Design and Experiment of Simple Dynamometer for Vehicle Cybersecurity Research

Jungho Lee
Hyundai Autoever, Seoul, South Korea
junghlee1987@gmail.com

Abstract

This study describes the design of a simple dynamometer, the creation of an environment for vehicle cybersecurity research, and the results of experiments performed on a real vehicle. Cybersecurity threats in the information technology (IT) environment have spread to vehicles owing to the convergence of vehicles and IT. Accordingly, a variety of research on vehicle cybersecurity has been conducted. Vehicle cybersecurity threats are made to vehicles in motion to trigger casualties. The risk of vehicle cybersecurity threats has been proven in many studies, and protection technology has been also proposed. However, in these studies, the experimental environments were such that the vehicle was simply placed above the ground or on restricted road conditions with no traffic of vehicles. In these experimental environments, unexpected situations can threaten the safety of the experimenter. Furthermore, because the driving environment on actual roads cannot be simulated, the vehicle's functions cannot operate normally. In this study, therefore, we proposed and designed a simple dynamometer to ensure the safety of the experimenter and created the same environment as that of the actual vehicle driving. The designed technology was then applied to a real vehicle to demonstrate the safety and practicality of the designed experimental environment.

Keywords: Vehicle, Cyber Security, Dynamometer

1 Introduction

Vehicles have evolved to improve driving functions. In particular, vehicles have evolved in recent years to improve driver convenience. To this end, a variety of information technology (IT) has been applied to vehicles, and it is now possible to control vehicles from a long distance through communication with external networks. In addition to the connection with external networks, autonomous driving technology has been used to drive vehicles instead of drivers, and currently, vehicles at levels 1 and 2 of autonomous driving are running on actual roads. Thus, the convergence of vehicles and IT has become a trend in new technological developments. Accordingly, vehicles have become new targets of cybersecurity threats in IT. Research on cybersecurity for vehicles began as a result of vulnerabilities in the internal network used to control the vehicle [1, 2, 3, 4, 5, 6, 7, 8, 9]. The main goal of exploiting the cybersecurity vulnerabilities of vehicles is to forcibly control the vehicles as intended by the attackers. To this end, many researchers have conducted studies on real vehicles. Experiments with real vehicles must be conducted in safe environments. Therefore, previous studies were conducted with the vehicle elevated above the ground or on roads where the surrounding traffic of vehicles was completely controlled [4]. Until now, studies have been conducted in such experimental environments; however, in the future, there will be many limitations to obtaining proper data in the same experimental environment as before because autonomous vehicles will be tested in actual driving conditions [10, 11, 12, 13]. In this study, we propose a simple dynamometer to conduct cybersecurity threat experiments for autonomous vehicles in the future. The remainder of this paper is organized as follows. Section 2 reviews related work and Section 3 explains

Research Briefs on Information & Communication Technology Evolution (ReBICTE), Vol. 7, Article No. 20 (December 15, 2021)
DOI:*10.22667/ReBiCTE.2021.12.15.020*

