Secure and Robust Ultrasonic Sensors for Autonomous Vehicles

Mayur Tulsibhai Lakhani
Dept. of Computer Science (Automotive Software Engineering)
Chemnitz University of Technology
Chemnitz, Germany
mayur-tulsibhai.lakhani@s2017.tu-chemnitz.de

***Abstract*—Since the past few years, road accidents are slightly increasing and many people losing their lives. At most time due to late response from the to handle when the vehicle or any object instantly comes towards to it. Autonomous vehicle consists of Ultrasonic sensors which takes several decisions and that's why it is necessary to make sensors consistent and reliable in hard real-time systems were missing the deadline must not be considered. In this paper, ultrasonic sensor's assessment under different kind of attacks are described which cause error while measuring the distance between vehicle and obstacle. To avoid these scenarios, one defense mechanism physical shift authentication is described by changing the certain parameters of the waveform such as phase, amplitude etc.**

***Index Terms*—Ultrasonic Sensor, Time of Flight, Security Analysis, Defence**

I. Motivation

The market has great impact due to use of Ultrasonic sensors which is increasing very rapidly from past few years. By market research magazines the compound annual growth rate is analyzed and evaluated 6% by the period of 2021-2027 as the significant growth in Automotive functional domain [1]. These sensors are used mostly for parking assistant application in passenger-centric domain and CrossAutomotive Functional Domain especially during the lane change to detect the vehicles. As given report by the Insurance Institute for Highway Safety of United States, approximately 14 percent vehicle meet with accident during parking in year 2018 [2]. Tesla model s is using 16 ultrasonic sensors to avoid accident during change of lane on the highway and safely park auto using summon mode [3] [4].

II. Introduction

Ultrasonic sensors have two transducers, from which one transducer can emit a signal and another can receive a reflected signal and give a measurement of the distance of the object. The IOT devices are used with these sensors in the parking systems with low speed. When the car is at high speed, then these devices are used to detect the object in the pathway of the car. When the auto vehicle is on autopilot mode, the safety of human beings is most necessary because the sensors are taking decisions and sensors can lose sensing power when any fault or error is produced on it by some external interface such as attacks or tapping fake signals between auto vehicle and object. So, here it might question comes and need to find answers to them. There are few experiments are taken including Tesla model S where some irregular measurements are evaluated and mention in Table I.

The first problem occurs when using on-board sensors to detect obstacles in the path by detecting a range of Ultrasonic sensors and with two different kinds of spoofing attacks such as random and adaptive analysis. The result says the attack can stop the running vehicle when there is an empty path or without any object in path. The second case when jamming and adaptive spoofing propagated on the automobile vehicle it gives inaccuracy. The non-existing object is populated in front of the sensor of auto vehicle which makes auto vehicle to stop. To empower the sensors is often challenging tasks because to make lot of modifications is not accepted by any automobile industries as it will cost more to develop it.
(a) Under different kind of attacks and scenario how Ultrasonic sensors are active to give response?
(b) What are the techniques to protect ultrasonic sensor from different kind of attacks? These answers are described in this paper by following sections.

This paper is well organized as follows: Section III presents the state-of-the-art of Ultrasonic sensors under different kind of attacks and the related work for this research, while in Section IV working principle is explained. The Section V describes attack overviews with different level attacks and Section VI describes different kind of attack strategies. Finally, at last the research conclusion and Acknowledgement described.

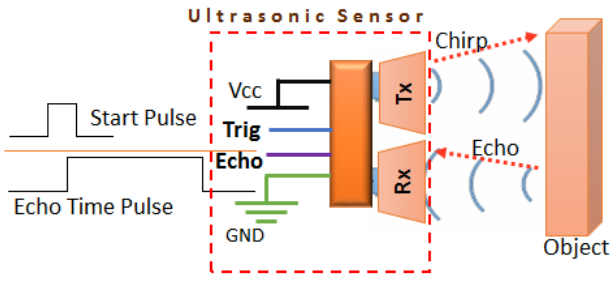


Fig. 1. Ultrasonic transducer block diagram [6]

TABLE I
AN OVERVIEW OF ATTACK AND GOALS [7]

Situation	Decision under Attack	Attacks
W/O obstacles	Stop Moving	Random Spoofing Adaptive Spoofing
W/ obstacles	Keep Moving	Jamming Adaptive Spoofing

III. STATE-OF-THE-ART

For parking assistant application Ultrasonic sensors introduced in 1990s. As the sensor emitting the ultrasound waves which will reflected from the surface of the obstacle and again catch by transducers. These waves have frequency beyond the upper limit of 20kHz. Time Of Flight is derived as first getting reflected echo from the propagated pings which is derived from the equation 1 where Where t_p is a propagation time and v_s is a velocity of the sound in air.

