Awesome project

z5321907 Longyu Gao

The title of my awesome project is “Autonomous Vehicle Security: Attacks and Defenses”.
It is a little essay about learning and analyzing Autonomous Vehicle’s security.
This report will be displayed in the following structure:
1. Evidence of 30hrs of work. It also contains brainstorming, research, planning phases and construction phases
2. Assay. It contains Introduction, Autonomous vehicle’s structure and system, Attacks on autonomous vehicles, Analysis of methods to defense various attacks, Design prospect of autonomous vehicles in the future and References.
3. Reflection phase. It contains what I learnt, challenges I faced, would I do differently.

Evidence of 30hrs of work.

WEEK 1-2
I thought about several project topics and discussed with tutor. She reminded me kindly that the big data privacy is a huge topic, and I should choose a specific topic. Then, I saw the automatic driving in the process of searching safety related topics. I thought that people often talk about the security of the driving ability of autonomous vehicles, but driving ability should only be a function of it. For the safety of autonomous vehicles, we should comprehensively analyze it from the perspective of one vehicle. Then, I began to search the literature, hoping to learn the structure and system of autonomous vehicles.

WEEK 3
I found an overview of autonomous vehicles in the searched literature, which introduces the structural characteristics, sensors and other components. This gives me some basic knowledge to determine the project structure: learn the autonomous vehicle system, investigate the methods of attacking vehicles, and analyze the methods of defending against attacks.

WEEK 4-5
I learned the electronic control unit, the three-layer core structure system and the sensor system of autonomous vehicles. I investigated and classified the attack methods against traditional and autonomous vehicles.

WEEK 6-7
I analyzed possible defense methods against various attack methods.

WEEK 8
I learnt intelligent transportation system and put forward my opinions on the design of autonomous vehicles in the future

Autonomous Vehicle Security: Attacks and Defenses

z5321907 Longyu Gao

1. Introduction

On February 10, the California transportation administration DMV released the new automatic driving data for the whole year of 2021. Data show that as of February 7, 2022, a total of 50 enterprises were granted automatic driving test licence in California, and nearly 1000 autopilot cars were put into operation. There were 117 collision accidents. This makes autonomous vehicles a hot topic again. However, when various media and commentators judge the safety of autonomous vehicle driving technology, the most basic nature of it, vehicle, is ignored. Autonomous vehicles belong to vehicle firstly. It has the physical security attributes and cyber security attributes of general vehicles. Then, it has the safety attributes of its unique sensors, electronic components and other new driving technologies.

Therefore, this paper will take a correct and comprehensive view of autonomous vehicles, introduce its basic structure, compare the similarities and differences between autonomous vehicles and the traditional vehicles, discuss and organize a variety of attack methods against it, put forward corresponding defense means in combination with the characteristics of autonomous vehicles, and finally look forward to the design focus in the future according to the defense means which needed to be strengthened.

2. Autonomous vehicle’s structure and system

The physical structure of modern vehicles usually includes, engine, chassis, body and electrical equipment. The engine is the main structure to supply kinetic energy to the vehicle. Chassis is the basic structure that transmits engine power to wheels to complete vehicle driving and braking. The vehicle body is used to accommodate the driver, passengers, and goods. Electrical appliances are composed of power supply, automobile lighting system, signal instrument, etc.

With the development of science and technology, the electronic structure of modern vehicles has changed dramatically. Today’s automobile contains a myriad of computers. These computers called electronic control units (ECUs) that are connected to each other via different kinds of bus systems in order to reduce cables needed. Different ECUs have different functions, and they are combined into different modules such as engine, monitor sensors, emergency brake and transmission. Indeed, one recent estimate suggests that the typical luxury sedan now contains over 100 MB of binary code spread across 50–70 independent computers—Electronic Control Units (ECUs) in automotive vernacular—in turn communicating over one or more shared internal network buses.

