Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-driving Vehicle

Chen Yan
Zhejiang University
yanchen@zju.edu.cn

Wenyuan Xu
Zhejiang University
& University of South Carolina
wyxu@cse.sc.edu

Jianhao Liu
Qihoo 360
liujianhao@360.cn

ABSTRACT

To improve road safety and driving experiences, autonomous vehicles have emerged recently, and they can sense their surroundings and navigate without human intervention. Although promising and proving safety features, the trustworthiness of these cars has to be examined before they can be widely adopted on the road. Unlike traditional network security, autonomous vehicles rely heavily on their sensory ability of their surroundings to make driving decision, which incurs a security risk from sensors. Thus, in this paper we examine the security of the sensors of autonomous vehicles, and investigate the trustworthiness of the 'eyes' of the cars.

Our work investigates sensors whose measurements are used to guide driving, i.e., millimeter-wave radars, ultrasonic sensors, forward-looking cameras. In particular, we present contactless attacks on these sensors and show our results collected both in the lab and outdoors on a Tesla Model S automobile. We show that using off-the-shelf hardware, we are able to perform jamming and spoofing attacks, which caused the Tesla's blindness and malfunction, all of which could potentially lead to crashes and impair the safety of self-driving cars. To alleviate the issues, we propose software and hardware countermeasures that will improve sensor resilience against these attacks.

Keywords

Autonomous vehicles; security; ultrasonic sensors; millimeter-wave radars; cameras

1. INTRODUCTION

Improving road safety, driving experiences, and driving efficiency has long been a focus of the automotive industry, and already we have witnessed the rapid development of ADAS (Advanced Driver Assistance Systems), which can sense its driving environment and warn drivers of immediate dangers. With the advances in sensing technology and information fusion, vehicles are going forward into a new era — fully autonomous vehicles. Numerous major companies and research organizations have developed their prototype autonomous cars. For instance, Tesla Motors has popularized driverless technology with its Autopilot system.

The safety of autonomous cars has been a focus of the prolonged debate over this technology. Comparing to traditional ones, autonomous vehicles requires almost no human inputs for driving control, therefore safety relies purely on the on-board computing systems, which in turn depend on sensors and their measurements of the surroundings to make driving decisions. Being the 'eyes' of on-board computing systems, sensors play an important role in autonomous vehicle safety, and their accuracy and immediacy have to be guaranteed to achieve safe autonomous driving.

The industry has been working on improving the accuracy and robustness of sensors. Yet the recent accident of a Tesla Model S car crashing into a white truck and causing one death using its on-board Autopilot system [26] shows that existing sensors cannot reliably detect neighboring cars even in normal yet special road conditions, not to mention intentional attacks against these sensors. In light of the fact that the security issues of sensors have not earned their due attention, we investigate attacks that utilizing the underlying principles of sensors to blind or deceive them, e.g. utilizing how to detect barriers leveraging lights, sounds, and radio waves. This type of attacks against sensors can lead to malfunctions, falsified readings, or even physical damage, and the consequences could be fatal both to one car and to a collection of cars nearby, i.e., in a Vehicle to Vehicle (V2V) network.

Understanding the attack methods, its feasibility, its influences on sensor readings, on-board computer systems and autonomous car behaviors will provide insights for improving the safety of self-driving automobiles. In this work, we performed an empirical security study on the sensors of autonomous cars. Specifically, we studied and examined three types of essential automotive sensors that are widely used for autonomous driving, i.e., ultrasonic sensors, Millimeter Wave Radars, and cameras. We have carried out several attacks against them, and proved the destructive impact of attacks on the sensor data, as well as on the automated driving systems by experiments on a Tesla Model S sedan.

Contributions. We summarize our contributions as follows:

- We raise the security risks and concerns of sensors used for Automated Driving and Advanced Driver Assistance Systems.
- To the best of our knowledge, we are the first to experimentally examine the feasibility of launching con-

ACM ISBN 978-1-4503-2138-9.
DOI: 10.1145/1235

tactless attacks on automotive ultrasonic sensors and MMW Radars. Our experiments in the laboratory and outdoors on vehicles have demonstrated the consequences of jamming and spoofing attacks by exploiting the underlying sensing principles.

- We have verified the attacks on a Tesla Model S with Autopilot systems, and demonstrated the impact of these attacks on automated driving system.

Roadmap. The rest of this paper is organized as follows. Background and related work on vehicle security are given in Section 2. We introduce automated driving system and relevant sensors in Section 3, and list the threat model and steps of study in Section 4. The details of attacks on ultrasonic sensors, MMW Radars, and cameras are given respectively in Section 5, 6, and 7, respectively. In Section 8 we discuss the attack feasibility and countermeasures, as well as limitations and future work. Section 9 concludes the paper.

2. BACKGROUND AND RELATED WORK

The security of automotive systems has been studied for more than a decade. The security risk stems from the structure of automotive system, i.e., the interconnection of communication buses and *Electronic Control Units* (ECUs). Today, the infrastructure of modern vehicles is designed in such a way that all components are networked with each other by the CAN-bus, and they can exchange data as well as control commands via the bus. This structure guarantees the functionality and efficiency of modern vehicles, but poses a serious threat in addition to potential insecure components [32][33]. For example, security breach on one ECU (especially those with external connections, e.g., telematics) could possibly lead to the exploitation of other safety-critical ECUs through the unprotected bus network (e.g., CAN bus) and endangers the whole vehicle.

