Autonomous Vehicle Ultrasonic Sensor Vulnerability and Impact Assessment

Bing Shun Lim
School of Computing Science
University of Glasgow
limbingshun@gmail.com

Sye Loong Keoh
School of Computing Science
University of Glasgow
SyeLoong.Keoh@glasgow.ac.uk

Vrizlynn L. L. Thing
Cyber Security Cluster
Institute for Infocomm Research, A*STAR
vriz@i2r.a-star.edu.sg

***Abstract*—Vehicles today are relying more on technologies to bring about fully autonomous features. The conventional wirings within are being simplified into a network of electronic components, and this network is controlled via advanced sensing of the environment to make decisions in real-time. However, with the heavy reliance on the sensor readings, any inaccurate reading from the sensors could result in decisions that may cause life-threatening incidents. As such, this research focuses on the in-depth assessment of potential vulnerabilities of an important and commonly used obstacle sensing device, which is the ultrasonic sensor, in modern as well as autonomous vehicles. This research will help bring awareness to the car manufacturers and AV researchers so as to mitigate such issues.**

I. Introduction

Motor vehicles became popular in the 20th centuries as the main mode of transport of people and goods. As technologies become more advanced, the motor vehicles evolved into a system which incorporates electronics to bring about modern entertainment, navigation, perception, and localization features. Thus, modern vehicles are not simply about motors and wheels anymore; they are equipped with a network system that connects the electronic components together, which allows these vehicles to have sensing capabilities (i.e. being able to detect obstacles and to warn drivers who are driving these vehicles [18]). However, these modern vehicles that are integrated with the network system have its own drawback - telematics and sensors equipped to the vehicle might be compromised by adversaries and the vehicle can be immobilised or be "instructed" to act in a disorderly manner, causing inconvenience or even danger to the road users [20] [15] [16].

An autonomous vehicle [21] is a self-driving vehicle that has the capability to reach its destination without any human intervention. The vehicle uses advanced sensors to detect and identify objects so as to make informed decisions to support automated navigations. The potential benefits of autonomous vehicles include the reduction of traffic collision and fuel consumption, and also the enhancement of the mobility of elderly, children, as well as the disabled. It can potentially help people save time on the road and have more time to do things while on their journey to the destination [19]. To do so in a safe manner, it is necessary to ensure that the autonomous vehicle operate in a safe and secure manner. It implies that, at a minimal, the availability and integrity of the sensor signals should be verified to be in place. However, with the major role that these sensors play in the automotive industry, it is very likely that they become the most common target of attacks for the adversaries.

Attacks on the sensor can be through a remote compromise or a physical attack to generate incorrect signals into the vehicle systems. In this paper, we aim to unveil the possibilities of a sensor being compromised, through different experiments to perform an in-depth safety and security assessment of the ultrasonic sensor.

This paper is organised as follows: Section II presents the background and the related work for this research, while in Section III, we present the threat model and experimental design. We discuss the test cases and evaluation results in Section IV. Finally, the research conclusion and the future work are discussed in Section V.

II. Background

Cyber-physical features [16] are semi-autonomous features that exist in modern vehicles as well as in autonomous vehicles [2] to assist the driver while parking or driving on the road to prevent accidents from happening. The vehicles rely on these sensors data and the data are being computed through the Electronic Control Unit (ECU) to determine each action to be taken subsequently. Park Assist is one of these features that are commonly used in a modern vehicle.

A. Park Assist

Park Assist [16] [8] is a feature that helps the driver park in tight spots. The system uses mainly the ultrasonic sensor to detect the obstacle and calculates the optimum steering angle during parking. The sensor then integrates its readings with the back-up camera to provide the parking information to the driver. This feature is only available when the vehicle is moving very slowly, and in practice, there are typically safety mechanisms that try to prevent the wheel from turning due to this feature when the vehicle is at anything but slow speed. Tesla has also integrated such a feature in its vehicle, which is known as the Summon self-parking feature [10].

With the implementation of such a "Park Assist" feature in vehicles as one of their primary cyber-physical features, vehicle manufacturers have also provided users with a user manual, in which it warns users to take note that the sensor may not function properly under certain conditions [6].