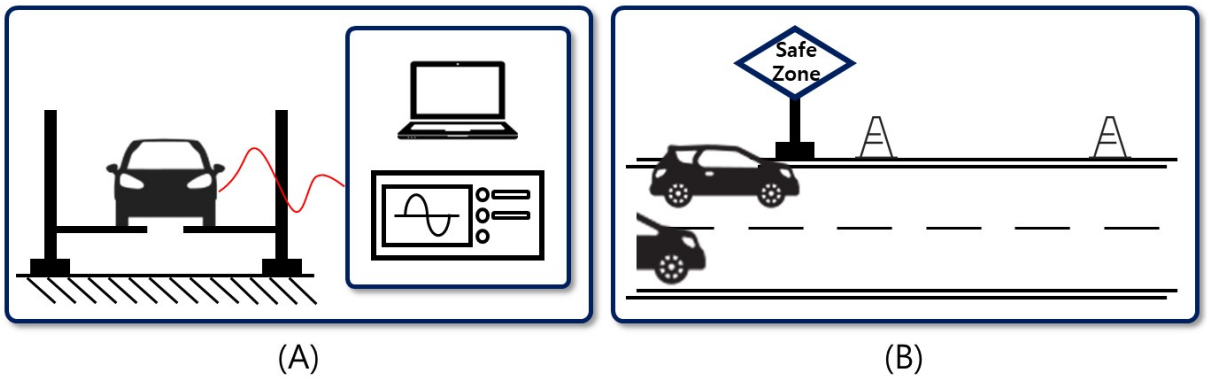

Figure 1: Koscher's Experiment Environment [4]
(A) Vehicle mounted on jack / (B) Vehicles traveling on a closed road

the background knowledge needed to understand this study. In Section 4, a simple dynamometer is designed, and in Section 5, it is installed in a real vehicle to validate the functions of the designed technology experimentally. The conclusion is presented in Section 6.

2 Related Work

In cybersecurity research for vehicles, experiments are conducted with a real vehicle in an environment where the vehicle is moving or stopped. In this section, we describe the experimental environments that have been used up to now for vehicle cybersecurity research.

2.1 In-Vehicle Network Cyber Attack Experiment Environment

Vehicle cybersecurity began with the report of internal network vulnerabilities of vehicles and studies on attacks based on the vulnerabilities. Koscher et al. [4] conducted experiments on the forced control of vehicles based on the known vulnerabilities of the internal network in a vehicle. The research team connected the vehicle's OBD-II port with a laptop computer to forcibly control the vehicle through the laptop. They succeed in forcibly controlling the vehicle in a connected wired environment. The forced-control experiment was conducted in two environments, as shown in Figure 1. In the first environment, the experiment was conducted by mounting the vehicle on the jack with all the wheels removed. In the second environment, the test was conducted while driving the vehicle on a road where the traffic was controlled.

2.2 Connected Car Cyber Attack Experiment Environment

The latest vehicles have begun to provide car services connected to external networks for user convenience. The connected car services allow users to control vehicles from a long distance. Charlie Miller and Chris Valasek succeeded in remotely performing forced control of a vehicle based on the vulnerabilities in the connected car service [19]. The researchers made unauthorized changes to the firmware of telematics that provides the connected car service remotely. The changed firmware contained the rights of the attacker to force control of the vehicle. To represent the experimental results practically, the researchers forcibly controlled certain functions, such as wipers and audio, on public roads. Furthermore, they moved to a safe road and performed driving-related forced controls, such as brakes and steering.

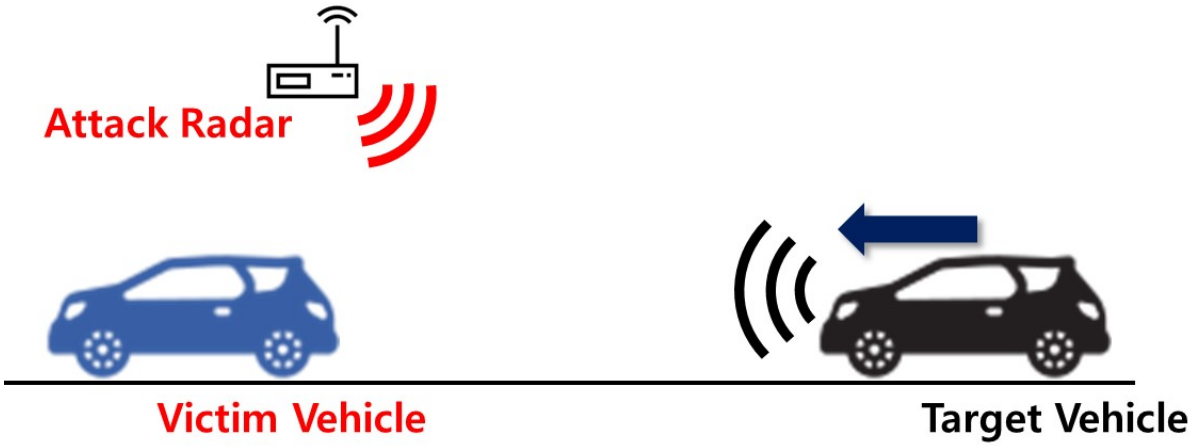

Figure 2: Radar Sensor Attack Experiment Environment [16]