Several studies [12][28] have shown the feasibility of launching CAN bus attacks (mainly through OBD-II port) which can cause malfunction and even take control of the car. It has been demonstrated that an attacker who is able to infiltrate virtually any ECUs can leverage this ability to completely circumvent a broad array of safety-critical systems, such as falsifying the control panel displays, disabling the brakes, killing the engine, and rolling the steering wheel.

In addition, it has been shown that the attacks can be launched without any physical access to the car. Checkoway et al. [3] analyzed the external attack surfaces of a modern automobile, and discovered that remote exploitation is feasible via a broad range of attack vectors (including mechanics tools, CD players, Bluetooth and cellular radio), and further, that wireless communications channels allow long distance vehicle control, location tracking, in-cabin audio exfiltration and theft. Miller and Valasek, after their survey [15] of 21 popular car models, performed a remote attack against un unaltered Jeep Cherokee that resulted in physical control of part of the vehicle [16].

Previous researches on vehicle security mostly focused on the internal network and Electronic Control Units (e.g., telematics and immobilizer). However, few attention has been paid to sensors. Existing attacks depend mainly on vulnerable information interfaces, while the sensory (physical) channels have not attracted their due attention and shall be exploited thoroughly.

Petit et al. has recently raised people's attention to sensors by his study on LiDAR and cameras [19]. Their work focused on remote attacks on camera-based system and LiDAR using commodity hardware, which achieved effective blinding, jamming, replay, relay, and spoofing attacks.

In our research, we focus on the security of popular vehicular sensors that have already been widely used in *Advanced Driver Assistance System* (ADAS) and self-driving cars. We will show experiment results that were conducted both in laboratories and on popular cars, including models of Tesla, Audi, Volkswagen, and Ford.

3. SYSTEM OVERVIEW

In this section we give a brief introduction to the Automated Driving System and Advanced Driver Assistance System, as well as the sensor technologies, and discuss the motivation to examine ultrasonic sensors, MMW Radars, and cameras.

3.1 Automated Driving System

Autonomous vehicles, saved for later.

3.2 Sensor Overview

Before discussing the detailed principles underlying these sensors, we overview their features and compare their difference.

Sensor categories. Ultrasonic sensors, MMW radars, cameras, and LiDAR are indispensable sensors on current self-driving vehicles. Each is designed for its dedicated sensing range. Nevertheless, they, in combination, can detect obstacles in a wide range. They can be roughly divided into proximity, close-range, middle-range, and long-range, as shown in Figure 1.

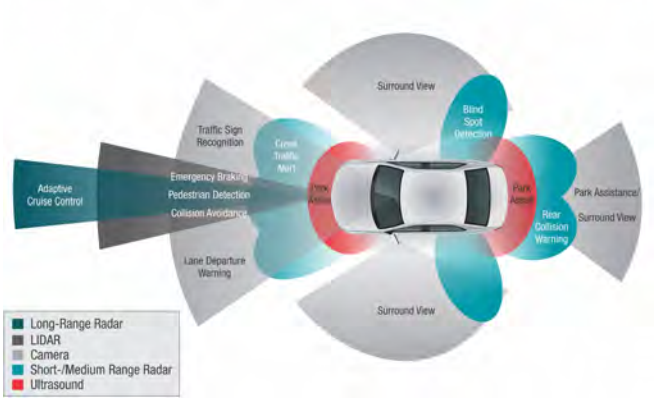


Figure 1: Major ADAS sensor types and typical vehicle positions [24].

1. *Proximity* ($5m$). Ultrasonic sensors are proximity sensors that aim at detecting barriers within several meters from the car body. They are mainly designed for low speed scenarios, e.g., parking assistance.

2. *Short Range* ($30m$). Forward-looking cameras are used for lane departure warning, Traffic sign recognition, and backward cameras are for parking assistance. Short-range radars (SRR) serve for blind spot detection and cross traffic alert.

3. *Medium Range* ($80 - 160m$). LiDAR and Medium-range radars (MRR) assists collision avoidance and pedestrian detection.

4. *Long Range* ($250m$). Long-range radars (LRR) are designed for Adaptive Cruise Control (ACC) at high speeds.

Because the physical principles underlying these technologies varies, their operation ranges are different as well. We emphasize the major differences of these technologies below.

Physical principle. On-board vehicle sensors for detecting barriers and road condition utilize three types of waves. Both LiDAR and cameras rely on lights (i.e., infrared and visible light) to recognize objects. In comparison, ultrasonic sensors detect obstacles by transmitting and receiving ultrasound, which is one type of mechanical waves with their frequency beyond human hearing ranges. MMW radars rely on millimeter waves, a band of electromagnetic wave whose frequency is much lower than light yet much higher than well-known radio frequency range (e.g., 2.4 GHz). Because each type of sensors rely on a distinct underlying principle, various methods and equipment have to be utilized to attack each type of sensors.

Cost. Costs of manufacturing sensors determine their market shares. The costs from low to high are the ones of ultrasonic sensors, cameras, radar, and LiDAR. Because of the low cost, ultrasonic sensors have been widely deployed on modern vehicles for parking assistance systems, but other sensors are reserved for high-end features. Cost-performance trade-off is perhaps the reason that car manufacturers (e.g., Tesla) abandon LiDAR [8], but self-driving prototype developers (e.g., Google [7] and Stanford [25]) tend to utilize every possible sensor.