Comparing to traditional vehicles, autonomous vehicles ones require almost no human inputs for driving control, therefore it relies purely on the on-board computing systems, which in turn depend on sensors and their measurements of the surroundings to make driving decisions. Therefore, the key structures and systems of autonomous vehicles will focus on the communication between vehicles and the environment and the processing of environmental data. There are two main types of communication between autonomous vehicles and the environment, one main type is the inter-vehicular (V2V, vehicle-to-vehicle) communications that occurs on the road via the vehicular ad hoc networks (VANETs). The second main communication method is the communication between vehicles and networked transportation equipment and facilities. Such scenes will appear more in the tide of the Internet of things in the future, which will be discussed in the prospection part at the end of the article.

However, no matter what kind of communication method is used, autonomous vehicles will be loaded with more sensors, such as millimeter wave radars, ultrasonic sensors and forward-looking cameras, to collect enough environmental data. After obtaining the data, the sensor and a large number of ECUs will interconnected via the controller area network (CAN) bus which acts as a central network where different modules can be added to or removed from it without affecting the entire vehicle's wiring architecture. The CAN bus is currently structured into three parts: Data link layer (responsible for transferring data between adjacent network nodes), High-speed CAN physical layer, Low-speed fault tolerant CAN physical layer. The High-speed CAN physical layer contains important ECUs such as engine control ECUs, emergency brake control ECUs. Other ECUs which do not have influence on the running of the vehicle like the radio and air conditioner, are connected to the low-speed CAN layer. Between these two layers, there is a gateway bridge which can route selected data between these two layers.

Now we have known that the physical structures, electronic devices, ECUs, CAN and so on about the autonomous vehicles. It is clear that the safety problem of driving technology of autonomous vehicles widely concerned by the society is only the linkage of several modules in the vehicle high speed CAN physical layer. Therefore, if we want to analysis and discuss the security roundly, we must search various dangers against autonomous vehicles from many aspects, which we will discuss in the next part. Then, to defense.

3. Attacks on autonomous vehicles

The basic structure and system of autonomous vehicles are introduced above. According to different component structures of the vehicle, attackers will have different attack methods, resulting in different effects. This section will discuss the classification and motivation of attackers, and analyzes the different attack methods, targets and corresponding effects for different component structures of vehicles.

First of all, we can divide attackers into hackers, thieves and terrorists. Hackers mainly attack for the purpose of collecting vehicle information and obtaining vehicle location. Thieves mainly obtain economic benefits by affecting vehicle functions, such as unlocking the vehicle, starting the vehicle without a key, etc. Terrorists directly or indirectly cause vehicle accidents and

casualties by affecting the normal driving of vehicles and even obtaining vehicle control. According to the attacker type and purpose, the classification of attack methods can be shown by this figure.

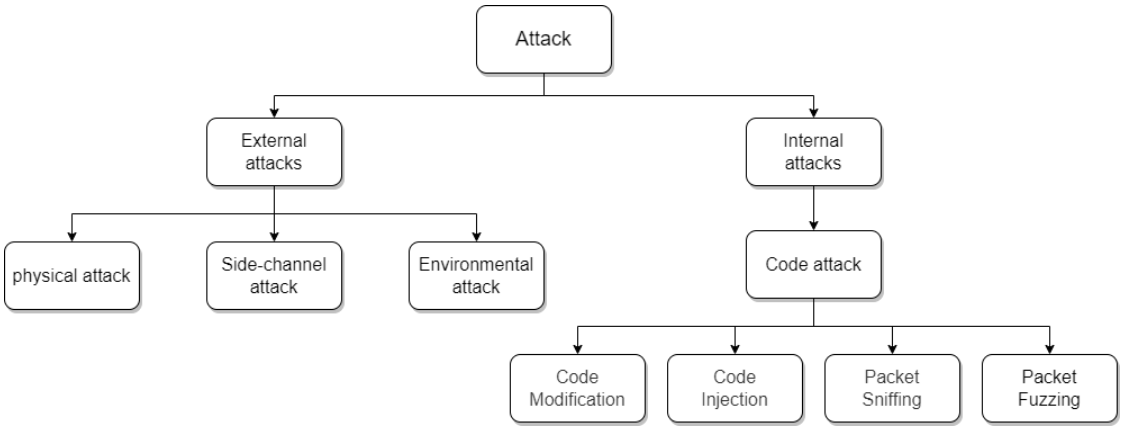

Fig.1: Classification of attack methods

3.1 External attack

External attack means that the attacker does not invade, affect or modify the internal code of the autonomous vehicle, but carries out physical attack or environmental interference from the outside of the vehicle.