$$d = 0.5 \cdot t_p \cdot v_s \tag{1}$$

Ultrasonic sensors on the Auto vehicle are working generally on the frequency band between 40kHz to 50kHz which has overcome against the disturbance by the noise. The Frequency which has an upper limit of 50kHz generates weak echoes on the membrane attached with the piezoelectric transducer and lower than 40kHz lot of sound of noise interference. The experiments have been taken for security assessment check against physical attacks on the Ultrasonic sensors placed in Automobile, on which black-box tests reverse engineering of the sensor's printed circuit boards and by generating fake signals and injecting into the path to make defect into the accurate measurement.

Table II shows the 11 standalone sensors are tested indoors under spoofing and jamming attacks between frequency 40kHz to 50kHz and using COTS with low-cost hardware, and results are shown. Table II describes that at 40kHz frequency Ultrasonic sensors under random and adaptive spoofing evaluates the stable measurement while jamming is also minimal. In Automobile Network sensors and actuators relating to the Electronic Control Unit transfer signals received by CAN bus. At 300 μs, the transducer receives the signal waves from ECU and the result of the vibration of the membrane Ultrasound is generated. Even if the transmission is stopped still the sensor is receiving the sound as the ring -down time is approximately 700 μs. As a result, the sensor will not respond to the obstacle in the surrounding place. The Analog signals are generated from the vibration of the membrane, then signals are compared to the threshold to observe receiving echoes.

IV. WORKING PRINCIPLE

Figure 1 show the HC-SR04 Module which is used to detect obstacle and measure the distance. It has two transducer where one can emit the ultrasound waves and another transducer can receive the signals. It consists of Vcc pin for positive and negative for the GND. The circuit works on the 5V where

TABLE II
OVERVIEW OF ATTACKS ON STAND-ALONE SENSORS [7]

Sensor	**Frequency (kHz)**	**Output under Spoofing Attack**		**Jamming**
		Radom	**Adaptive**	
SRF05	40	Steady	Steady	Min
HC-SR04	40	Steady	Steady	Min
JSN-SRO4T	40	Steady	Steady	Min
US-100	40	Steady	Steady	Min
URM37	40	Steady	Steady	Min
RCW-0001	40	Steady	Steady	Min
URM04	40	Unsteady	Steady	Min
Grove U.R.	42	Steady	Steady	Min
SRF01	42	Unsteady	Steady	Min
MB1200	42	Unsteady	Steady	Max
AUDI Q3	50	Unsteady	Steady	Max

first the TRIG pin will be toggled high until and after goes low. It emits eight sound wave which makes Echo pin to pull high and while return it makes low[7][8][9].

A trigger of an ultrasound wave from the sensor gets reflected from a nearby object. This reflected echo sound wave returns to the sensor. This propagation time of sound waves is inversely proportional to the sound speed. The propagation time in this scenario is called the "time of flight". As the sound wave travels in the air two times the distance, distance between sensor and the object can be determined by following equation 2.

$$D = \frac{TOF \times C}{2} \tag{2}$$

where D is the distance between sensor and object, C is the speed of the sound wave, and TOF is the time of flight [10].

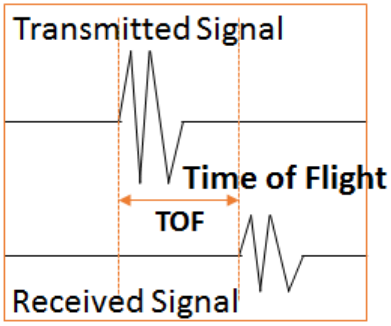


Fig. 2. Time of Flight [11]

The Ultrasonic sensor properties are analysed with parameters such as object detection range.As from the Figure 3 the object detection range is further classified as short range (15cm - 100cm) and long range (1m to 5m). The other parameter is angular range or directivity. Both the parameters depend on the sensor diameter and sound wave frequency. As the sound wave propagates through air, the ultrasonic energy decays. Therefore the detectable range reduces due to the attenuation. The high frequency transducers on one hand have more resolution and narrower directivity, on the other hand,it

have more attenuation. And therefor below relationship is plausible.