Since not all manufacturers utilize LiDAR, we examine the other three types of sensors that have been widely applied on existing vehicles for driver assistance system, with a focus on ultrasonic sensors and MMW radars in this work. The security vulnerabilities of automotive ultrasonic sensors and MMW radars have never been discussed before. We believe that our work is complementary to Petit's work, and together we provide a better picture of the sensor issues in self-driving vehicles. Apart from in-lab studies on standalone sensors, we carries out outdoor experiments on vehicles in this work. Note that Tesla model S cars employ all three sensors in the 'Autopilot' systems and thus most of our work involves testing on a Tesla model S vehicle.

4. ATTACK OVERVIEW

This section gives an overview on our attacks. In the threat model we propose the assumptions and requirements of an attacker. In the attack model we introduce our basic ideas and research steps.

4.1 Threat Model

Knowledge Threshold. We assume that the attacker may not have prior knowledge of the sensing mechanism, and need to learn or consult professionals. In the extreme case that the attacker being a sensor expert himself, he may be well-aware of the vulnerabilities or proficient with the attack skills, but he still need to overcome the knowledge threshold of other sensors. We further assume he is medium financed and qualified for independent or collaborative research.

Equipment Awareness. We can assume that an attacker has access to the targeted sensors or similar ones for prior study, considering that sensors of the same kind but from different vendors can exhibit distinctive patterns in the physical channel. The attacker may be proficient with hardware design, or can exploit off-the-shelf hardware to fulfil his attack purposes. We don't think he has access to expensive equipments or well-funded research facilities.

Attacker Position. The attacker has to be outside the car in order for the attacks to be executed and remain stealthy.

Limitations. No physical alteration or damage is allowed or can be made to the targeted vehicle with the purpose of dampening the performance, i.e., the vehicle and sensors have to remain unaltered.

Attack Outcome. With dedicated research effort and at least the above mentioned qualities, we think an attacker can cause malfunction of low-priority close-range sensors, and cause collisions in maneuvering. He may have a chance in disturbing safety-critical sensors, but the attack is likely impractical when the vehicle is fast moving.

4.2 Attack Model

Three very different kinds of sensors are under the scope of our attacks, therefore their approaches also exhibit great diversity. Before presenting the specifics, there are some common points they share that we would like to stress.

4.2.1 Sensor Attacks

The most significant distinction between sensor attacks and cyber attacks is the use of physical channels. Sensor attacks utilize the same physical channels as the targeted sensor in most cases, which can disrupt or manipulate the sensor readings. Since sensors are categorized as the lower layers of a control system and are normally trusted, falsified readings could lead to unexpected consequences of a system. A recent example would be the acoustic attack against the gyroscopic sensors on a drone [23].

Comparing with cyber attacks, sensor attacks have the disadvantages of close attack range, extra hardware requirement, long exploitation cycle, and high knowledge threshold. Given the fact that different sensors may depend on completely different physical principles, very different methods must be used against them, which means low transplantability. In this work, we use ultrasound against ultrasonic sensors, radio against MMW radars and laser against cameras. Noticeably, ultrasound, radio, and laser all promise no physical contact with the targeted sensors, thus make our attacks contactless.

4.2.2 Basic Idea

Our basic idea for examining the security of all three sensors is to analyze their following abilities by injecting noise and crafted signals, i.e., jamming and spoofing attacks in their physical channels.

I. Resistance to noise (Jamming Attack)

The sensors are designed to resist environmental noise, which exists in normal working conditions. For example, there may occur acoustical interference from other objects near the vehicle, in particular the noise of compressed air (e.g., truck brakes) and metallic friction noise from track vehicles [21]. However, their ability to resist intentional noise or loud noise has not been published. The injected noise will very likely lower the Signal to Noise Ratio (SNR) and make

the detection impossible.

II. Resistance to malicious physical channel injection (Spoofing Attack)

Receiving genuine physical signals from the wrong source can happen when sensors are wrongly positioned, e.g., facing each other. By analogy, if malicious injected signals are made to emulate physical patterns of the real ones, it is possible for them to be taken as real measurements, so as to disrupt sensor readings. If the crafted signal can be further controlled, the readings could possibly be manipulated.

4.2.3 Research Steps

To examine the security of vehicular sensors, we basically went through the following steps.

1. Taking stand-alone sensors for laboratory experiments.
2. Studying the sensors by any means.
3. Performing jamming and spoofing attacks.
4. Testing the attacks on vehicles.
5. Testing the attacks on automated driving system.
6. Improving and looking for new attack methods.

Potential attack surfaces including sensors in autonomous automated vehicle has been discussed in [19], but most of them have not been examined or validated by experiments or on vehicles. In the coming sections, experimental attacks on ultrasonic sensors, MMW radars, and forward-facing cameras are illustrated and discussed in details.

5. ATTACKING ULTRASONIC SENSORS

Ultrasonic-based parking assistance system was first introduced in the European market in the early 1990s. This system monitors the front and rear of the vehicle, and warn the driver if there are obstacles in the vicinity of the vehicle that can cause collisions. Power functionalities like semiautomatic parking assistance, fully automatic parking, parking space detection, and Tesla's new summon feature (parking with driver outside the vehicle) [27] have been realized based on the same sensor technology. Ultrasonic sensors can help to have an eye on the invisible parking space and to park the vehicle easily, quickly, and safely [11].