2.3 Experimental Environment for Cyber Attack of Core Sensors of Self-Driving Cars

Technological developments in automobiles are evolving in the direction of improving driver convenience. This evolution is advancing toward self-driving technology. The self-driving function uses the vehicle's surrounding information collected from the radar, LiDAR, cameras, and ultrasonic sensors mounted on the vehicle. If an arbitrary attacker carries out an attack to prevent each sensor from functioning properly in an autonomous vehicle, the self-driving function will not work. Figure 2 shows an example of the environment where an experiment was conducted to attack sensors of an autonomous vehicle [19]. The attack experiment aimed at attacking the radar sensor mounted on the vehicle to prevent related safety functions from working [14, 15, 16, 17, 18]. The attack experiment was conducted on a road where there were no people. The attack tool was installed in the front direction of the vehicle.

3 Background

3.1 Vehicle Safety Function Manual

Car manufacturers have begun to add various functions to vehicles for the safety and convenience of drivers. Because various functions have been added, drivers need to learn how to operate them. To learn how to operate the safety functions, drivers use the manuals provided by car manufacturers. Previously, automakers provided manuals as booklets; however, they are now available on each manufacturer's website. For some manufacturers, vehicle maintenance manuals are also available. Through the publicly available function operation and maintenance manuals, users can check the conditions for operating the safety functions of the vehicle.

3.2 Dynamometer

The driving performance of a vehicle is determined by the speed, fuel economy, and acceleration capability. There are two main methods of measuring the driving functions of a vehicle: real road tests (outdoor) and dynamometer tests (indoor). In real road tests, the operation of driving functions can be tested accurately to measure the vehicle's driving function. However, real road tests lack consistency in test environments because the functions need to be measured in irregular environments of outdoor