3.1.1 Physical attack

The most common and simplest way to enter the vehicle. The objects it targets include windows, door locks, trunk locks and other physical structures. Thieves or robbers without technical support usually enter the vehicle by prying the lock, smashing the window and other methods, steal cash or goods in the vehicle, and even forcibly start the vehicle to steal it. Generally, physical attack will only cause the owner's property loss, vehicle damage or theft, and will not pose a threat to the personal safety of the owner and passengers.

3.1.2 Side-channel attack

Different internal components of the general vehicles and its ECUs transmit data through the data link layer for interaction, and ECUs also interact frequently, which will generate information that can be captured, such as electronic leaks, acoustic signal, etc. Autonomous Vehicles contain more ECUs, and the vehicle will also interact with other vehicles and transportation facilities, which will produce more leakage signals. Hackers use signal receiving equipment and electromagnetic detectors to obtain the geographical location, driving speed and real-time control operation of the vehicle by capturing and analyzing timing information, power consumption, electronic leaks, acoustic signal analysis and data removal. Side-channel attacks will disclose the travel information of car owners and passengers, which may indirectly cause safety problems for passengers.

3.1.3 Environmental attack

General vehicles interact less with the environment during driving, including only GPS and a few detectors. However, autonomous vehicles rely heavy on their sensor ability of their surroundings to make driving decision, which means that these mechanisms are the eyes and ears of the car. We know that people's eyes and ears can be tricked, so does cars. Sensors whose measurements are used to guide driving such as millimeter-wave radars, ultrasonic sensors, forward-looking cameras and GPS can all be tricked by intentional attacks. Sensor attacks utilize the same physical channels as the targeted sensor in most cases, which can disrupt or manipulate the sensor readings. Since sensors are categorized as the underlying layers of a control system, they are normally trusted, which means that the falsified readings could lead to unexpected decisions of the driving system and serious consequences.

The following figure shows the sensor distribution of an autonomous vehicle, in which ultrasonic sensors, MMW radars, cameras, and LIDAR are independent sensors on current autonomous vehicles. Because the physical principles underlying these technologies varies, their operation ranges are different as well, Proximity (5 m), Short Range (30 m), Medium Range (80 m) and Long Range (250 m).