Besides automotive application, ultrasonic sensors are also used in many other fields since long, such as in military for submarines, in medicine for diagnostics, in materials for testing, and in industry and robot technology for distance measurement [2][13][29]. We believe studies on the security of ultrasonic sensors can shed light rather than on automotive itself.

In this section, fundamentals of ultrasonic sensors are to be first introduced as the background of our attack, then we present our attack methods and results acquired in the lab and outdoors. By making a DIY ultrasonic jammer with a low-cost Arduino, we managed to launch jamming and spoofing attacks on ultrasonic sensors, and tested on several popular car models, including a Tesla Model S. We will demonstrate the following:

- Jamming attack can make objects **undetectable** so as to cause collisions, or force the car to stop while performing self-parking.

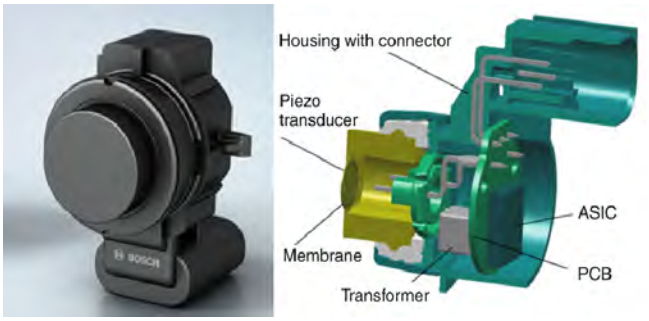


Figure 2: Appearance and cross-section of an ultrasonic sensor from Bosch.

- Spoofing attack can manipulate the sensor readings, and lead to the display of pseudo-obstacles.
- Acoustic cancellation is possible, but dedicated hardware and algorithms are required.

5.1 System Model

The distance measurements using ultrasonic sensors according to the pulse/echo principle are very straightforward from the technical viewpoint because of the comparably low speed of sound. Ultrasonic sensors detect objects by emitting ultrasonic pulses, and measure the time taken for the echo pulses to be reflected back from obstacles. The distance to the nearest obstacle is calculated from the propagation time (time-of-flight, TOF) of the first echo pulse to be received back according to the equation

$$d = 0.5 \cdot t_e \cdot c \tag{1}$$

with t_e: propagation time of ultrasonic echoes, c: velocity of sound in air (approximately 340 m/s). A method called *trilateration* is further used to calculate the real distance to the vehicle from the direct readings of neighboring sensors.

Components. The sensor consists of a plastic housing with integrated plug-in connection, an ultrasonic transducer, and a printed circuit board with the electronic circuitry to transmit, receive, and evaluate the signals, see Figure 2.

Piezoelectric Effect. The acoustic part of an ultrasonic sensor is the transducer. Same as transducers in the hearing range (better known as microphones and speakers), ultrasonic transducers are build on the piezoelectric effect [17]. The piezoelectric effect describes the electromechanical context between the electric and the mechanic status of a crystal. If a voltage is applied at the electrodes on two sides of a piezoelectric crystal, a mechanical deformation results and generates acoustic wave. Vice versa, an incoming acoustic wave creates oscillations of the crystal. As a consequence, an alternating voltage is generated at the electrodes which can be amplified and further processed.

Mechanisms. When the sensor receives a digital transmit signal from the ECU, the circuit excites the membrane with square waves (approx. 300 μs) at its resonance frequency (40 – 50 kHz), so it vibrates and emits ultrasound. No reception is possible during the time taken for it to stop oscillating (approx. 700 μs), which is also known as the ringdown problem. Once rested, the membrane can be made to vibrate again by the echo reflected back from the obstacles. These vibrations are converted by the piezoelectric crystal

to an analog signal, which is then amplified, filtered, digitized, and compared to a threshold to determine the echo's arrival. The time-of-flight diagram is finally transmitted to the ECU for further distance calculation.

Frequency. For ultrasonic transducers in automotive parking aid systems, an operating frequency between 40 and 50 kHz is commonly used. This has been proved as the best compromise between good acoustical performance (sensitivity and range) and high robustness against noise from the surrounding of the transducer. Higher frequencies lead to lower echo amplitudes because of higher dampening of the airborne sound, whereas for lower frequencies the proportion of interfering sound in the vehicle environment is always increasing [18].

Based on the above knowledge, we design an attack system which can generate ultrasound in the same frequencies as automotive sensors, and can craft ultrasound pulses to emulate sensors' working patterns. We then launch jamming and spoofing attacks in observation of sensor reactions and vehicular system reactions.

5.2 Jamming Attack

Jamming attack aims to generate ultrasonic noises and cause continuing vibration of the membrane on the sensor, which make the measurements impossible. Failing to detect obstacles can lead to collisions in parking or maneuvering.

5.2.1 *Inherent Vulnerabilities*

Ultrasonic sensors are known to have weakened performance in two scenarios [18]. On the one hand strong extraneous acoustic emitters in the region of ultrasonic working frequency in the immediate vicinity of a vehicle can lower the signal-to-noise ratio such that measurements are no longer possible. In practice, noise sources are above all compressed air noises (e.g., air brakes in trucks) and metallic grating noises, (e.g., from railed vehicles). On the other hand, any layers of dirt, snow, or ice on the sensor diaphragms can form a sound bridge with the bumper that can prolong the decay behavior of transmission excitation in an undefined manner.