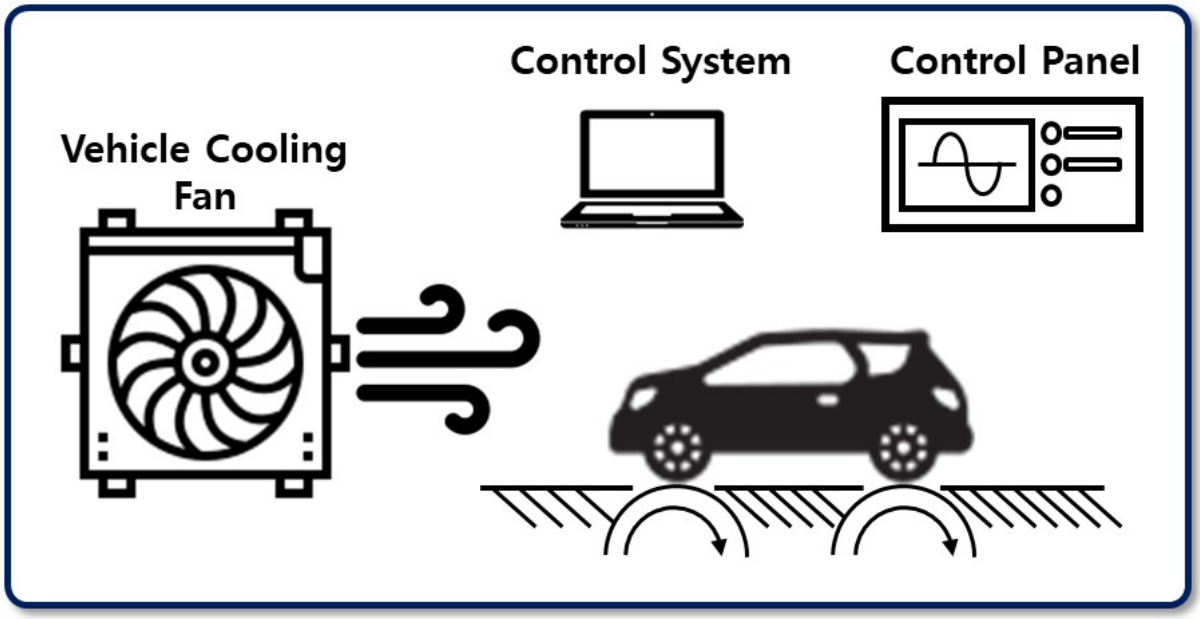

Figure 3: Dynamometer Configuration

conditions, such as wind, temperature, and humidity. Conversely, in the case of dynamometer tests, the test conditions of the tested vehicle can be set the same.

A dynamometer is a machine that measures power by rotating in the opposite direction of the vehicle's engine (wheels). The basic principles of the dynamometer are similar to those of motors or power generators. In the case of the dynamometer, the vehicle's performance is determined by measuring the electric energy generated through the rotational energy.

4 Simple Dynamometer

The vehicle's safety and convenience functions are activated while driving for the driver's benefit. Automakers perform tests in various environments to check whether these functions operate accurately and measure their performance. Among them, the environment for testing under certain conditions is the one that uses a dynamometer. However, dynamometers are very expensive, thus making it difficult for common researchers to set up experimental environments using a dynamometer. Thus, dynamometer testing is limited to car manufacturers, repair shops, and specialized research centers. As a result, the experimenter requires a simple and safe environment in which to conduct experiments. To this end, this section explains the process of designing a simple dynamometer.

4.1 Functional Analysis

Advanced driver assistance systems(ADAS) for the driver's convenience operate when the vehicle runs above a certain speed. Similarly, autonomous emergency braking(AEB) operates when the vehicle's driving speed is greater than equal to 10 km/h. The description of this function is usually provided in the manual for the driver when the vehicle is purchased. It is also available on the car manufacturer's website. A more detailed description is available in the maintenance manual or on the automaker's website for maintenance and repair.

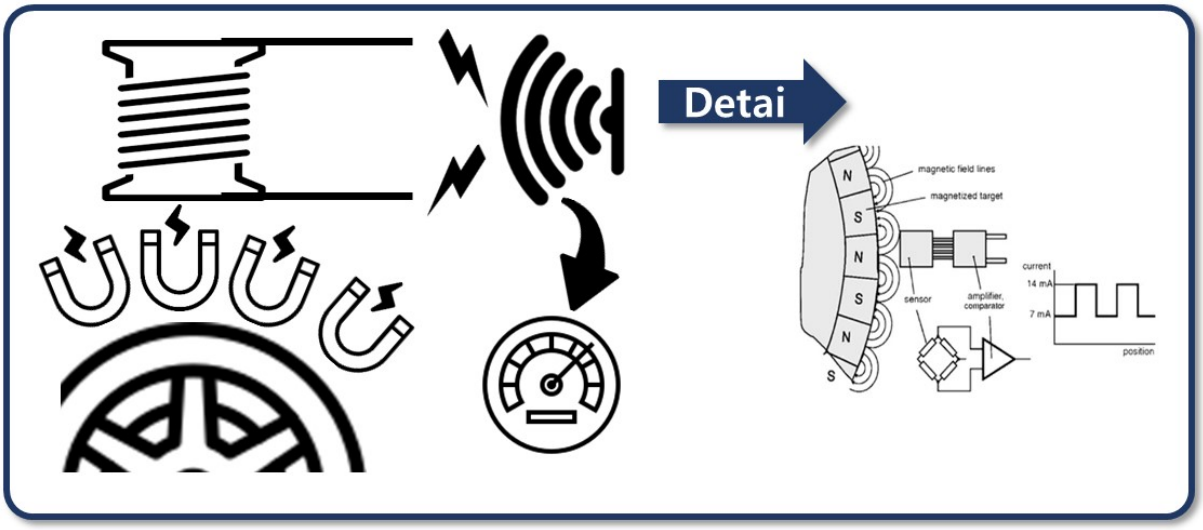

Figure 4: Principle of speed measurement sensor

In previous studies, a vehicle was placed above the ground to check whether the vehicle's functions worked, or some functions were checked on a road with limited traffic. In this section, we propose a simple dynamometer that can operate the vehicle's safety and convenience functions using publicly available information in a stationary vehicle. The following sub-section describes the method of measuring speed, a condition required to operate the vehicle's safety and convenience functions.