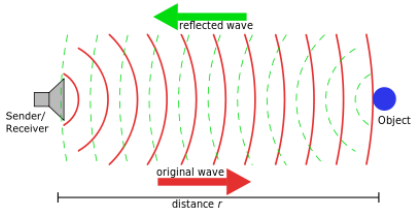

Fig. 1. Echolocation used by ultrasonic sensor

Ultrasonic sensor (also known as sonar) is a sensor that uses echolocation (see Figure 1) [3] to determine if an object is in the range of the sensor. The sensor is also capable of determining the object distance by using the time taken by the signal to come back to the ultrasonic sensor after emitting it. However, the limitation of ultrasonic sensors is its blind zone at close proximity and the noise interference, which might cause the readings to be inaccurate [12]. Readings of ultrasonic sensors can also be compromised by materials like acoustic foam as such materials have sonic wave dampening ability [5].

B. Related Work

There have been several studies in the security of the automotive system and they mainly focused on the network system of the vehicle - CAN Bus. CAN Bus is a standard designed to allow Electronic Control Unit (ECU) and devices to communicate with one another in applications without a host computer [18]. Each of these ECUs has its own responsibility to read signals coming from the sensor placed at different parts of the vehicle. The CAN bus allows the ECU to send these readings to other ECUs in the network. The ECU will act accordingly if the readings are relevant to its operations. As a substitution of the conventional multi-wire looms, the CAN Bus allows these ECUs to communicate on a single or dual-wire network data bus supporting up to 1Mbps [18].

In [15], the authors have demonstrated attacks like unauthorised actuation, Denial of Service (DOS), faking a system state and eavesdropping internal information of the vehicle and these attacks violated the security model of the information being exchanged - CIA traits. These attacks can result in catastrophic effect, such as potential road accidents, monetary loss, and even loss of human lives. These attacks can be carried out simply by injecting malicious code to the ECUs, given physical access to the vehicles.

In [16] [17], the authors have researched on the CAN transport protocol. The paper mentioned that even though some of the vehicle manufacturers deviate from the standards, the means of invoking an attack are very much similar. There are also services that an adversary can tap on to compromise the ECU, the CAN-Bus physically as well as through its telematics features. Denial of service is also demonstrated by using the compromised ECU to flood the network with packets.

In [14], the researchers focused on the physical aspects of autonomous vehicle attacks. The idea of their research is that the hacker may not need to access the CAN-Bus remotely to manipulate a vehicle as the adversary would be able to attack a vehicle through the use of jammers. A jammer can manipulate readings from various sensors such as the ultrasonic sensors and radar sensors. However, conducting such an attack would be costly as it requires a high-end sophisticated frequency jammer. In [4], another group of researchers demonstrated an attack to negatively affect the ultrasonic sensors' sensing capability through the use of acoustic foam, to show that acoustic materials have sonic wave dampening effect on the sensors.

III. Experimental Attacks on Ultrasonic Sensors

It is now evident that many (autonomous) vehicles in the market are using ultrasonic sensors as the basis to detect obstacles to assist in driving and parking. This section outlines some experimental attacks that can be launched on ultrasonic sensors in a laboratory environment, which could cause a serious impact on the road. Specifically, this paper investigates the impact on the ultrasonic sensor in the following scenarios:

- Blind-spot range is affected by the area of exposed surface of the obstacle.
- Covering of either or both ultrasonic transmitter and receiver affects the detection accuracy.
- Obstacle made of certain material will cause the reading of ultrasonic sensor to be inaccurate.
- A secondary ultrasonic sensor or any sound waves device will interfere with the primary ultrasonic sensor, and thus affecting the reading of the sensor.

The experiment set-up and test-cases to validate these hypothesis are explained in the following sections.

A. Adversary Model

Knowledge of vehicles – The CAN-bus architecture and its communication model is public knowledge. This allows the adversary to study about CAN-Bus as well as the sensors used by the (autonomous) vehicles. In addition, by consulting the various experts in the automotive industry, the adversary gets a better understanding of the functionalities and capabilities of the vehicle sensors. Thus, enabling the adversary to learn the capability of creating devices that can be used to alter the sensor signal, or to interfere with the sensor readings.

Access to vehicles – The adversary is assumed to have no access to the vehicle other than the vehicle's exterior. Hence, tapping on the CAN-bus communication is not possible, and injection spurious messages into the vehicle's internal communication system is not feasible. However, the adversary have full access to the ultrasonic sensors visible on the vehicle's exterior, and potential tampering of the sensor is possible by exploiting the flaws of the exposed sensors.