These inherent vulnerabilities indicate the feasibility of performing physical attacks on ultrasonic sensors. To simulate the extraneous noise source, ultrasonic transducers will be a good choice that can exhibit higher sound pressure level and better frequency performance as well as controllability than truck air brakes or metal key chains. On the other hand, specially made sound absorbing masks can be adhered to the surface to prevent transmission, but it is against our threat model by physical alteration and contact.

5.2.2 *Description*

Jamming attack is built on a very straightforward idea — continuously emitting ultrasound at the sensor to lower its Signal to Noise Ratio (SNR), as shown in Figure 5. Our major considerations are listed as follows.

Resonant Frequency. Ultrasonic sensors for parking assistance generally operate on frequencies between 40 kHz and 50 kHz. From our observation on several car models, this frequency appears to be near 50 kHz. Ultrasonic transducers are manufactured with a fixed resonant frequency which is determined by the diameter of the piezoceramics. Within several kHz around the resonant frequency like a bandpass filter, the transducer exhibits the best emittance and sensitivity. Thus it would be best to choose jamming transducers in the same frequency band as of the sensors, which in our case is 50 kHz. Unfortunately 50 kHz transducers were not available on the market, so we used the popular 40 kHz transducers, which turned out to have passable performance.

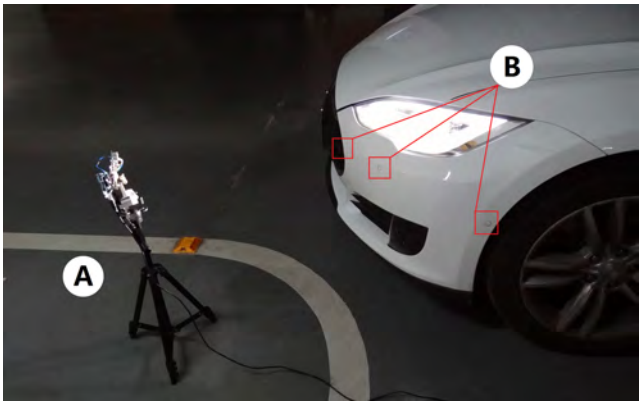


Figure 3: Setup of ultrasound experiment on Tesla Model S. A is the jammer, B is 3 ultrasonic sensors on the left side.

Emitting Ultrasound. Piezoelectric effect describes the generation of acoustic wave by applying alternating voltage. Moreover, the frequency of the AC signal determines the oscillation frequency, and hence the frequency of generated acoustic wave. By applying 40 kHz square wave to the transducer, we are able to generate ultrasound of 40 kHz. This principle works for other frequencies with compatible hardware, as well as for microphones and speakers.

Equipment. To generate controllable square wave of 40 kHz, we find Arduino Uno board [1] competent as a low-cost, off-the-shelf hardware. It can output square wave of specified frequency on the digital I/O pins with a built-in function called `Tone()`, which is mainly used for generating tones on speakers. There is observable frequency jitter at 40 kHz and higher, though the jamming performance does not seem to be affected. To achieve accurate frequencies for phase-sensitive attacks like acoustic cancellation, dedicated hardware is recommended.

Voltage Level. Sound pressure level relies on the voltage level in piezoelectric effect, and vice versa. To acquire farther attack distance, higher voltage has to be applied in order for acceptable sound pressure level at the targeted sensor after airborne attenuation. Arduino outputs at 5 volts, which works well within a very limited range. In some cases, we used a function generator to achieve higher frequency precision and voltage level. One can consider designing his own piece of equipment to fulfil such attacks.

5.2.3 *Results*

We have tested jamming attack on many ultrasonic sensors indoors and outdoors on real cars with parking assistance. We further tested on Tesla Model S's self parking and summon function. All the experiments are carried out with the setup that an obstacle always exists and can be detected by the sensor when no attacks are going.

On Ultrasonic Sensors. We have tested on 8 different ultrasonic sensors/systems in the laboratory. Six of them

(a) Normal. (b) Spoofed. (c) Jammed.

Figure 4: Tesla parking distance display at normal, being spoofed, and being jammed[2].

are individual ultrasonic ranging modules, one of them is an aftermarket vehicular sensor, and the other is an OEM parking assistance system consisting of one ECU unit and four sensors. We have observed two very opposite kinds of sensor output under jamming attacks, one is *ZERO distance*, while the other is *MAXIMUM distance*. Zero distance means the detection of something very close that nearly touches; maximum distance indicates the detection of nothing. We think the opposite results are due to different sensor designs. For the first kind, a fixed threshold is set for the detection of returning echoes. Our jamming signal always exceeds the threshold, and will be falsely recognised as an returning echo as soon as receiving mode is made possible, so the readings under jamming will be zero. Another kind of design implements flexible threshold to eliminate noise. Our jamming signal is recognised as noise because it exists throughout the whole cycle, and hence lowers the SNR. No measurements are possible, so the readings will be maximum consequently.

On Cars with Parking Assistance. Four cars with driver assistance system have been tested. They are popular models from Audi, Volkswagen, Tesla, and Ford. Systems on these cars differ with each other, but they all inform the driver about obstacles by either acoustic or visual distance information. As shown in Figure 3, the ultrasonic jammer is placed in front of the bumper, and can be correctly detected when idle. When jamming attack is launched, the obstacle can no longer be detected by the vehicle, therefore no alarm is given to the driver (Figure 4(c)). This can be considered as the maximum distance case in above sensor test, and the reasons similar. We further tested when the cars are moving in reverse gear, and results are the same. Jammer-sensor distance for effective attack have been measured to be as long as 10 meters for Tesla. Failing to detect obstacles can lead to collisions, the consequence of which could be vital when pedestrians are hit.