4.2 Operating Condition Analysis

The vehicle's safety functions operate while driving. This means that the vehicle's safety functions operate at a certain speed or higher. If the vehicle's speed can be controlled arbitrarily in a situation where the vehicle is stopped, the vehicle's safety functions will operate. The method of measuring the vehicle's speed is detailed in the vehicle's maintenance manual. The vehicle's speed is measured using a sensor mounted on the vehicle's wheel. Figure 4 illustrates the working principle of the speed measurement sensor mounted on the wheel. The N- and S-poles of magnets are attached repeatedly to the wheel. As the vehicle moves, the wheel rotates, thus generating alternating current (AC) voltage frequencies at the sensor owing to the repetition of the N-poles and S-poles attached to the wheel. The size of the generated AC voltage frequency amplitude increases as the wheel's rotational speed increases. The size of the amplitude of the frequencies measured by the sensor determines the value of the speed.

4.3 Simple Dynamometer Design

As explained in the previous sub-section, the vehicle's speed is measured by the sensor mounted on the vehicle's wheel. If the speed measured by the sensor can be changed arbitrarily, the changed value will be recognized as the vehicle's speed. Furthermore, if it is changed to a speed at which the vehicle's safety functions can operate, the functions will operate normally.

The vehicle speed changer can easily adjust the speed measurement value if the sensor's working principle is used. The speed is determined by the size of the frequency amplitude measured by the speed measurement sensor. If the size of the frequency amplitude occurring at a high speed can be established, the sensor will perceive the speed as high.

