S/W and network-related security measures for vulnerabilities are presented.

The level of autonomous driving is defined by the National Highway Traffic Safety Administration (NHTSA) as Level 4 and the Society of Automotive Engineers (SAE) as Level 5. SAE 4 and 5 are the same as NHTSA 4, and the difference between SAE 4 and 5 is whether or not unmanned driving is supported. The level of autonomous driving is defined by the Society of Automotive Engineers (SAE) as Levels 1 to 5 and the National Highway Traffic Safety Administration (NHTSA) as Levels 1 to 4. Table 1 introduces the autonomous driving stages defined by SAE, and NHTSA stage 4 corresponds to SAE stage 4-5.(Kwon, 2017).

In order to realize autonomous driving at SAE level 3 or higher, cooperative autonomous driving that combines autonomous driving and cooperative driving is required. The trend of automobile technology for autonomous driving can be defined as the expansion of connectivity and the efficiency of the network with the inside of the vehicle.(Kwon, 2017). In a highway environment, the service combining ACC and LKS (Lane Keeping System) maintains a distance from the vehicle in front, and while driving along the lane, the driver can receive control at any time as needed.

Current autonomous vehicle technology uses Lidar and Global Positioning System (GPS) to recognize the surrounding road environment and locate the vehicle. In addition, distributed processing is performed using a plurality of computer clusters for recognition information processing and judgment. In order to control operation, speed, and gear, the functions are controlled through modifications such as adding motors and sensors.(An et al., 2013).

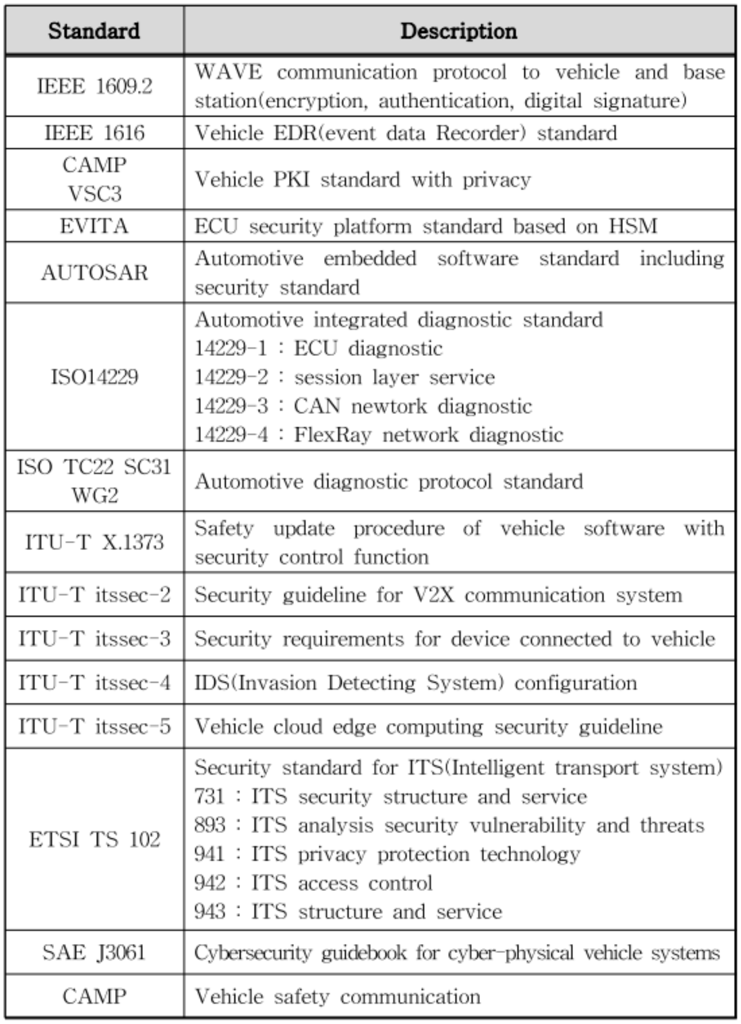
For safe autonomous driving, it is important to be aware of the surrounding road environment. These cognitive technologies are recognized by integrating ADAS (Advance Driver Assistance System), V2X (Vehicle to Everything), and maps. ADAS is to determine the surrounding road environment using equipment such as radar, camera, and lidar. V2X is a technology that recognizes the surrounding traffic environment with a wide field of view through communication between OBU (OnBoard Unit) and RSU (Road Side Unit) possessed by each vehicle. Finally, there are GPS and precision maps. When this information is collected, the result determined using an artificial intelligence algorithm is transmitted to each device of the autonomous vehicle for control.(Sim, 2014).