On Tesla Model S with Automatic Parking. We further tested on the self parking and summon feature of Tesla Model S. If jamming attack can also cause false negative to automatic parking system, the aftermath will be worse in this case without human supervision. To our surprise, Tesla seems to have switched to another algorithm for handling sensor readings at automatic parking, and it would stop at once as soon as we launched jamming. Neglect of obstacles are only possible when the jammer are aimed at the sensor deliberately, and the jammer-sensor distance is greatly reduced.

[2]This is a strange display of tire pressure. It pops out every time we do ultrasonic jamming, and disappears once we stop. Anyway, NO distance information can be displayed during jamming.

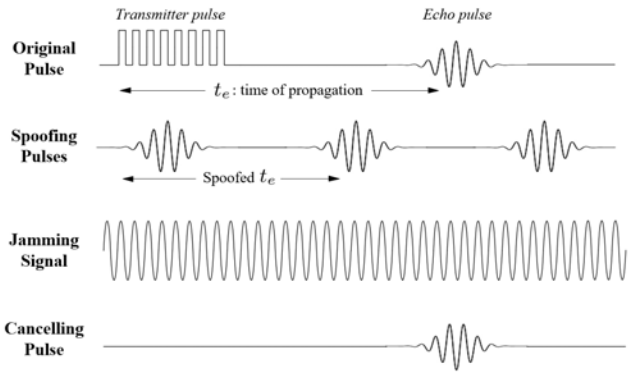


Figure 5: Illustration of all ultrasonic attacks. From up to down are original signal, spoofing signal, jamming signal, and acoustic cancellation signal. The last 3 attack signals overlay with the original signal at the sensor side.

5.3 Spoofing Attack

Spoofing attack shares the same physical channel and hardware with jamming attack, but it is more carefully crafted with the purpose of deceiving the sensors. This attack can lead to disturbance or manipulation of the sensor readings, which will lead to more controllable collisions, or just fool the driver/autonomous car.

5.3.1 Description

Spoofing attack is based on the assumption that if carefully crafted ultrasound pulses from adversaries can be recognized as echoes from obstacles, and arrive at the sensor ahead of the real ones, then the sensor readings will deviate from the real one. By adjusting the timing of carefully crafted pulses, an attacker can manipulate sensor readings, i.e., distance measurement. An illustration is shown in Figure 5.

Setup. The setup is similar to jamming attack, except that the transducer is excited with 50 kHz square wave, which exhibits better performance than 40 kHz.

Pattern. To spoof the sensor, an emulation of its physical pattern (300 μs excitation and 700 μs ring down) is reasonable, though not necessary. An excitation time of 200 – 300 μs normally works well, but we do not recommend more than 1 ms.

Difficulty. Timing is a trick for spoofing attack. Unlike LiDAR, ultrasonic sensors only care about the nearest obstacles. This means only the first justifiable echo will be processed, other echoes in the following will be totally ignored. Thus the counterfeit echo have to be ahead of the real ones in order to be effective, which means the spoofed measurement can only be subtractive. Here we define the *Attack Slot* for spoofing attack, which is the time slot between the end of transmitted pulse and start of first echo. Our injection must reside within the attack slot, the length of which depends on the obstacle distance. Another problem is that the measurements repeat at approximately 100 ms intervals. If the 300 μs counterfeit echo is blindly injected, the probability of hitting the attack slot will be lower than 10% for an obstacle 2 meters away, and will only decrease as the obstacle approaches.

Approach. There is no way an attacker can transmit counterfeit echoes earlier than the real ones by listening to them, so relay attack is impossible for ultrasonic sensors. Another solution is listening and inferring the next cycle by calculating the delays, but neither will it work because the 100 ms cycle time fluctuates due to desired jittering or to asynchronous cycles [18]. Our approach is injecting the echoes with a smaller cycle time of several milliseconds. It may cause unstable spoofed sensor readings, but guarantees successful injection in the attack slot.

5.3.2 Results

As mentioned above, results of spoofing attack depend on the timing of injection, as well as the length of counterfeit echo and cycle time. However, by trial and error we are able to find a set of parameters that can cause interesting sensor outputs, such as abrupt change, steady oscillation between near and far, and jitter around a certain reading, as shown in Figure 4(b). In the vast remaining cases, the sensor readings are just disturbed randomly. When there is no obstacle in the detection range at all, spoofing attack can cause the display of pseudo-obstacles.

5.4 Acoustic Quieting

Besides jamming attack, another way to hide something from the sensors is to eliminate its noise and passive echoes. This approach of *Acoustic Quieting* has been well researched [4][5][14], and well developed for miliary submarines to stay stealth[10][30]. Methods include silent running, hull coatings that reduce active sonar response, and hydrodynamic hull design that reduces noise and active sonar response. We propose two similar methods of acoustic quieting for vehicles.

Cloaking. Sound absorbing materials (e.g., plastic foam) are hardly seen by the ultrasonic parking system. For persons wearing absorbing cloths (e.g., woman with a fur-coat), the system has a shorter detection range. Our initial idea is to cover the obstacle with deadenings like sound absorbing foam. The damping foam can eliminate a portion of the returning echoes, hence reduce the detection range.