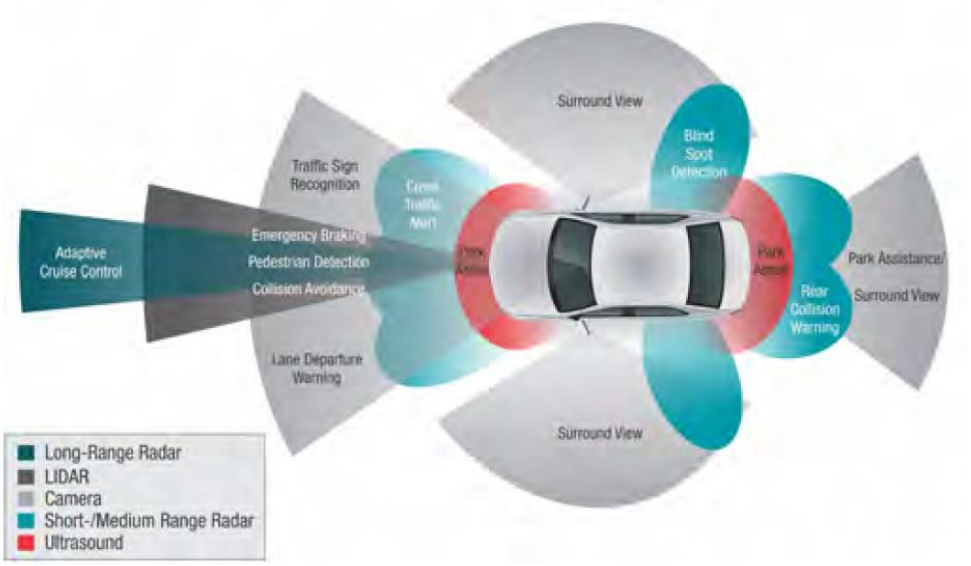

Fig. 2: Sensor distribution of an autonomous vehicle

There are three kinds of waves are used for detecting barriers and road condition. Ultrasonic sensors detect obstacles by transmitting and receiving ultrasound. MMW radars rely on millimeter waves. Both LIDAR and cameras rely on lights to recognize objects. Because each type of sensors rely on a distinct underlying principle, various methods and equipment have to be utilized to attack each type of sensors. However, all attacks on sensors can be divided into jamming attack and spoofing attack. Jamming attack means that hacker injected noise to lower the Signal to Noise Ratio (SNR) and make the detection of car impossible. Although sensors are designed to resist environmental noise, their ability to resist intentional noise is uncertain. Spoofing Attack is more elaborate attack, it is also a way to inject signals, but it can emulate physical patterns of the real ones, which makes it possible for them to be taken as real measurements, so as to disrupt sensor readings.

Attack Ultrasonic sensors. The principle of the Ultrasonic sensors is to emit ultrasonic pulses, and measure the time taken for the echo pulses to be reflected back from the first obstacle to detect objects nearly. Jamming attack aims to generate ultrasonic noises and cause continuing vibration of the membrane on the sensor, which make the measurements impossible. Spoofing Attack is that hackers or terrorists send a signal which can arrive at the sensor ahead of the real ones and can be recognized as echoes from obstacles. In this way, attackers can create a non-existent obstacle and affect the judgment of autonomous vehicles.

Attack MMW radars sensor. The working principle of MMW radars sensor is similar to that of ultrasonic sensor. It detects multiple obstacles at a long distance by transmitting modulated electromagnetic wave and receiving demodulated electromagnetic wave. Due to the fast propagation speed of electromagnetic wave, we can't use the calculation method of ultrasonic wave, but the frequency shift of electromagnetic wave. If an object moves relative to the radar, the reflected electromagnetic wave will undergo a frequency shift, which is described as Doppler effect. The 76.5 GHz range Bands, which is exclusive for automotive radar and available worldwide, dominates at present. Therefore, the attack mode of MMW radars sensor is to modulate 76.5ghz electromagnetic wave. Jamming attack is to produce high noise signal to reduce the signal-to-noise ratio of reflected electromagnetic wave. Because only when the signal-to-noise ratio is high enough, the sensor will receive the current signal. Spoofing attack will modulate the long-distance false obstacle electromagnetic wave immediately after detecting the electromagnetic wave emitted by the sensor. The fake wave will connect to the real reflected electromagnetic wave, and return to the sensor together to create a false long-distance obstacle.

Attack camera. With the continuous development of machine learning, more and more efficient image recognition technology has been applied to vehicle cameras. Autonomous vehicles use it to identify environmental factors such as road markings, vehicle number plates, road pedestrians and so on. The data of camera can be combined with the data of other sensors to help vehicles make more authoritative driving decisions. The basic principle of the camera is to receive optical signals through CCD / CMOS devices and generate images in the camera module. However, photoelectrical sensors are very sensitive to the intensity of light. At the same time, its absorption peak is limited and easy to be damaged under strong light irradiation. Therefore, the attack method on the camera is to use LED lights or laser light to illuminate the camera lens, resulting in blindness or damage to the camera.

To sum up, environmental attacks actually are to interfere with the normal driving decisions of autonomous vehicles. Existing sensors might not reliably detect nearby cars even in some special road conditions, not to mention intentional attacks against these sensors by terrorists or hackers with high-tech capabilities. This will pose a serious threat to the personal safety of passengers. In addition, although the current sensors have fair filtering function for noise, there is no special design for the noise or signal of malicious attack, which make it easy to be affected or deceived. In an experiment about the Tesla Model S, all targeted attacks have played an obvious interference effect, leading to many wrong decision-makings of vehicles, which is very prone to accidents.