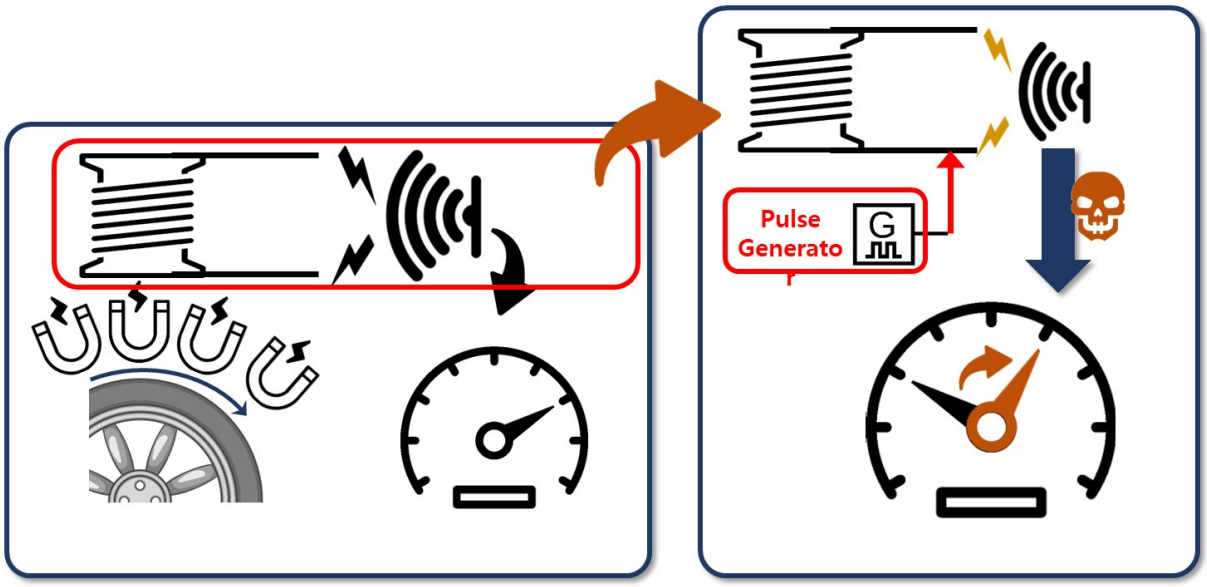

Figure 5: Vehicle Speed changer configuration

It is necessary to determine whether the vehicle's speed is altered by the speed-changing device. First, the device that changes the speed measurement sensor's value was installed on the vehicle's front wheel, and the experiment was conducted. However, when it was installed on only the front wheel, the vehicle's speed did not change. Therefore, we installed the speed changer on every wheel of the vehicle. It was found that the vehicle's speed could be changed arbitrarily by changing the speed on every wheel identically at the same time. However, the brake sensor failed frequently when the speed changers were used repeatedly. The failure of the brake sensor was caused by the overload due to the brake's malfunction. The vehicle with a speed changer installed had a constant speed. In this state, if the vehicle's safety function related to the brake is activated, the brake will operate continuously. However, if the brake operates continuously without reducing the changed speed, the sensor will become overloaded. Therefore, the conditions for configuring the simple dynamometer proposed in this study are as follows:

- The sensor values on all wheels of the vehicle must be changed identically.
- It must be possible to generate a certain frequency that the speed measurement sensor measures.
- The packet information for acceleration, braking, and RPM must be known.

Based on the above conditions, the operation logic of the simple dynamometer can be designed, as shown in Figure 6 (A) below. The installation environment is set up, as shown in (B).

5 Evaluation

This section evaluates whether the simple dynamometer designed in Section 4 operates normally. If it operates normally, it can activate the high-speed safety and convenience functions speeds even if the vehicle has stopped or is moving at a low speed. Figure 7 indicates that the speed can be controlled after installing a simple dynamometer on a real vehicle. At the same time, it confirms that the safety function operating at a certain speed or higher is activated. In other words, the safety functions that operate at high speeds can be activated by increasing the vehicle's speed while it is stopped.