Acoustic Cancellation. *Active Noise Control* (ANC), also known as noise cancellation, or Active Noise Reduction (ANR), is a method for reducing unwanted sound by the addition of a second sound specifically designed to cancel the first [6]. Helicopter pilots rely on this technology to speak on the radio; it can also been seen on many high-end headphones. Though originally designed for cancelling low frequency noise, we believe this method can also be applied to cancel ultrasound pulses from vehicular sensors, because the frequency is fixed and patterns are predictable. Note that the cancelling pulse in Figure 5 is in reverse phase. We have done preliminary experiments that proved the feasibility of canceling ultrasound by minor phase and amplitude adjustment. We are not going into details here, but dedicated high-speed hardware is definitely required for vehicular ultrasound cancellation.

6. ATTACKING MMW RADARS

RADAR (Radio Detection and Ranging) originates from the military technology since the Second World War, and has been bound to military applications for a long time. The first vehicle with Radar for adaptive cruise control was made available until 1998. This technology boosted 5 years later due to the development of automatic emergency brake and lane changing assistance. Automotive radars have very different requirements and solutions compared to military applications, such as smaller distance, lower Doppler frequency, high multitarget capability, small size, and significantly lower cost [9][22]. A Medium Range Radar (MRR) is installed under the front bumper on Tesla Model S. It is the underlying sensor support for many of the Autopilot functions, e.g., front collision avoidance and traffic-aware cruise control.

In this section, we will present our security research on the Radar and Autopilot system in Tesla Model S. By using a signal analyzer we were able to identify the frequency band, modulation scheme, and waveform pattern of the Tesla Radar. Then we tried to jam and spoof the radar system with electromagnetic waves in the same frequency band generated by a signal generator. Our results show that automotive MMW Radar can suffer from electromagnetic jamming and spoofing. We will demonstrate the following:

- Jamming attack can make detected objects disappear from the Autopilot system.
- Spoofing attack can alter the object distance.

6.1 System Model

Due to the complexity of Radar system, this paper will not go into the details and mathematics, but rather present an overview of the basic principles of Radar telecommunication technology in layman's terms.

Basic Principle. Similar to ultrasonic sensors, Radar works on the basic principle of emitting and receiving electromagnetic waves, and measure the time-of-flight. However, due to the way faster propagation speed of electromagnetic wave, methods used for ultrasonic sensors are no longer possible. The emitted electromagnetic waves must be given an identifier for recognition and a time reference for the measurement of time-of-flight, the task of which is referred to as modulation. At the receiver side, demodulation is required. The waveform can be described as a harmonic wave function in a general form:

$$u_t(t) = A_t \cdot \cos(2\pi f_0 t + \varphi_0) \tag{2}$$

Modulation is therefore possible with three variables: amplitude A, frequency f, and phase φ. Amplitude modulation is basically pulse modulation, frequency modulation includes *Frequency Shift Keying* (FSK), *Frequency Modulated Shift Keying* (FMSK), *Frequency Modulated Continuous Wave* (FMCW), and *Chirp Sequence Modulation*. In the scope of this paper, frequency modulation and FMCW especially are introduced as it is how our target Radar works.

Frequency Modulation. In frequency modulation, the frequency f_0 is varied as a function of time. Fugure 6 shows the basic structure of FM radar. The instantaneous frequency is varied by a voltage-controlled oscillator (VCO) which enables the desired modulation via a control loop (e.g., phose-locked loop, PLL). The received signal is then mixed[3] with the signal currently being transmitted, filtered, sampled, and converted.

FMCW. Frequency modulated continuous wave is a frequently used modulation for automotive radars. As shown

[3]The process of signal multiplication is described as mixing in high-frequency technology. By mixing it is possible to measure the signal at much lower frequencies.

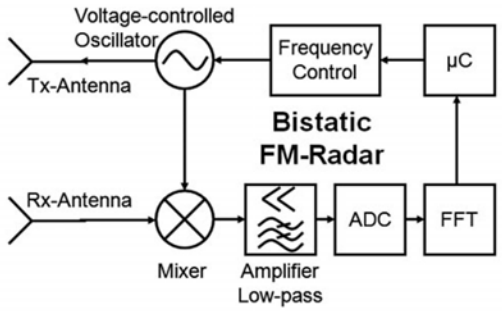


Figure 6: Block diagram of a bistatic Radar with frequency modulation [31].

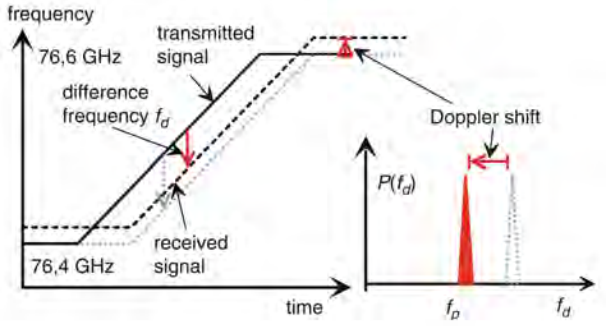


Figure 7: Spectral display of FMCW with a positive ramp for an approaching object [31].

in Figure 7, the instantaneous frequency is continuously changed in the form of a linear ramp. With known slope m_ω, the measurement of time-of-flight can be converted to the measurement of difference frequency f_d, which is easier by signal mixing. The relative speed can be further calculated from the Doppler shift. By means of additional ramps with different slopes m_ω, the ambiguity of linear combination can be resolved for a small number of objects.