↑ Frequency :: ↑ Resolution :: ↑ Narrower Directivity :: ↑ Attenuation :: ↓ Distance [12]

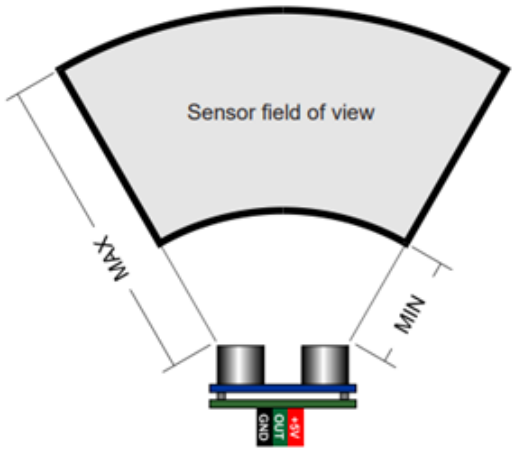


Fig. 3. Ultrasonic Sensor Range Illustration [11]

A. Classification of Ultrasonic Transducers

1. The mono-static transducer and bi-static transducer: the mono-static has only one transducer for transmission and reception, whereas bi-static has two separate ones

2. Low frequency and High frequency 30 kHz - 80 kHz frequency range is classified as low frequency, whereas 80 kHz - 130 kHz is classified as high frequency for ultrasonic sensors.

The low frequency transducers have benefits such as maximum long range performance and large off-the-self selection for purchase, whereas they have disadvantages such as long blind-zone in monostatic topology, and have low resolution.

The high frequency transducer have benefits such as maximum resolution, short blind-zone in monostatic topology, whereas having disadvantages such as short maximum detectable range and limited off-the-shelf selection for purchase [12]. Due to compact design and off the shelf large selection, a mix match of Monostatic Ultrasonic Sensor with lower frequency band is used in PPAS.

V. Overview of Attacks

In this section what kind of threats could be possible on the ultrasonic sensors and what results of effects on automobiles are analyzed and described.

A. Threat Model

This paper mainly focused on how can distort sensor's output using physical signal level channels. The capabilities are assumed as follows.

(a). Assessment of Sensor: Adversary requires certain parameters of design such as operational bandwidth, frequency, etc. It could be also smart with hardware design and can damage the functionality of the hardware to finish the task of the analysis.

(b). The scenario of Attack: The attacker can inject the crafted signals from sensors located on-board and continuously produces faked echoes in an arbitrary form which can modify certain parameters such as duration, frequency amplitude, and phase by increasing the strength of the transmitted signal.

(c). Contactless: An attacker can be located at any place surrounding the auto vehicle and can transfer with the auto vehicle. However, it has control on the selected auto vehicles but without physical attach it could observe the functionality of the on-board sensors.

B. Physical Signal Level

This kind of level attack is able to modify recognizing physical channels and modify calculation by sensors. Now the security question arises regarding the reliability of the sensors and needs to find answers for the following questions:
(a) If there is physical object, Will sensor remove and measure as blind spot?
(b) If there is no obstacle, Will the sensor evaluate the presence of any physical object?
(c) If the sensor collecting data, Will it automatically handle the Automobile vehicle and takes accurate decisions?
(d) If the sensor is under attack what kind of defense mechanism needs to accept?

Ultrasonic sensors release the ultrasound waves to find obstacles into the path, we can utilize two types of well-known attacks: spoofing – crafted signals are injected into the path so if there is no object it will detect an object and in jamming the noise injected into the signal which will deceive into the computation.

C. Categorization of Attack

The Electronic Control Unit(ECU) controls different kinds of active sensors In an Automobile vehicle which will transmit the waves and calculate the distance of the obstacle by receiving reflected echoes. One ECU will transmit to another ECU via CAN or LIN bus communication. The attacks are classified into three types which are as followed.

(1) Physical Signal Level Attack: It takes the benefit of a physical sensing channel to modify or obstruct the analog measurement of the sensor. Figure 5 shows that these attacks will not make any defect to the processing path of the data into the sensor.
(2) Sensor Hardware Level Attacks: In this kind of attack inside the sensor sensory signal mechanism is manipulated. For example, by injecting a voice signal to the Bluetooth headset and fake heartbeat into the pacemaker by blasting international EMI on the wire inside the sensor [13]. Same

as acoustic foam causes MEMS gyroscope and accelerometer to malfunction.[14][15]
(3) Digital Level attack: A digital level attack is a kind of cyber-attack that alters digital information or causes system down by exploiting digital channels such as network interface, file systems, memories, etc. For instance, researchers have demonstrated using cellular networks[16] and CAN bus [17] on automobile attacks can be done.

VI. Attack Methodology

(I) Injecting into the signal pathway: By changing the voltage supply on piezoelectric crystal it generates acoustic wave and frequency and amplitude of input signals resolve the acoustic waves. As a result by evaluating the AC signals will acknowledge vision AC signals and will report discrimination of the perceptive signals, and we manage to use oscilloscopes to avoid the cyclic waves that drive the piezoelectric crystal.