Limitations – It is further assumed that the adversary can only launch attacks on the ultrasonic sensors without being seen by a human user, i.e., the driver or owner of the attacked vehicle. Any sign of tampering on the ultrasonic sensors cannot be detected by the bare eyes. We further assume that the

Fig. 2. HC-SR04

vehicle's internal system is protected by security mechanisms (e.g. data encryption and device authentication).

B. Sensor Platform and Experiment Setup

The experiments to validate the hypothesis were conducted in a laboratory environment. Figure 2 shows a commercially available off-the-shelf ultrasonic sensor, HC-SR04 used in our experiments to simulate the obstacle detection mechanism in vehicles [13]. The ultrasonic sensor was connected to an Arduino Uno R3 as illustrated in Figure 3. Arduino was chosen as a microprocessor for its portability, cost and simplicity to interface with the sensors [1]. Vehicles use beeping sound to indicate that there's an obstacle detected in real life. In our experiments, three LED were used as a replacement of the beeping sensor.

Fig. 3. Arduino Uno R3

Figure 4 shows the experimental platform interconnecting the ultrasonic sensor with the Arduino Uno R3 and three LED lights. In this set-up, the Arduino Uno draws its power through a USB connection and then supplies the power to the circuit by connecting 5V and GND to the positive and negative side of the breadboard respectively. The HC-SR04 ultrasonic sensor is powered by connecting the VCC pin and the GND pin to the positive and negative side of the breadboard. Digital pin 11 was set as OUTPUT mode, while digital pin 12 was set as INPUT mode where they were connected to the trigger pins and echo pins on the HC-SR04 sensor respectively. Digital pins 8, 9, 10 were set as OUTPUT mode as they were attached to the positive side of the LED to light the relevant LED depending on the distance detected from the ultrasonic sensor. The negative side of the LED was then connected to the negative side of the breadboard to form a complete circuit.

The sensor platform exhibits the following behaviour: All LEDs are lit when it first starts up. After the LED is lit for 2 seconds, it will start lighting up the relevant LED based on the obstacle's distance away from the ultrasonic sensor. If the distance is more than 30 cm, the green LED (the left most LED as shown in Figure 4) will be lit up. For a detected distance between 15 cm to 30 cm, the yellow LED, i.e., the middle

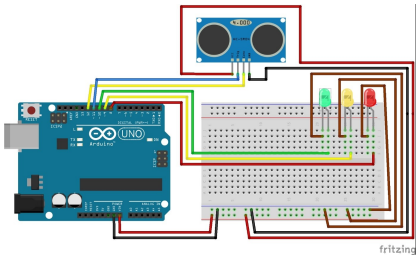

Fig. 4. Design of the experimental platform

LED, will be lit up. Lastly, if the distance falls below 15 cm, which means that the obstacle is very near to the sensor, the red LED will be lit up, the right-most LED.

The ultrasonic sensor produces an *output* value (in microsecond), which is used to derive the distance of the obstacle from the sensor. The *output* is a measure of the round trip time between the sensor emitting a pulse, and receiving the pulse in return when there is an obstacle. The *output* is divided by two because it is the time taken for the pulse to be sent out from the sensor and returned back to the sensor. Since the speed of sound is 340 m/s, i.e., 29 microseconds per cm, the distance can be calculated using the following equation [9].

$$distance = (output/2)/29 \quad (1)$$

C. Simulation of Attacks on Ultrasonic Sensors

Modern vehicles are mostly equipped with their proprietary "Park Assist", which relies on the ultrasonic sensors to determine and to avoid obstacles that are in the vehicle's way. Furthermore, drivers using these features are required to leave their key in the ignition. As such, some test cases may not be applicable to the modern vehicles as the drivers would have some form of control over the vehicle. However, accident may still happen if the drivers are not cautious about their surroundings or if the drivers fully rely on the sensor's feedback.