3.2 Internal attack

3.2.1 Code attack

The autonomous vehicles have a diagnostic OBD-II port which is an opening where people can connect to. Meanwhile, if the vehicle is connected to the external network through mobile phone or vehicle management platform, it will be possible for external users to connect to the vehicles. In this connection state, users can gain access to the vehicle's bus systems and ECUs, and various types of code attacks also occur at the same time. Code Modification, The OBD-II scanner is a tool which has a chip-tuning feature which is able to extract and modify ECU codes. If an attacker can get close to a vehicle, it can maliciously modify the code through OBD-II scanner, thus affecting the system of the vehicle. Code injection: different from code modification, any user who can access to the vehicle's networks and ECUs can inject code into the autonomous vehicle, which means that remote access attack is possible. Once malicious payloads such as viruses and spyware are injected into the vehicle system, ECUs and vehicle function modules will be severely affected. Packet Sniffing: A packet sniffer can intercept and log traffic that is transmitted over a communication link. Through it, hackers can obtain the unencrypted data transmitted between the vehicle ECUs and each layer to execute data collection and replay attacks so as to monitor the vehicle status and disrupt the vehicle system. Packet fuzzing: when invalid data packets are sent to the vehicle internal module, unknown vulnerabilities or errors may be triggered, causing unexpected damage to the vehicle.

4. Analysis of methods to defense various attacks

4.1 Physical attack

Although physical attacks do not need technologies, they are simple and brutal. There are few corresponding defense methods for such violent entry. It is unrealistic to popularize explosion-proof windows and thick solid body structures for each vehicle. Therefore, our defense measures should focus on preventing attacks and coping methods after being attacked. The first defense method is to implement a stricter access permit system for private garages or public parking lots to minimize the access of irrelevant personnel. The second method is to combine a more sensitive theft response system using the characteristics of different sensors of autonomous vehicles, such as face recognition through camera, recording strangers around, and detecting the proximity and residence time of personnel with ultrasonic sensors. The third one is to bind the vehicle theft alarm with the mobile phone. It can remind the risk of theft, use GPS to track the stolen vehicle, automatically lock the computer driving after confirming the theft, and set the police station as the destination.

4.2 Side-channel attacks

The main reason for the success of side channel attacks is the change of magnetic field during data transmission in the vehicle. Due to many interactions between autonomous vehicles, the signal leaking is more serious. Therefore, it is necessary to build shielding mechanisms to reduce electrical emissions. MWCNT / PP is a kind of composites, which can absorb and reflect

electromagnetic waves. The greater the thickness, the stronger the effect. We can make MWCNT / PP protective case to protect the core ECUs signal from long-distance eavesdropping.

4.3 Environmental attack

Although the method of attacking the ultrasonic sensor is simpler than that of attacking other sensors, because the ultrasonic sensor has a short detection distance and only receive the first encountered object, if the hacker wants to implement signal interference and input during the high-speed running vehicle, their signal jamming equipment needs to be laid near the location of the automatic driving vehicle, such as the trunk of the front car, the surrounding car and so on. Therefore, we can detect whether there is an attack vehicle through passenger observation or multi-sensor, and remind passengers to change driving the mode. Before parking or starting the vehicle, the driver also needs to observe the surrounding environment for suspicious signal emission sources.

For MMW radars sensor attack, improving the anti-noise ability of the sensor is the primary choice to improve the safety of MMW radars sensor. If the high-noise attack signal exists for a long time, the sensor will not accept any reading, which is equivalent to losing a key environmental detection ability. The vehicle shall be equipped with a function detection ECU which is specially used to monitor the operation status of various functions of the vehicle in real time. If there is a problem, this ECU should warn the passengers in time and switch the driving mode at the same time. Secondly, due to the fast propagation speed of electromagnetic wave, the attack signal can only follow the real signal to simulate long-distance obstacles, we can comprehensively judge the road conditions ahead by combining the sensor information with camera to defend MMW radars sensor attack.