(II) Sampling over the air: Microphone or Ultrasonic sensors are not able to record the ultrasound waves so in the experiment microphone can be used which covers (4KHz - 9KHz) to sample the ultrasound which will analyze on the spectrum, oscilloscope, or smartphone apps. The sensor emits perceptive signals eventually with two sensor algorithms which are shown in Figure 4. SA1 according to the first echo and SA2 eventual perceptive signal. Most all the tested sensors are working with the SA1 and wait for a fixed amount of time. before the first echo or a time out to transmit to the next probes. All the sensors on the Automobiles are with SA2 and transmit ping every t2 without checking if echo occurs or not. The reason is ECU triggers with multiple sensors in a predefined order.

A. Random Spoofing Attack:
These attack randomly transmits the recorded signal waves at the exact time to deactivate the sensor signals and receive them and makes the fake object which is looked like as real object. Only the first reflected echo was received by the sensor. If there is not any obstacle nearby the sensor will wait for receiving it and after a certain period shows timeout duration before the new cycle starts. Its sensing range is 2 meters. is nearly 11.7ms. for an effective attack injected signals will be received before the transmitted real one. For attack need the ultrasonic transducer which has the same frequency as the target senor. For the transducer to run an Arduino [18] or waveform generator is used. Arduino gives digital input of the selected frequencies on a digital I/O pin. However, Arduino with its low-cost nature cannot generate the perfect ultrasound. Where in comparison function generator is more stable with high frequencies and amplitude.

Result: As a result of this kind of attack it will decrease the sensing value of the sensor. The experiments are validated on the Stand-alone sensors and On-Board sensors.

(1) Stand-alone sensors: Most of the stand-alone sensors adopt SA1, by choosing a period of spoofing, larger than T_1 and smaller than $T_1 + T_0$. It creates a non-existing obstacle that is not existing and similarly looks stationary. The reason is the sensors are transmitting the next probing signal after the waiting time of the T_1 as the first echo received. If we transmit a modified signal at a period shown in 3.

$$D = \frac{T_1 + 2d}{v_s} \tag{3}$$

where v_s is the velocity of the sound and the sensor will output constant measure the distance d.

(2) On-Board Sensors: by transmitting crafted signals over a certain period of time with few milliseconds automobile reports a non-existing obstacle. In Tesla Model S, this attack will force it to stop in self-driving mode. The attack distance was 2 meters when power was supplied to Arduino and can be increased when the high transmission power. Since the Vehicle ECU triggers each sensor creation time o period as SA2, random spoofing is unable to synchronize strictly with each ping. As a result, imaginary obstacles are tracked in the measurement of the sensor.

B. Adaptive Spoofing Attack: in Random Spoofing Attack, the location of non-existing obstacles could not be exactly found and create closer to the real one. So it will stop the automobiles unnecessary. The main goal of this attack is to create a non-existing obstacle that will be still at a fixed distance either closer or far from the real obstacle. Consequently, Automobiles may collide with physical objects. To form a fixed obstacle with any distance d for SA2 sensors, The adaptive spoofer has to transmit a spoofed signal at the exact timing. The sensor will receive a crafted signal at delay $2d/v$ as transmitting of probed pings and v denotes velocity. There are mainly three steps that occurred during this phase.(a) receives the transmitted sensor signals (b) discards the real echoes (c) transmits the spoofed signal instead of real ones. The spoofer consists of two transducers for transmitting and receiving signals. In the experiment, two ultrasonic transducers, amplification circuits, Arduino, a buffer amplifier are used. Adaptive spoofers analyze the sensor signals and control the timing for the transmission.

Results: Adaptive spoofing can either decrease or increase measure distance. The fixed non- existing object can be created for both the stand-alone and on-board sensors, and even manipulate the movements. The spoofer can be placed anywhere by the sensor's detecting range.in this experiment, the adaptive spoofer was placed 20 cm away from the sensors.The spoofer transmits the signal at delay time $2\,n\,Tv_0/v_s$ (n= 0,1,2.....) where v_0 is the velocity of the speed of imaginary obstacle, n is a sequence of the echoes and t is sensing period.

C. Jamming Attacks: Jamming attacks generate ultrasound towards a sensor such that these signals overcome to the echoes. Resonant frequency: From experiments on several vehicles, it showed the operation frequency appears to be near 50kHz. In the experiment, 40kHz transducers are used for jamming the signal as the 50kHz were unavailable. Since ultrasound transducers are working on narrow band 40kHz

transducers can supply 50kHz ultrasound efficiently. As 40kHz frequency is not effective and needs to expend to the 50kHz transducers.