Situation awareness, judgment, and control must work convergence, and driving can be dangerous if a problem occurs in one part by an attacker. In 2015, Black Hat Europe successfully attacked LiDAR systems and cameras installed in cars. Based on these cases, an attack on the camera can be attempted, but the camera acts as the eyes of an autonomous vehicle. Therefore, the deep learning used for image recognition can be hacked and the user can have the computer judge unknown information, which can lead to dangerous results.(Sim et al. 2014).

The first attack of the camera is an attack that paralyzes the function of the camera by inserting a laser into the camera. The attack must be performed after finding the appropriate light intensity for the attack according to the light intensity of the surrounding environment. Second, the attack is a method of attacking the automatic adjustment function in order to interfere with the stabilization of the system. Because the laser is always shooting, the camera has a problem that it is difficult to detect a hacker attack. As a countermeasure against this, standardization related to vehicle security is prepared as shown in Table 1.

As an autonomous driving sensor attack issue, the radar, lidar, camera, and ultrasonic sensors installed in autonomous vehicles are vulnerable to attacks such as espoofing, jamming, and Denial of Service (DoS). Research is needed, such as how to respond to physical attacks. Currently, related research is mainly conducted in terms of recovery / restoration in case of sensor attack.(Seo et al., 2018). As the next-generation Internet of Things (IoT) autonomous vehicle security, it is also necessary to consider the security of autonomous vehicles in a connected environment in the form of IoT. This is because the threat increases as the connection expands and diversifies. In particular, there is a need for research on deriving and solving security threats in an environment in which transportation infrastructure, ICT infrastructure, and autonomous vehicles are all converged.

Table 1. Standardization related to automobile security



Standard	Description
IEEE 1609.2	WAVE communication protocol to vehicle and base station(encryption, authentication, digital signature)
IEEE 1616	Vehicle EDR(event data Recorder) standard
CAMP VSC3	Vehicle PKI standard with privacy
EVITA	ECU security platform standard based on HSM
AUTOSAR	Automotive embedded software standard including security standard
ISO14229	Automotive integrated diagnostic standard 14229-1 : ECU diagnostic 14229-2 : session layer service 14229-3 : CAN newtork diagnostic 14229-4 : FlexRay network diagnostic
ISO TC22 SC31 WG2	Automotive diagnostic protocol standard
ITU-T X.1373	Safety update procedure of vehicle software with security control function
ITU-T itssec-2	Security guideline for V2X communication system
ITU-T itssec-3	Security requirements for device connected to vehicle
ITU-T itssec-4	IDS(Invasion Detecting System) configuration
ITU-T itssec-5	Vehicle cloud edge computing security guideline
ETSI TS 102	Security standard for ITS(Intelligent transport system) 731 : ITS security structure and service 893 : ITS analysis security vulnerability and threats 941 : ITS privacy protection technology 942 : ITS access control 943 : ITS structure and service
SAE J3061	Cybersecurity guidebook for cyber-physical vehicle systems
CAMP	Vehicle safety communication

Autonomous vehicles are equipped with intelligent and cutting-edge ICT technologies that can be said to be equipped with computers. Therefore, there is a possibility of receiving a cyber hacking attack on the car. A vehicle can be divided into a drive unit responsible for movement, an electronic control unit (ECU) that controls the engine and transmission of the vehicle, and an infotainment system that connects the inside of the vehicle to the outside.