The main target of attacking camera is the optical signal receiving module. Since strong light irradiation will permanently damage the optical module, protecting the camera lens is a direct means to prevent such attacks. When the vehicle is parked, it shall be ensured that there is a lens cover or any opaque protective layer to isolate the lens from the outside. When the vehicle is running, the deployment mode of dual camera sensors and light intensity detection device is adopted. During normal operation, the main camera processes images, and the vice camera sleeps with filter lens. When the vehicle detects excessive or abnormal light intensity, turn off the main camera and start the vice camera. The vice camera sacrifices part of the sensor performance in exchange for the ability to resist strong light. At the same time, the vehicle shall remind the owner to switch driving mode or stop.

To sum up, although sensors do not have strong means to resist malicious signals, we still can specialize effective defense means due to the uniqueness of environmental attack, that is, different sensors can only be attacked by corresponding methods. Of course, there are some common restrictions on environmental attacks, which can be used by us for defense. Attack range. The jamming signal sent by hackers must be a certain distance from the vehicle before it can be detected by sensors. Even the long-range radar does not exceed 300m. Therefore, we can set up new road infrastructure to ensure the safety of the environment within a certain

range of autonomous vehicles or provide a special lane for autonomous vehicles to separate autonomous vehicles from general vehicles or buildings. Extra hardware requirement. different jamming devices with different signals need to be purchased and set separately. Therefore, the defense method we can think of is to record the purchase and configuration of various signal transmitting devices to facilitate query and management. High knowledge threshold. It requires a lot of professional knowledge and even sensor experts to transmit specific types of signals for autonomous vehicles. Although we can't carry out specific defense against this weakness, it also provides guidance for the detection after the incident.

4.4 Code attack

Code modification, because the OBD-II scanner can only be used when approaching the vehicle, we only need to focus on the defense of vehicles in parking status, which is the same as the defense of physical attacks. Strengthening parking lot control and combined theft response system are effective defenses. Code injection, since this attack can be implemented by remote access, we need to establish a firewall inside the vehicle system to check the operation and code of any visitor, including the owner, and conduct timely interception and alarm. (The owner is likely to access or carry malicious code in an unknown situation) Packet sniffing, this is different from side channel attacks, although they have the same result that hackers obtain the data transmitted between the vehicle ECUs and various layers. The packet sniffing directly obtains unencrypted data, which is more convenient for attackers to analyze data and attack vehicles. Therefore, for this attack mode, we need to encrypt the transmitted data, but at the same time, we need to ensure the transmission speed of the data, which may require a new design of data transmission mode or encryption method. In addition, in order to prevent replay attacks, we can use time-related encryption or authentication technology to ensure freshness of the communication signals sent and received. Packet fuzzing, such attacks actually take advantage of unknown errors or unpatched vulnerabilities in the vehicle system. Therefore, regular inspection of security vulnerabilities and timely system updates are effective defense methods.

5. Design prospect of autonomous vehicles in the future

From the above, we can conclude that there are still many problems in the security of autonomous vehicles, especially in the interaction between vehicles and the environment. One of the characteristics of autonomous vehicles is to use sensors to replace human beings for road condition recognition and driving judgment. At present, neither sensors nor driving decision algorithms are ready for full production and popularization, but we can still look forward to the design of autonomous vehicles in the future through the current information and analysis.

From a practical point of view, the most important design should be the switching of driving mode. Due to the immaturity of automatic driving, the vehicles should provide driving mode switch to drivers at any time. No matter what kind of environmental attack or code attack, the vehicle may be confused or even out of control. If the vehicle cannot make correct driving

decisions and the driver cannot control the vehicle, the consequences caused are serious and unacceptable. Therefore, in terms of vehicle system logic, we should ensure that the first treatment method of any sensor error, high speed CAN physical layer error, and system abnormality is to unlock the manual driving mode so that the driver can make emergency treatment. At the same time, the driver monitoring module shall also be set in the vehicle to remind the driver to pay attention to the road conditions at any time to ensure rapid response in case of emergency.