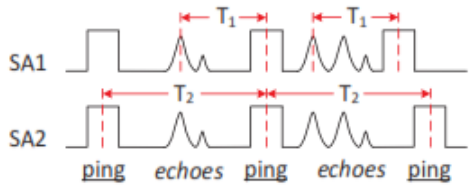


Fig. 4. Two probing algorithms [7]

Voltage Level: the sound's amplitude produced by the piezo-electric crystals depends on the voltage. So effective jamming can be applied by giving voltages. In our experiments, Arduino can produce square waves at a maximum of 5 volts and the function generator gives output up to 20 volts. An ultrasonic transducer can obtain 70 volts and it observed that effective range can go beyond what is observed. Results: Results are taken under the following scenario and validated.

1) Stand-Alone Sensors: Under jamming attacks, it is observed for the minimum distance the sensor reports an obstacle with minimum distance (0-10cm) and maximum distance no obstacle detection. The existence of the obstacle can be determined at a minimum distance if the amplitude of received ultrasounds is larger than a predefined threshold. Under the jamming attack if the sensor passed through the analysis period it will receive the jamming signal and echoes in the resulting minimum distance. Thresholds are adjusted to reduce the noise in the maximum distance. From the Figure[] by tapping into the path of signal realized that noise come into the jamming signal and threshold increased by the noise. In these situations sensor can not detect the object as the amplitude of the legitimate echoes is smaller than threshold.

(2)Vehicle with auto-parking mode: in Automobiles, the ultrasonic sensors are placed on the front of car bumpers and obstacles can be detected. Once a jamming attack is released vehicle will not alarm or not detecting the obstacles in the path. The function generator can easily attack running Tesla from a distance of 10 meters away.

(3) Autopilot Mode (Tesla Model S): There are several experiments are taken on Tesla Model S with Auto Park and summon mode. As several tasks are performed to check obstacle reliability under jamming attacks where it can stop the vehicle in the Auto Park system or also the functionality of obstacle distance measurement. The results are conspicuous and worrisome. In the Auto Park mode if a jamming attack happens then Tesla ignores the obstacle and hits them, and this could be done by increasing power amplifiers.

D. Summary

In this summary, the following attacks are validated

• Random Spoofing: This attack creates non-existing objects which are near or far from the physical objects, and it can force running autonomous vehicles to stop when it should keep running on the track.

• Adaptive spoofing: This attack creates the non-existing object which is very near or far from the real object which creates irrelevant decisions and stops vehicles when it should keep moving ahead on the track.

• Jamming attacks: In this attack, the sensor stops detecting the obstacle's functionality and a crash happens.

VII. Enhancing ultrasonic Sensors

How We can enhance the security of the Ultrasonic sensors, this section describes some techniques and which kind of security level of function needs that is described here.

(a) Exposure of Attack: Minimally defense mechanism should be able to find occurrence of it and report as an attack so the driving system can take proper decisions correctly.

(b) Resilient Obstacle Detection: Due to Spoofing attacks needs proper enhanced algorithm to identify crafted signals from the real echoes.

(c) Attack Localization of Attack: The Most challenging thing is to detect the location of the attacker.

As From Figure 5 automobile vehicles consist set of ultrasonic sensors and ECU and using this sensors there two types of the schemes can be described:

(I) Physical Shift Authentication uses individual sensors to detect attacks and perform Resilient Obstacle Detection.

(II) Multiple sensor Consistency Check uses set of ultrasonic sensors as a group to perform Resilient Obstacle Detection.

We abstract the functions of every schema against different attacks in Table III. These schema will not sufficient individually to handle attack but as combine strategy it can enhance the reliability of the sensor system.

(A) Physical Shift Authentication: This method verifies the physical signals by the changing waveform parameters. Ultrasonic sensors are transmitting the signals at the same waveform throughout the lifetime and search for only the first echo based on the power supply. It uncovered ultrasound which has adequacy is higher than the limit So there's no association between transmitted pings and echoes. To detect the attack and make it possible to remove spoofed signals it is necessary to make bondage between them. PSA suggests modifying the ping waveform and co-relate it with received echoes. The procedure of PSA is summarized as following steps:

(1) Customize the ping Waveform X. Transmit it.

(2) Receive the echoes. Measure the echo waveform Y.

(3) if $C(X, Y) > \alpha$, accept otherwise reject echoes.

Consider the sonar applications where certain parameters of the waveform are analyzed and measured or estimated for advanced target measurement and identification [19]. There is still no assurance that physical parameters can be used for signal authentication when they include uncertainty after reflection. To assess the feasibility of the sensor system, it can be done by modulating certain parameters of the ping waveform (such as amplitude, phase, etc.) as candidates for

the waveform feature . Generally a sequence of the customized pings, and let the waveform of the i[th] ultrasonic ping be.