The ECU can be controlled by CAN (Controller Area Network), and an attacker can use CAN to suddenly brake the vehicle or malfunction the brake pedal in the ECU area. In the infotainment part, the 'Mirror Link' technology was found as a weakness in the car's internal navigation. AVN (Audio, Video, Navigation) systems are also vulnerable to vulnerability attacks through CD and hacking through GPS, and malicious codes can be infected through files transmitted externally using Bluetooth.(Kim and Lee, 2017)

First of all, the hardware used for the experiment is an autonomous vehicle model composed of an Orange Pi board, a camera, a sub-motor for wheels, and an acrylic board for the exterior of the car. The Orange Pi board, which plays a key role, is operated by Linux OS (Armbian) and can be used like a general computer by connecting a keyboard, mouse, or monitor. ReplayAttack is an attack in which the attacker saves the message the user communicated with the server in the last session, and then retransmits the same message in the subsequent session to be authenticated as normal by the server. In other words, it is an attack disguised as a legitimate user by selecting a valid message on the protocol, copying it, and retransmitting it.

In the second experiment in this paper, after saving the signal source, the attack was conducted to retransmit this signal back to the device, and the experimental result was confirmed.(Choi, 2017).

2.2. Attack on S/W of autonomous vehicle

The system proposed in this paper was tested in an indoor environment. A road with a combination of curved and straight lines of 30 cm in width (based on twice the width of the model car) was installed on the floor with two black (tape) lines with a length of 4 m. The experiment was conducted with an autonomous driving (model) vehicle, and the specifications and system configuration of the model vehicle are as shown in Figure 1.(Orange pi board, 2016).

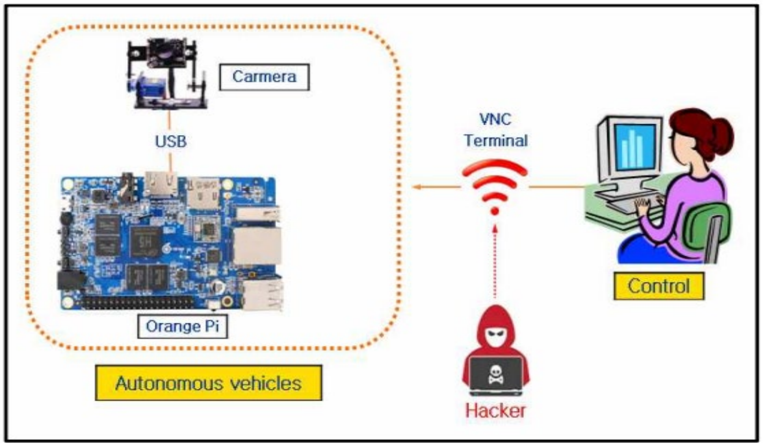


Figure 1. Autonomous Vehicle Hacking Attack Experiment System Configuration

This is to block the h4ckerAP (Wireless Access Point) connection that connects the laptop and the autonomous vehicle. Directly inputting the SSID and MAC address, the Death packet is transmitted to block the connection. When the connection is disconnected, an error is detected immediately and reconnection is attempted, so the packet is continuously transmitted in seconds.(Jeon, 2015). Autonomous driving vehicles for road driving are capable of driving on a fixed road, but in case of a hacking attack in an emergency or when the driver's direct control is required, the Wi-Fi network of the autonomous driving vehicle is blocked and training and control are impossible.(Lee, 2017).

2.3. Network attacks on autonomous vehicles

In this study, the self-driving vehicle has the same access door system as the general vehicle, so instead of the autonomous vehicle, an RF (Radio Frequency) hacking attack experiment was conducted on the K company's S model vehicle, and the configuration of the experimental system was (It is shown in Figure 2). HackRF One is an SDR (Software Defined Radio) device capable of transmitting and receiving radio signals from 1Mhz to 6Ghz.

URH (Universal Radio Hacker) is a Windows-based Open Source, complete radio protocol investigation software that natively supports radio frequencies. It allows for automatic detection of modulation parameters and easy modulation of the signal, making it easy to identify bits and bytes in the air. As shown in (Figure 3), input 433.92Mhz to Frequency, click the start button, and then press the car smart key door open button 4 times to collect the radio signal of the smart key through the HackRF One device.