Tesla on the other hand, has its car equipped with a semi-autonomous function – *Summon* [10], which provides the user with the capability to perform auto-pilot on the car and to enable auto-parking. This auto-park capability allows *Summon* to park the vehicle while the driver is away from the vehicle. *Summon* can be activated with a mobile application [7], which is the fulcrum of the test case as the test case seeks to investigate the vulnerability of these autonomous features such as its limitations and the triggering of false warnings. Upon analysing the Tesla Model S owner's manual [6] and other vehicle manufacturer's user manuals [11], we designed four test cases to simulate attacks on ultrasonic sensors, to demonstrate the effect of tampering of the sensor on a semi-autonomous vehicles.

1) Test Case 1: Thin Object as an Obstacle: The objective of this test case is to determine if the object's area of exposure affects the distance detection limit of the ultrasonic sensor. This experiment was conducted to proxy a scenario, whereby

the vehicle can park itself inside a parking lot which has a thin obstacle in its way.

Typically, a vehicle is equipped with four sensors at its rear and it is believed that there could possibly be a blind spot in which a thin obstacle could not be detected by the ultrasonic sensors. It is hypothesised that the relatively widely spaced sensors may not be able to detect a thin obstacle when the vehicle reverses into the sensor's blind range. In this experiment, a straw, chopstick, hairpin and a card were used as a thin obstacle to simulate such an attack.

Although the sensor used in the experiment is different from any modern vehicle, the vehicle's and the experiment's sensor use the same underlying mechanism to detect an obstacle. Therefore, in this test case, the blind range of the thin obstacle can be determined.

2) Test Case 2: Covering of the Transmitter and Receiver: This test case aims to determine the accuracy of the ultrasonic sensor's readings when either or both of the transmitter and receiver are blocked. This experiment was conducted to demonstrate a scenario in which the sensors are being covered by an object, and to show that such an attack has an adverse effect on the accuracy in obstacle detection. The sensor used in the experiment should work the same way as the sensor used by any vehicle in the market, thus allowing us to draw a conclusion from this experiment. Scotch tape was used to cover both the transmitter and receiver of the ultrasonic sensors in this experiment.

Many vehicle manufacturers have warned that users should not install any accessories or stickers on or near the parking sensor. The postulation is that the installation of stickers or accessories on or near the parking sensor might cause a false reading recorded by the sensor. In situations where the autonomous feature is used to park the car, if the parking sensor (i.e., ultrasonic sensor) has been compromised or tampered with physically, the vehicle might not be able to detect any obstacle, and thus may cause a collision to occur.

3) Test Case 3: Using Acoustic Foam: The objective of this test case is to demonstrate that using materials such as acoustic foam can mask the presence of an object to the ultrasonic sensor. This experiment was conducted to proxy a scenario whereby the acoustic foam is attached to the adversary's vehicle, thus causing the inability of the parking sensor to detect the adversary's vehicle.

Acoustic foam is an open cell foam which can absorb sound waves of medium to high range in the frequency spectrum [5]. The sound absorbed by the foam will then be dissipated, thus resulting in the inability of ultrasonic sensors to detect any obstacle. In this experiment, acoustic foam was used as a medium between an object and the ultrasonic sensor.

It is envisaged that when the vehicle is performing auto-parking without its driver's supervision, the detection of obstacles must be accurate. If there exists an adversary's vechicle in the vicinity and it is covered with an acoustic foam, this could potentially cause the vehicle to collide with the adversary's vehicle. Such an attack can be exploited, allowing the adversary to file for a claim from the insurance company or to cause monetary loss to the victim if the situation is not assessed carefully.

4) Test Case 4: Creating Interference using Additional Ultrasonic Sensors: The objective of the test case is to prove that interference can cause inaccurate readings. When two ultrasonic sensors are placed opposite to each other, it will cause interference.

This experiment was conducted to demonstrate a scenario in which the rear of both vehicles are facing each other while performing feature like auto-parking. In this case, it may cause both vehicles to behave abnormally due to the inaccurate sensor readings caused by the interference as there is no human intervention. Such an attack can be simulated by placing two ultrasonic sensors facing each other, thus causing the ultrasonic sensors to receive echo of itself and the echo of the other sensor. As a result, the readings of the ultrasonic sensor will be inconsistent, degrading the accuracy of the sensor.

A possible attack scenario would be while the user is performing auto-parking in between two stationary vehicles, if one of the stationary vehicles has an ultrasonic sensor installed at the same level to the parking sensor of a car in order to cause interference to the vehicle trying to perform auto-parking; it could possibly cause the parking vehicle to collide with the stationary vehicles due to the interference with the parking sensors, thus resulting in potential vehicle damage.