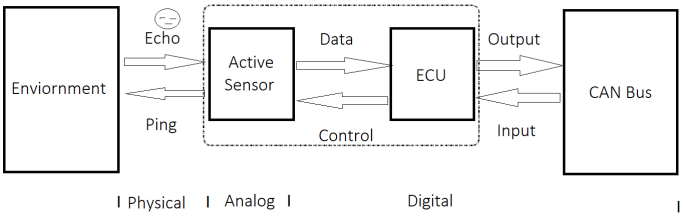


Fig. 5. Active sensor systems [7]

$$s_i(t) = A_i \cos(2\pi f_i t + \varphi_i), t \in [\sum_{j=1}^{i} \Delta_j, \sum_{j=1}^{i} \Delta_j + T_i] \quad (4)$$

Where A_i is the amplitude, f_i is frequency, φ_i is the phase, and T_i is duration of the ith ping . Di is the period. i.e., the time period between the i[th] and (i -1)[th] ping let D1=0

The exact concept is analyzed with Radio Frequency signals on Ultrasonic sensors in automobile industries and still, there is not much evidence to prove it correct. The Following questions come, and which need to find the answer. (a) is there a possibility to do modification into the amplitude Ai, frequency fi phase Oi, duration Ti, and period Di of every ping? (b) If the ping waveform is modified, does it change to the reflected echoes? (c) From passive attacker, how accurately it can be discriminated against the modulated echoes with crafted echoes?

To find answers to these questions, we use a set of two transducers – one transducer connected to the signal generator and another one is with an

oscilloscope. Side by side towards an obstacle close by you. The echoes can be observed or measured on an oscilloscope after amplification.

(1) Frequency Shift: Here mainly two questions arise. Firstly, are there different frequencies that can be generated by the Ultrasonic sensors? Secondly, if reflected signals are received, will it make changes to the frequency randomly? Since ultrasonic sensor emits ultrasound in a narrow frequency band centered at their resonant frequencies determined by the diameters of the piezoceramic. In the test wideband microphone was placed 10 cm far from the ultrasonic transducers [20]. The frequency is modified between 35kHz to 45kHz and the Sound Pressure Level (SPL) is plotted of received echoes. From Figure 6(a), As the frequency of stimulation signals deviates from the resonant frequency (40 $\pm$ 1 kHz), the SPL receives reduce ultrasound. So, to ensure the detection range of an ultrasonic sensor, it is analytical to choose in between 38.5kHz to41.5kHz.

The startup time fluctuated with the different transducers, and which is generally larger than the typical ping duration (8 - 20 cycles of sinusoid). By setting the duration 2.5ms at 40kHz per ping to 100 cycles so that frequency is stable and not affected by the ring-down period. Figure 6(b) shows if an obstacle is stationary, the frequency of echoes closes to the transmitted pings where maximum alternation of 0.212 kHz in-band between 39 kHz to 41 kHz. When a vehicle is moving at a time the maximum alternation will be the speed 15km/h Doppler shift will be 0.48kHz. From the experiments, it concluded that f_i can be shifted randomly between the different pings, and authentication can be done per ping by checking $t(i) == x(i)$.