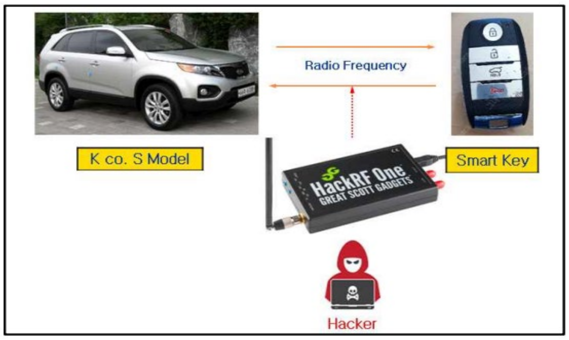
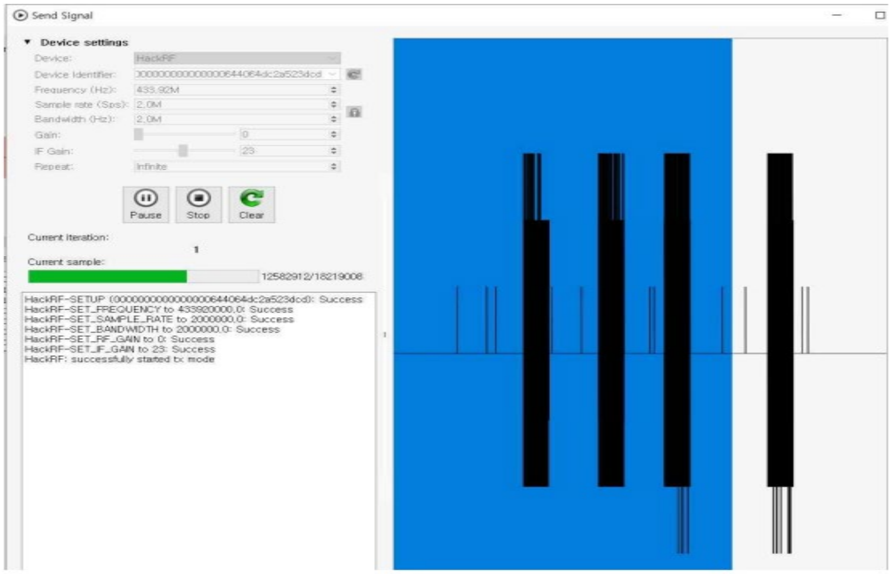


Figure 2. Hack RF ONE Hacking Attack Experiment System



```
▼ Device settings
Device:                HackRF
Device Identifier:     0000000000000000644064dc2a523dcd
Frequency (Hz):        433.92M
Sample rate (Sps):     2.0M
Bandwidth (Hz):        2.0M
Gain:                  0
IF Gain:               23
Repeat:                Infinite

Current iteration:
1
Current sample:
12582912/18219008

HackRF-SETUP (0000000000000000644064dc2a523dcd): Success
HackRF-SET_FREQUENCY to 433920000.0: Success
HackRF-SET_SAMPLE_RATE to 2000000.0: Success
HackRF-SET_BANDWIDTH to 2000000.0: Success
HackRF-SET_RF_GAIN to 0: Success
HackRF-SET_IF_GAIN to 23: Success
HackRF: successfully started tx mode
```

Figure 3. Car smart key frequency transmission

URH (Universal Radio Hacker) is a Windows-based Open Source, complete radio protocol investigation software that natively supports radio frequencies. It allows for automatic detection of modulation parameters and easy modulation of the signal, making it easy to identify bits and bytes in the air.(WIRED, 2016). As shown in (Figure 3), input 433.92Mhz to Frequency, click the start button, and then press the car smart key door open button 4 times to collect the radio signal of the smart key through the HackRF One device.

If the collected smart key signal is played, the locked car door is opened even without the smart key as shown in Figure 3. Therefore, if you use HackRF One equipment, you can analyze the frequency used for communication between devices, so the user's signal can be easily eavesdropped, and hackers can try retransmission attacks. Physical damage may occur due to cyber hacking attacks such as vehicle theft.