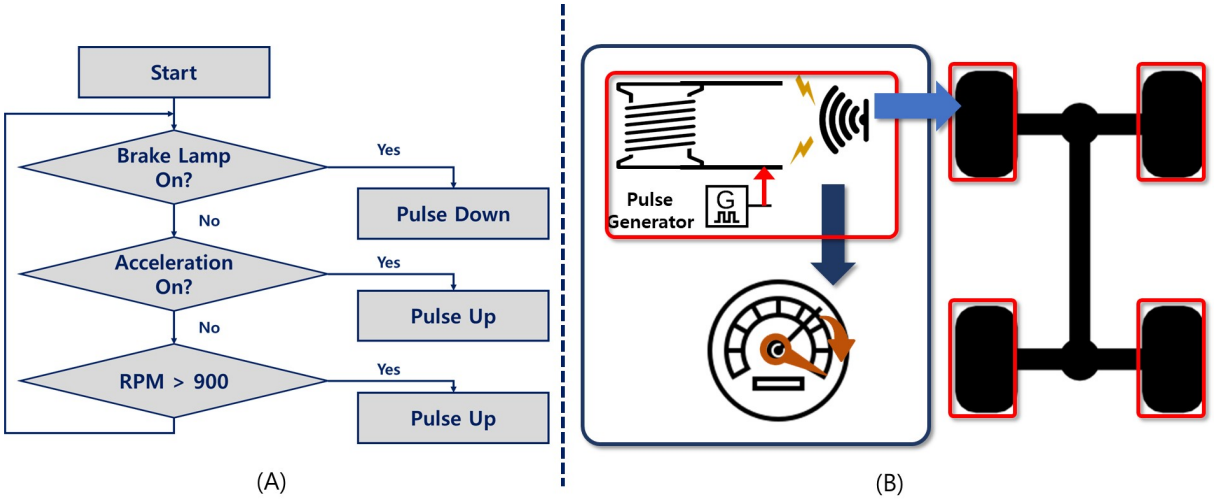

Figure 6: Simple Dynamometer Design

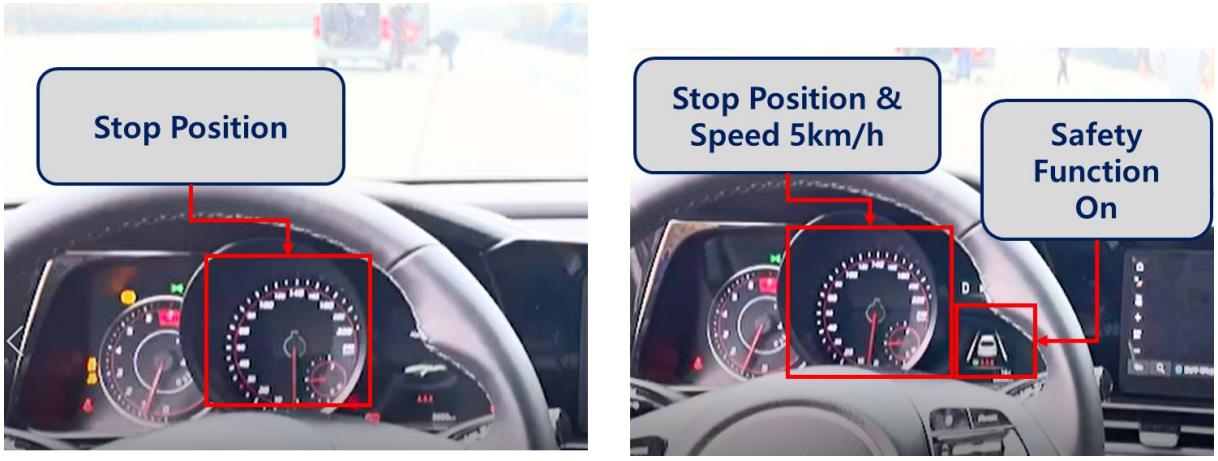

Figure 7: Simple Dynamometer Evaluation

6 Conclusion

In this study, we designed a simple dynamometer and created a test environment for future research on cybersecurity threats of autonomous vehicles. It was then used to conduct experiments on a real vehicle. The simple dynamometer proposed in this study is safer than the conventional experimental environments used for vehicle cybersecurity threat research. Experiments on the safety and convenience functions of a vehicle can be conducted in the same manner that they are normally operated by the vehicle. When conducting experiments on vehicle cybersecurity in future studies, the proposed simple dynamometer will offer the advantage of being safe while also facilitating experiments with all functions of the vehicle turned on.

References

[1] M. Wolf, A. Weimerskirch, and C. Paar. Security in automotive bus systems, February 2022. `http://www.weimerskirch.org/files/WolfEtAl_SecureBus.pdf`, [Online; Accessed on December 1, 2021].

[2] T. Hoppe and J. Dittman. Sniffing/replay attacks on can buses: A simulated attack on the electric window lift classified using an adapted cert taxonomy. In *Proc. of the 2nd Workshop on Embedded Systems Security (WESS'07), Salzburg, Austria*, pages 66–72, October 2007.

[3] T. Hoppe, S. Kiltz, and J. Dittmann. Security threats to automotive can networks – practical examples and selected short-term countermeasures. *Reliability Engineering & System Safety*, 96:11–25, 2008.

[4] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. Mccoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage. Experimental security analysis of a modern automobile. In *Proc. of the 2010 IEEE Symposium on Security and Privacy (S&P'10), Oakland, CA, USA*, pages 447–462. IEEE, May 2010.

[5] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar. Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study. In *Proc. of the 19th Usenix Security Symposium, Washington DC, USA*, pages 323–338. Usenix, August 2010.

[6] S. Checkoway, D. Mccoy, D. Anderson, B. Kantor, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno. Comprehensive experimental analyses of automotive attack surfaces. In *Proc. of the 20th Usenix Security Symposium, San Francisco, CA, USA*. Usenix, August 2011.