IV. Evaluation and Results

A. Test Case 1: Thin Object as an Obstacle

This experiment was conducted to determine the blind range of the ultrasonic sensor, in particular to determine the ability of the sensors to detect thin objects as obtacles. Four test subjects, namely a straw, a chopstick, a hairpin, and a card were used in this experiment.

Figure 5 shows the experimental setup in this test case. The ultrasonic sensor was calibrated with the ruler, indicating distance of the test subjects from the sensor. The shaded area shows a path located in between the ultrasonic sensors, as this is to allow the test subjects to traverse through the shaded path away from the ultrasonic sensors during the experiment. The set-up was kept at a distance range of up to 30 cm as the test subjects were small and it was difficult to traverse within the shaded path for a distance longer than 30 cm. The yellow box at the other end marks the end point of the test.

TABLE I
Blind-spot Range for Thin Objects

Test Subjects	Blind-Spot Range
Straw	0 - 1 cm
Chopsticks	0 - 1 cm
Hairpin	0 - 10 cm
Card	0 - 20 cm

Table I shows the results of the experiment, indicating the thinnest test object has the highest blind-spot range. This means that if an ultra thin object is placed in between two

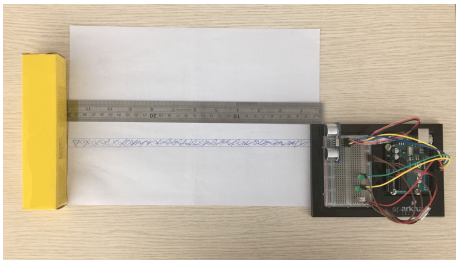

Fig. 5. Physical set-up for Test Case 1, 2, 3

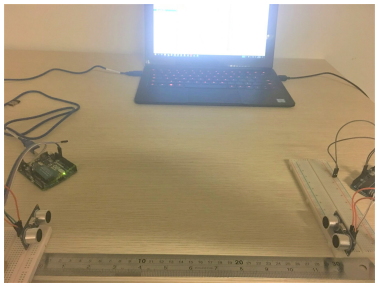

Fig. 6. Ultrasonic set-up for Test Case 4

ultrasonic sensors, this object has a higher probability that it will not be detected. In our experiment, the card is the thinnest object and the result shows that the card could not be detected by the ultrasonic sensors when it was placed between 0-20 cm away from the sensors.

There is a possibility that the ultrasonic sensor built in a vehicle has a higher blind-spot range. Thus, it may require more ultrasonic sensors to be placed on different parts of the vehicle to detect obstacles at various angles. Alternatively, the vehicle manufacturer can include multiple sensors to work together in order to detect obstacles more accurately.

B. Test Case 2: Covering of the Transmitter and Receiver

Test case 2 was conducted using a similar set-up as shown in Figure 5. The experiment tested the accuracy of the ultrasonic sensors in three different conditions: (1) Both the transmitter and the receiver were blocked or covered. (2) Only the transmitter was blocked, and (3) Only the receiver was blocked.

A credit-card sized cardboard was used as the obstacle, traversing through the shaded path away from the ultrasonic sensors until it reached the end point. Table II shows the results of the readings by an ultrasonic sensor at various distances away from the ultrasonic for different sensor conditions. We conclude that for all three conditions experimented, the ultrasonic sensors were unable to detect the obstacle, and returned *out of range* readings.

TABLE II
ULTRASONIC SENSOR READINGS WHEN SENSORS ARE BLOCKED

Sensor Conditions	10 cm away	20 cm away	30 cm away
Both transmitter and receiver blocked	*out of range*	*out of range*	*out of range*
Transmitter blocked	*out of range*	*out of range*	*out of range*
Receiver blocked	*out of range*	*out of range*	*out of range*

Therefore, it is important that the ultrasonic sensors are examined regularly to ensure that they are not covered or blocked in any ways, so that accidents and collusions can be avoided.