2.4. Security measures for S/W vulnerabilities of autonomous vehicles

In-vehicle communication maintains data integrity between communications through message authentication through MAC information. In data communication with other ECUs in the vehicle, using the MAC information shared with the message at the manufacturing stage, reliability verification is performed in the sensor verification procedure to prevent forgery of messages. It is possible to implement a cyber security self-driving vehicle environment enhanced through hardware authentication and user authentication that can respond to illegal access to autonomous vehicles and spoofing attacks, and encryption in data and communication sections to respond to wiretapping and information leakage on the network. . Accordingly, cyber security countermeasures and security application technologies were derived for each security threat in the autonomous vehicle environment.

Autonomous vehicle hardware hacking threat prevents data exposure by extracting memory through data encryption (public key encryption), and cyber security response is possible by removing the functions of interfaces such as LIN (Local Interconnect Network) and UART (Universal asynchronous receiver/transmitter) to hardware do. The threat of information exposure of vehicle drivers can be countered by cyber security through public key driver information data encryption, autonomous vehicle management system, biometric authentication (iris and fingerprint recognition), and vehicle identification number.

The threat of control right through control data forgery attack between wireless communication is countered by providing integrity when communicating with smart devices of MD5 (Message-Digest algorithm 5) and AES (Advanced Encryption Standard), and authentication threats through forged user information are It is possible to respond to hacking attacks by verifying forgery and verifying integrity through user authentication and user authentication.(An et al., 2017).

Data transmission threats related to communication interference between vehicle sensors and systems can respond to hacking attacks through authentication techniques that only authenticated devices and users can use when communicating between vehicles and systems. In this way, when cyber security technology is applied and technical support is provided to counter hacking of autonomous vehicles, a popularized autonomous driving society can be built based on the safety of autonomous vehicles.

2.5. Security measures for network vulnerabilities in autonomous vehicles

In this study, we tested the vulnerability of hijacking the vehicle by duplicating the smart key radio wave of the autonomous vehicle and found a weakness that can easily analyze the communication frequency using the RF transceiver, and it is possible to easily listen to the user's normal signal. Yes, through this, an attacker can try a retransmission attack.

Encrypting the communication contents of the smart key prevents data tampering and communication protocol information leakage, but is vulnerable to retransmission attacks that replicate and transmit encrypted data identically. Therefore, in order to solve the vulnerability of the retransmission attack, it is necessary to verify the RF signal used for communication between the autonomous vehicle smart key devices.

As a result of testing using a case where aluminum foil was wrapped outside the smart key and the smart key was stored in an electromagnetic wave blocking pouch in order to compensate for the vulnerability to prevent theft of autonomous vehicles, after using the actual smart key, aluminum foil and an applied smartphone with electromagnetic wave blocking function It has been confirmed that it is safe for cyber security when using the case.

3. Conclusion

In this paper, in an experimental model of an autonomous vehicle equipped with an AI function, a hacking attack in a normal communication state is performed, security vulnerabilities are discovered, and a model to establish security measures is proposed.The self-driving vehicle is an orange pie-based self-driving vehicle that is directly controlled with a laptop, and machine learning training is implemented to communicate via Wi-Fi. When the autonomous vehicle and the laptop were connected, image information was output through the camera on the front of the autonomous vehicle, and while checking real-time image information, four motors were driven to make forward-reverse-left-right rotation possible. Connected between the autonomous vehicle and the laptop due to the S/W attack of the autonomous vehicle

The vulnerability was confirmed by performing a hacking attack on the Wi-Fi network. In addition, the RF vulnerability of the smart key was confirmed by the network attack in the autonomous vehicle as well. Although many studies on autonomous driving vehicles and V2X wireless communication at home and abroad are being conducted, research on system security of autonomous vehicles equipped with various sensors and artificial intelligence functions is insufficient. An overview of autonomous vehicles and security vulnerabilities were confirmed through hacking attack test results, and cyber security measures for vulnerabilities in autonomous vehicles and AI were introduced for cyber security measures. In order to compensate for the vulnerabilities for, the results of security enhancement using aluminum foil and electromagnetic wave blocking pouch are presented.