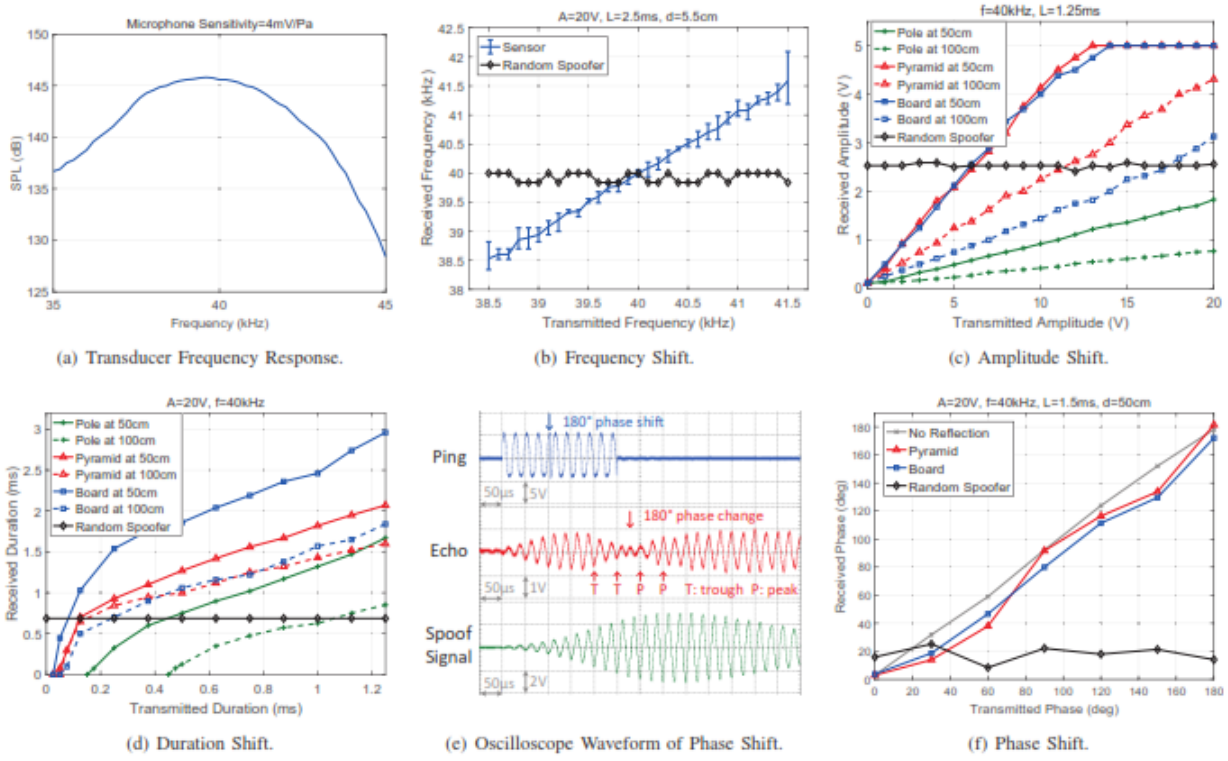
Phase Shift: As Figuer 6(c) shows, ultrasonic sound is mechanical vibration to change the phase of it is difficult immediately not similar to how radio signals change. Here the phase shift at 180 Degree is a sudden shift of force direction and vibrating the membrane of the transducer. So when forced is shifted in the reverse direction the amplitude decreases and increases by a new phase. For validation of arbitrary phase shift, ultrasound transmitter with vector signal generator [32] capable of phase modulation and calculate phase shift of the intensifying received waveform. Consider phases before and after phase shift were φ_A and φ_B. For calculating the phase shift $|\varphi_A - \varphi_B|$, needs a reference signal with phase φ_R on another flag of the oscilloscope and extracts two phase differences $|\varphi_A - \varphi_R|$ and $|\varphi_B - \varphi_R|$. As shown in the figure received phase shift is near to modulated phase shift validation and can be achieved per every cycle.

VIII. Conclusion

The experiments validate that by changing certain parameters such as shifting frequency, phase, amplitude, duration, and the period from the waveform, it can be used to differentiate the spoofed echoes from the transmitted pings and does not change modulated pings. During each cycle at the same time and frequency, the performance rank is Duration Shift ¡Amplitude Shift ¡ Phase Shift ¡ Frequency Shift. With minimum two-cycle frequency shift detection rate is 98.35% under a false positive rate of 5% and the successful detection rate with three cycles of frequency shift is 99.8% and can be increased with a wider transducer frequency range. The effective range of the attacks relies on both the operational range of sensors and the transmission power of the attacking equipment, which can be improved with budgets. The reliability of ultrasonic sensors still remains a critical question under different kinds of attacks and by using security intensification mechanisms.[7]

Acknowledgment

The report is drafted under the direction of the staff of Professorship Measurement and Sensor Technology, Chemnitz University of Technology, Germany. Special thanks say to the Dr.-Ing. Olfa Kanoun, Chair for Measurement and Sensor Technology, TU Chemnitz for providing the course Automotive Sensor Systems as a platform to initiate and perform an extensive study on Ultrasonic sensor and also like to thank to fellow faculties including Dr. Sonia Bradai, Dr. Slim Naifar and all other responsible person of this course for their ceaseless input, amid addresses and activities which enhanced the nature of the examination.



(a) Transducer Frequency Response. (b) Frequency Shift. (c) Amplitude Shift.

(d) Duration Shift. (e) Oscilloscope Waveform of Phase Shift. (f) Phase Shift.

Fig. 6. The experiment results of the Physical Shift Authentication [7]

REFERENCES

[1] Grandviewresearch.com, "Ultrasonic Sensors Market Size, Share & Trends Analysis Report By Technology". "Ultrasonic Sensors Market Size, Share & Trends Analysis Report By Technology (Retro-reflective Sensor, Through-beam Sensor), By Type, By End-use (Automotive, Consumer Electronics), By Region, And Segment Forecasts, 2021 – 2027. May 28, 2021. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/ultrasound-sensors-market

[2] H. Lee, D. Kang and W. Moon, "Design and Fabrication of the High Directional Ultrasonic Ranging Sensor to Enhance the Spatial Resolution," TRANSDUCERS 2007 - 2007 International Solid-State Sensors, Actuators and Microsystems Conference, 2007, pp. 1303-1306, doi: 10.1109/SENSOR.2007.4300377.