Sensor optimization. At present, the sensor technology of automatic driving vehicle lacks the ability to identify and resist malicious signals. However, in fact, the malicious signal is the ultrasonic wave returned in advance, the electromagnetic wave corresponding to the waveform, etc. When the autonomous vehicles are popularized in the future if the adjacent vehicles just transmit the MMW radars signal with the same waveform or the ultrasonic detection signal that arrives successively, it will also cause signal interference or signal deception. Therefore, sensors must be optimized to deal with the environment of a large number of sensor signals and hacker attacks.

Security sharing of data transmission. In the future, with the popularization of autonomous vehicles and the coverage of intelligent transportation systems in cities, the vehicles, various transportation facilities, buildings, and all intelligent devices of pedestrians will interact like vehicles. When the city becomes a data network, each device connected to the network, including autonomous vehicles, not only needs more advanced defense system, but also has the responsibility to maintain the security of the whole network. When the autonomous vehicle detects that it may be infected with virus or has an abnormal system failure, the vehicle shall be able to independently leave the network without transmitting virus or wrong data information to other devices. When the vehicle recovers from error or attack, the vehicle shall be able to send problem information and solutions to the network to form community immunity.

In conclusion, there is a long way to go to improve the safety of automatic driving. Before the popularization of autonomous vehicles, we still have many technologies and concepts to develop and practice, but considering the convenience and efficiency brought by intelligent transportation system to people in the future, all efforts are worth it.

6. References

[1] “AUTONOMOUS VEHICLE COLLISION REPORTS.” *California Department of Motor Vehicles (DMV)*, 2022, https://www.dmv.ca.gov/portal/vehicle-industry-services/autonomous-vehicles/autonomous-vehicle-collision-reports/.

[2] K. Koscher et al., "Experimental Security Analysis of a Modern Automobile," 2010 IEEE Symposium on Security and Privacy, 2010, pp. 447-462, doi: 10.1109/SP.2010.34.

[3] Hoppe, T., Kiltz, S. and Dittmann, J., 2011. Security threats to automotive CAN networks—Practical examples and selected short-term countermeasures. *Reliability Engineering & System Safety*, 96(1), pp.11-25.

[4] Ali Alheeti, K., Gruebler, A. and McDonald-Maier, K., 2016. Intelligent Intrusion Detection of Grey Hole and Rushing Attacks in Self-Driving Vehicular Networks. *Computers*, 5(3), p.16.

[5] Yan, C., Xu, W., & Liu, J. (2016). Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle. *Def Con*, *24*(8), 109.

[6] Nasir, M. K., Islam, A. K., Rahman, M. T., & Sohel, K. (2013). Taxonomy of security in vehicular ad-hoc network.

[7] V. L. L. Thing and J. Wu, "Autonomous Vehicle Security: A Taxonomy of Attacks and Defences," 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2016, pp. 164-170, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.52.

[8] Al-Saleh, M. and Sundararaj, U., 2009. Electromagnetic interference shielding mechanisms of CNT/polymer composites. *Carbon*, 47(7), pp.1738-1746.

[9] Kerns, A., Shepard, D., Bhatti, J. and Humphreys, T., 2014. Unmanned Aircraft Capture and Control Via GPS Spoofing. *Journal of Field Robotics*, 31(4), pp.617-636.

[10] Sumalee, A. and Ho, H., 2018. Smarter and more connected: Future intelligent transportation system. *IATSS Research*, 42(2), pp.67-71.

3.Reflection phase

Through this awesome project, I learned the structure of traditional vehicles and autonomous vehicles, focusing on the electronic control unit, the three-layer core structure system and the sensor system of autonomous vehicles (Section 2). I also learned the principle of several kinds of sensors (Section 3), and investigate the methods of attacking each component of the vehicles (Section 3). I put forward my own defense methods for various attacks, and verify them (Section 4). Then, I learned the basic concepts of intelligent transportation system (Section 5), and provided my opinions on the design of autonomous vehicles in the future (Section 5). In order to complete this project, I consulted many references (section 6), which is quite interesting and challenging. If there was no COVID-19, I would go to some autonomous vehicle's exhibitions for investigation and interview. It would be better if I could do simulated intrusion. In conclusion, in this project, I learned the relevant knowledge of vehicles and sensors, researched attacks, analyzed defenses, which is a very meaningful experience.