C. Test Case 3: Using Acoustic Foam

Test case 3 was also conducted using a similar set-up as Figure 5 It was thought that acoustic foam can not be easily detected by the ultrasonic sensors due to its sound-wave absorbing characteristic. In this experiment, we investigated the accuracy of detecting an object made of acoustic foam using the ultrasonic sensors. Three scenarios were tested, namely: (1) Using acoustic foam singularly, (2) A plastic bottle wrapped with acoustic foam, and (3) A softdrink can wrapped with acoustic foam.

The experiment was conducted by moving the test material along the shaded path. If the test material was detected, its distance from the ultrasonic sensors was recorded. In this experiment, the boundary of the experiment setup was extended to 35 cm for the test material to be in place.

TABLE III
SENSOR READINGS FOR DETECTING OBJECTS WRAPPED WITH FOAM

Test Materials	10 cm Away from Sensor	20 cm Away from Sensor	30 cm Away from Sensor
Acoustic foam	37 cm	37 cm	37 cm
Bottle wrapped with Foam	69 cm - *out of range*	91 cm - *out of range*	*out of range*
Drink Can wrapped with Foam	70 cm - *out of range*	*out of range*	*out of range*

Table III shows the results of the readings recorded by the ultrasonic sensors. The results clearly show the inaccuracy in the detection of obstacle, in which when the drink can was wrapped with an acoustic foam, even though it was placed 30 cm from the sensor, the sensor returned *out of range* reading, indicating that the obstacle could not be detected. We conclude that acoustic foam can effectively be used to mask the obstacle presence from the sensor, thus giving an inaccurate reading.

This attack is cost effective and it targets users who are not aware of their surroundings. This attack can be dreadful since the obstacle can mask its presence, thus resulting in the inability of the sensor to detect obstacles accurately.

D. Test Case 4: Interference with Additional Sensors

Figure 6 shows the experimental setup for this test case, by using two ultrasonic sensors facing one another to create interference. The distance recorded by each ultrasonic sensor was then recorded to determine whether any interference had occurred.

Table IV shows the results indicating the sensor readings of the ultrasonic sensor. The obstacle detection distance seems to be always shorter than the actual distance between the two sensors. For example, when the sensors are 30 cm apart from each other, Sensor 1 detected that there was an obstacle 14-

17 cm away, and similar readings were recorded by Sensor 2. We thus conclude that both ultrasonic sensor readings are inaccurate when facing each other, as the sound waves from external source would significantly affect the accuracy of the ultrasonic sensor.

TABLE IV
RESULTS SHOWING INTERFERENCE FROM ADDITIONAL SENSOR

Actual Distance	Sensor 1 Readings	Sensor 2 Readings
10 cm	5 - 7 cm	3 - 4 cm
20 cm	3 - 20 cm	0 - 17 cm
30 cm	4 - 29 cm 14 -17 cm (intermittent)	1 - 26 cm 12 - 16 cm (intermittent)

As the autonomous vehicle would be deployed in the near future, if any of its features rely heavily on ultrasonic sensor readings, it may cause serious issues (e.g. traffic congestion) as the sensor may falsely detect obstacles due to the interference from other ultrasonic sensors in the vicinity.

E. Countermeasures and Mitigation Strategy

The test cases results have shown that the ultrasonic sensor can be easily compromised by off-the-shelf materials and this causes devastating effects on the road. In this section, we propose countermeasures to mitigate and reduce the risks to guarantee the safety of the vehicles and its passengers.

Multi-sensor fusion consisting of multiple ultrasonic sensors should be adopted to allow for multiple sensor data to be validated and cross-checked to mitigate the discrepancy resulting from Test Case 1, 3, and 4. We anticipate that ultrasonic sensors will continue to be used in autonomous vehicles as its detection speed is fast, and effective. Additionally, it can be used in combination with camera mounted on the vehicle for obstacle detection purpose, so that the detection can be corroborated with multiple data sources.

Test case 2 can be mitigated by performing a fast calibration upon vehicle starts-up, to ensure that all sensors (including the ultrasonic sensors) are working properly.

V. CONCLUSIONS

The experiments conducted in this research were based on scenarios that could possibly occur in real life. Although they were performed in a laboratory setting, we have successfully demonstrated and simulated four attack scenarios on ultrasonic sensors, resulting in the inaccuracy in detecting obstacles using ultrasonic sensors.