[3] IndustryARC, "Ultrasonic Sensor Market - Forecast(2020 - 2025), " doi: AIR0069. May 02, 2020. [Online]. Available: https://www.industryarc.com/Report/214/Ultrasonic-sensor-market-analysis-Forecast-report.html.

[4] Tesla, "A tragic loss, "https://www.tesla.com/blog/tragic-loss, 2016.

[5] U. Khalil, A. Nasir, S. M. Khan, T. Javid, S. A. Raza and A. Siddiqui, "Automatic Road Accident Detection Using Ultrasonic Sensor," 2018 IEEE 21st International Multi-Topic Conference (INMIC), Karachi, 2018, pp. 206-212, doi: 10.1109/INMIC.2018.8595541.

[6] Manpreet Kaur, Jai Pal, "Distance Measurement of Object by Ultrasonic Sensor HC-SR04," "International Journal for Scientific Research Development,Vol. 3, Issue 05, 2015.

[7] W. Xu, C. Yan, W. Jia, X. Ji and J. Liu, "Analyzing and Enhancing the Security of Ultrasonic Sensors for Autonomous Vehicles," in IEEE Internet of Things Journal, vol. 5, no. 6, pp. 5015-5029, Dec. 2018, doi: 10.1109/JIOT.2018.2867917

[8] B. S. Lim, S. L. Keoh and V. L. L. Thing, "Autonomous vehicle ultrasonic sensor vulnerability and impact assessment," 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 2018, pp. 231-236, doi: 10.1109/WFIoT.2018.8355132.

[9] Amebaiot. "[RTL8195AM] [RTL8710AF] GPIO - Measure the distance by ultrasonic module", May 14,2021 [Online]. Available: https://www.amebaiot.com/en/ameba-arduino-gpio-ultrasonic/

[10] Texas Instruments, "Ultrasonic Sensing Basics, " Application Report,Sep. 2019 [Revised Mar. 2020]. Apr 18, 2020. [Online]. Available: https://www.ti.com/lit/an/slaa907c/slaa907c.pdfts=1590259077412.

[11] BAGRAM, "Subminiature Motion Sensor 5V CRN-5480," CRN-5462 Ultrasonic Sensor Data-sheet. May 18, 2020. [Online]. Available:https://stairslight.com/14,subminiature-motion-sensor-5v-crn-5480.

[12] Texas Instruments, "Ultrasonic Proximity-Sensing Module (PSM) Reference Design Design Guide: TIDA-060024 Ultrasonic Proximity-Sensing Module (PSM) Reference Design, "TIDA-060024 Data-sheet, Sep. 2019 [Revised Mar. 2020]. May 15, 2020. [Online]. Available: http://www.ti.com/tool/TIDA-060024

[13] D. Foo Kune, J. Backes, S. S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, and W. Xu, "Ghost talk: Mitigating EMI signal injection attacks against analog sensors," in Proceedings of the IEEE Symposium on Security and Privacy. IEEE, 2013.

[14] Y. Son, H. Shin, D. Kim, Y. Park, J. Noh, K. Choi, J. Choi, and Y. Kim, "Rocking drones with intentional sound noise on gyroscopic sensors," in Proceedings of the 24th USENIX Security Symposium, 2015.

[15] T. Trippel, O. Weisse, W. Xu, P. Honeyman, and K. Fu, "WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks," in Proceedings of the IEEE European Symposium on Security and Privacy, 2017.

[16] R. Katzwinkel, R. Auer, S. Brosig, M. Rohlfs, V. Schöning, F. Schroven, F. Schwitters, and U. Wuttke, "Einparkassistenz," in Handbuch Fahrerassistenzsysteme. Springer, 2012, pp. 471–477

[17] M. Noll and P. Rapps, "Ultraschallsensorik," in Handbuch Fahrerassistenzsysteme. Springer, 2012, pp. 110–122.

[18] Arduino, "Arduino and Genuino project,", May 20, 2021,[Online]. https://www.arduino.cc/, 2016.

[19] R. D. Hippenstiel, Detection Theory: Applications and Digital Signal Processing. CRC Press, 2001.

[20] Cry Sound, “Cry343 free field measurement microphone,” [Online]. http://www.crysound.com/productinfo.php?4/35/63, 2017.