As a result of the hacking attack, it was found that cyber security against attacks is safe when using aluminum foil and electromagnetic wave blocking function as a substitute for smart key case. A technical solution for cybersecurity against the cyberattack threat of Wi-Fi and Bluetooth is presented.

Reference

Kwon, H. C. "Smart car trendsand security issues interms of connectivity.", *Journal of the Korea Telecommunications Society (Information and Communication),* Vol34, No.10, pp.17-23, 2017.

Kwon, H. C., S. J. Lee, J. Y. Choi, B. H. Chung, S. W. Lee, J. C. Nah, "Trends in autonomous vehicle security technology", *Electronics and Telecommunications Trends,* Vol.33, No.1, pp.78-88, 2018.

An, K. H., Lee., S. W., W. Y. Han, J. C. Son, "Autonomous driving technology trends", *Electronics and Telecommunications Trends,* Vol.28,No.4, pp.35-44, 2013.

Seo, H. J., Kwon, Y. B., Kwon, H. D., An, K. H., "Security trends for autonomous vehicles", *Korea Institute Of Information Security And Cryptology,* Vol.28, No.5, pp.9-14, 2018.

Kim, Y. J., Lee, Y. S., "Vulnerability and security considerations of autonomous vehicles", *Proceedings of the Korean Society for Computer and Information Science Summer Conference*, Vol. 25, No.2, pp.165-168, Jul. 2017.

Choi, S. Y., "RF communication environment Replay Attack Vulnerability analysis", *Korea University Information Protection Department of Cyber Securityp.* 6, 2017.

A Feasibility Study on Driving Technologies for Dedicated Freeway Construction," *KISTEP*, pp.154, May 2016.

Sim, S., and Kim, D., and Lee, Y., "*Security Technologies for V2X Communication*," April 2014.

Jeon, H., and Lee. S. J., "*Driver gives freedom to the driver, Traffic accidents are Zero,"* pp.3, May 2015.

Orange pi board, "*What's Orange Pi Pc Plus ? "*, Available: http://www.orangepi.org/, 2016.

Business Insider, "*These car keys are so ridiculously high-tech you won't even recognize them"*, Available:
https://www.businessinsider.com/8-amazing-car-keys-2016-3, Mar. 2016.

WIRED, *"Radio Attack Lets Hackers Steal 24 Different Car Models",* Available:
https://www.wired.com/2016/03/study-finds-24 -car-models-open-unlocking-ignition-hack/, 2016.

Lee., W., "*Car smart key hack, how long will you turn away",* Available:
https://m.post.naver.com/viewer/postView.nhn?volumeNo =8508344&memberNo=28648285,Jul. 2017.

Defense and Technology, "The Army establishes a dronebot combat group", *Korea Defense Industry Association,* No.477, pp.14-16, 2018.

Defense Inside, *"AI unmanned robot...Easy removal of ballpoint pen explosives"*, Available:
https://news.naver.com/main/read.nhn?mode=LPOD&mid =tvh&oid=215&aid=0000810398, Sep. 2019.

The PiHut,"*The Raspberry Pi Tutorial-A Beginner's Guide"*, Available: https://thepihut.com/blogs/raspberry-pi-tutorials/the-ras pberry-pi-tutorial-beginners-guide, May. 2019.

Biography

Se In Jung is graduated in MY PAUL SCHOOL. She is interested in artificial intelligence, deep learning, cryptography, robots, block chains, drones, autonomous vehicles, etc., and is conducting related research.

Shin Dong Ho is Professor and Teacher in MY PAUL SCHOOL. He obtained his Ph.D in semiconductor physics in 2000. He is interested in artificial intelligence, deep learning, cryptography, robots, block chains, drones, autonomous vehicles, the Internet of Things, metaverse, virtual reality, and space science, and is conducting related research.