We further demonstrated that the findings from our experiments show that an adversary can easily cause the ultrasonic sensors to behave abonormally when they are blocked, interfered by another ultrasonic sensor in the vicinity. In fact, these attacks are relatively low cost and can be easily replicated.

We thus advocate that in order to use ultrasonic sensors for guiding vehicle control, a multi-sensors should be implemented in order to allow these sensors to collaborate with each other to improve the accuracy of detection. Similarly, for fully autonomous vehicles, it is important that ultrasonic sensors are used in collaboration with the other-type of sensors so that these attacks on ultrasonic sensors can be mitigated.

In the future, we plan to extend the research by exploring the vulnerabilities of other sensors used in both modern and autonomous vehicles. It is also possible to attempt to compromise a set of sensors working together, so as to identify the vulnerabilities (and the associated impact) that lay within these autonomous features.

REFERENCES

[1] Arduino vs raspberry pi: Differences between the two. [Online] Available from: https://circuitdigest.com/article/arduino-vs-raspberrypi-difference-between-the-two [Accessed 16-March-2017].

[2] Autopilot. [Online] Available from: https://www.tesla.com/autopilot [Accessed 14-March-2017].

[3] Echolocation. [Online] Available from: https://askabiologist.asu.edu/echolocation [Accessed 14-March-2017].

[4] Hackers fool tesla ss autopilot to hide and spoof obstacles. [Online] Available from: https://www.wired.com/2016/08/hackers-fool-tesla-ss-autopilot-hide-spoof-obstacles/ [Accessed 20-March-2017].

[5] How acoustic foam works. [Online] Available from: http://www.proacoustic.co.uk/how-acoustic-foam-works/ [Accessed 16-March-2017].

[6] Model s owner's manual. [Online] Available from: https://www.tesla.com/sites/default/files/blog_attachments/model_s_owners_manual_europe_1.0_9.pdf [Accessed 16-March-2017].

[7] Model s release notes. [Online] Available from: https://www.tesla.com/sites/default/files/Model_S_release_notes_7_1_1_us_cn.pdf [Accessed 16-March-2017].

[8] Park aids. [Online] Available from: https://www.toyota-europe.com/world-of-toyota/safety-technology/parking-aids [Accessed 12-March-2017].

[9] Ping. [Online] Available from: https://www.arduino.cc/en/Tutorial/Ping [Accessed 16-March-2017].

[10] Summon your tesla from your phone. [Online] Available from: https://www.tesla.com/blog/summon-your-tesla-your-phone [Accessed 16-March-2017].

[11] Toyota rav 4 user manual. [Online] Available from: http://www.trav4.net/intuitive_parking_assist-112.html [Accessed 21-March-2017].

[12] Ultrasonic proximity sensor. [Online] Available from: http://www.globalspec.com/learnmore/sensors_transducers_detectors/proximity_presence_sensing/ultrasonic_proximity_sensors [Accessed 14-March-2017].

[13] Ultrasonic ranging module hc-sr04. [Online] Available from: http://www.micropik.com/PDF/HCSR04.pdf [Accessed 16-March-2017].

[14] Y. Chen, W. Xu, and J. Liu. Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle. *DEF CON*, 2016.

[15] T. Hoppe, S. Kiltz, and J. Dittmann. Security threats to automotive can networks–practical examples and selected short-term countermeasures. In *International Conference on Computer Safety, Reliability, and Security*, pages 235–248. Springer, 2008.

[16] C. Miller and C. Valasek. A survey of remote automotive attack surfaces. *black hat USA*, 2014.

[17] Miller.C and Valasek.C. Adventures in automotive networks and control units. *DEFCON*, 21:260–264, 2013.

[18] K. Mucevski. Automotive can bus system explained. [Online] Available from: https://www.linkedin.com/pulse/automotive-can-bus-system-explained-kiril-mucevski [Accessed 12-March-2017].

[19] M. Stoffel. The top 4 potential benefits of self-driving vehicles. [Online] Available from: https://9clouds.com/blog/potential-benefits-of-self-driving-vehicles/ [Accessed 17-April-2017].

[20] V. L. L. Thing and J. Wu. Autonomous vehicle security: A taxonomy of attacks and defences. *IEEE International Conference on Internet of Things*, pages 164–170, 2016.

[21] Waymo. Google self-driving cars. [Online] Available from: https://waymo.com/ [Accessed 19-April-2017].