[7] S. Woo, H. Jo, and D. Lee. A practical wireless attack on the connected car and security protocol for in-vehicle can. *IEEE Transactions on Intelligent Transportation Systems*, 16(2):993–1006, April 2014.

[8] J. Lee, S. Woo, S. Lee, and D. Lee. A practical attack on in-vehicle network using repacked android applications. *Journal of the Korea Institute of Information Security and Cryptology*, 26(3):679–691, June 2016.

[9] Y. Lee, S. Woo, J. Lee, Y. Song, H. Moon, and D. Lee. Enhanced android app-repackaging attack on in-vehicle network. *Wireless Communications and Mobile Computing*, 2019:5650245:1–5650245:13, February 2019.

[10] B. Nassi, D. Nassi, R. Ben-Netanel, Y. Mirsky, O. Drokin, and Y. Elovici. Phantom of the adas: Phantom attacks on driver-assistance systems. In *Proc. of the ACM SIGSAC Conference on Computer and Communications Security (ACM CCS'20), Virtual Event, USA*, page 293–308. ACM, November 2020.

[11] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl. Remote attacks on automated vehicles sensors: Experiments on camera and lidar, 11/2015 2015. `https://www.blackhat.com/docs/eu-15/materials/eu-15-Petit-Self-Driving-And-Connected-Cars-Fooling-Sensors-And-Tracking-Drivers-wp1.pdf` [Online; Accessed on December 1, 2021].

[12] W. Xu, C. Yan, W. Jia, X. Ji, and J. Liu. Analyzing and enhancing the security of ultrasonic sensors for autonomous vehicles. *IEEE Internet of Things Journal*, 5(6):5015–5029, December 2018.

[13] G. Brooker. Mutual interference of millimeter-wave radar systems. *IEEE Transactions on Electromagnetic Compatibility*, 49(1):170–181, February 2007.

[14] N. Miura, T. Machida, K. Matsuda, M. Nagata, S. Nashimoto, and D. Suzuki. A low-cost replica-based distance-spoofing attack on mmwave fmcw radar. In *Proc. of the 3rd ACM Workshop on Attacks and Solutions in Hardware Security Workshop (ASHES'19), London, UK*, pages 95–100. ACM, November 2019.

[15] R. Komissarov and A. Wool. Spoofing attacks against vehicular fmcw radar. In *Proc. of the 5th ACM Workshop on Attacks and Solutions in Hardware Security Workshop (ASHES'21), Virtual Event, Republic of Korea*, pages 91–97. ACM, November 2021.

[16] F. Jin and S. Cao. Automotive radar interference mitigation using adaptive noise canceller. *IEEE Transactions on Vehicular Technology*, 68(4):3747–3754, April 2019.

[17] Y. Cao, C. Xiao, B. Cyr, Y. Zhou, W. Park, S. Rampazzi, Q. A. Chen, K. Fu, and Z. Mao. Adversarial sensor attack on lidar-based perception in autonomous driving. In *Proc. of the 2019 ACM SIGSAC Conference on Computer and Communications Security (ACM CCS'19), London, UK*, pages 2267–2281. ACM, November 2019.

[18] H. Shin, D. Kim, Y. Kwon, and Y. Kim. Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications. In *Proc. of the 2017 International Conference on Cryptographic Hardware and Embedded Systems (CHES'17), Taipei, Taiwan*, volume 10529 of *Lecture Notes in Computer Science*, pages 445–467. Springer, Cham, 08 2017.

[19] C. Miller and C. Valasek. Remote exploitation of an unaltered passenger vehicle. IOActive Technical White Paper, 2015. `https://privacy-pc.com/articles/remote-exploitation-of-an-unaltered-passenger-vehicle.html` [Online; Accessed on De-

cember 1, 2022].

Author Biography

Jungho Lee received the master's degree in information security from Korea University,Seoul, South Korea, in 2019. He was a Researcher with the Korea Information Certificate Authority Inc., (KICA), in 2016. He is currently an Reserecher with the Hyundai Autoever, Seoul, South Korea. His research interests include V2X security, public key infrastructure (PKI), and vehicular security.