Doppler Effect. If an object moves relative to the Radar, the reflected electromagnetic wave will undergo a frequency shift, which is described as Doppler Effect. Accordingly, the frequency shift can be used to measure the relative velocity.

Frequency Bands. There are currently four bands available for use in road traffic ($24.0-24.25$ GHz, $76-77$ GHz, and $77-81$ GHz in addition to a UWB band of $21.65-26.65$ GHz suitable for close range). The 76.5 GHz range, which is exclusive for automotive Radar and available worldwide, dominates at present. The 24 GHZ range has also claimed a large share of the market, especially for medium-range and close-range applications.

Attenuation. Atmospheric attenuation is below 1 dB/km at 76.5 GHz, and therefore only 0.3 dB for the return path to a target 150 m away. However, heavy rain with big raindrops that achieve the magnitude of the wave length (3.9 mm) will result in serious attenuation, and leads to significant range reduction. In addition, heavy rain results in an increased interference level (clutter) and decreases the signal-to-noise ratio (SNR), which will in turn reduce the detection range.

6.2 Signal Analysis

The Radar technology used on Tesla Model S is not publicly known, but certain parameters and patterns of this Radar sensor is necessary for our understanding and crafting attacks. Instead of rearing down the front bumper and looking for the manufacturer and model information (which we could), we turned to a more straightforward and trustworthy way — directly observing the spectrum and waveform. However, seeing them for ourselves cannot be easily done.

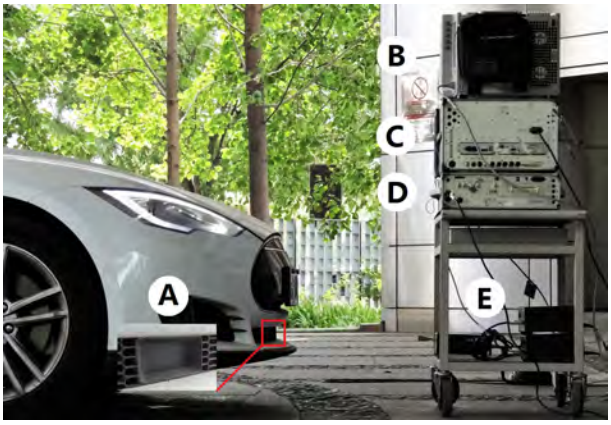


Figure 8: Setup of Radar experiment on Tesla Model S. A is automotive Radar, B is oscilloscope, C is signal analyzer, D is signal generator, E is frequency multiplier, harmonic mixer, and their power supplies.

6.2.1 *Description*

It is said that Bosch 76 – 77 GHz MRR Radar sensor is installed on Tesla. If 76 – 77 GHz band is used indeed, special equipments that can reach this band is the only practical way we can observe its waveform. Normal spectrum analyzers and signal generators can work at high frequencies of several giga Hertz at most. As the maximum frequency increases, they can get very pricy. Even the best signal analyzers and generators (like the ones we used) can only reach 40 – 50 GHz, frequency multipliers and mixers have to be further attached to fulfil this purpose.

Equipments. The following equipments have been employed for signal analysis: Keysight N9040B UXA Signal Analyzer (3 Hz – 50 GHz), DSOS804A High-Definition Oscilloscope, 89601B VSA Software, and VDI 100 GHz harmonic mixer. Mixer acts as the RF frontend and down-converts the 77 GHz signal to a lower frequency that the signal analyzer can process. An oscilloscope is attached to the signal analyzer for better observation in the time domain. VSA software is used for further signal analysis.

Experiment Setup. Figure 8 shows the setup of radar experiment. To achieve higher receiving power for signal analysis, we put the antenna 0.5 m away and on the same horizonal level in line with the automotive Radar.[4] After switching to Drive gear, Radar on the Tesla is powered on, which can be tell from the detection of a car (the equipments in this case) in the middle of the dashboard.

6.2.2 *Results*

From the signal analyzer, the center frequency of Radar

[4]A caution of safety in doing the alignment is NOT to look at the functioning Radar closely and directly in the eyes.

(a) Drive gear. (b) Autopilot. (c) Jammed.

Figure 9: Tesla dashboard display at drive gear, Autopilot, and Autopilot with radar jamming.

signal is confirmed to be around 76.65 GHz, which proves that the automotive Radar on Tesla works within the 76 – 77 GHz band. After some discussion and manual correction, we further determined the bandwidth (ramp height) to be approximately 450 MHz. The modulation is FMCW with slow chirp sequence of 5 ramps, which all seem to correspond to the technical data of Bosch MRR4.

6.3 Jamming Attack

After knowing the waveform parameters, a straightforward idea of attack is jamming the sensor within the same frequency band, i.e., 76 – 77 GHz.

6.3.1 Description

In normal functioning, the signal received must be sufficiently higher than the electrical noise so that detection can take place. Depending on any other signal evaluation for flare suppression, the threshold is above the electrical noise by a factor SNR threshold of approximately 6 – 10 dB [31]. Jamming signal can be considered by the system as strong noise or false input, which will possibly cause lowered SNR or computing errors, and therefore lead to radar system failure.

Jamming Waveform. There are many choices with the jamming waveform. We came up with two approaches, one is fixed frequency at 76.65 GHz, and the other is sweeping frequency within the 450 MHz bandwidth.

Equipments. Keysight N5193A UXG Agile Signal Generator (10 MHz – 40 GHz) and VDI WR10 frequency multiplier (75 – 110 GHz) are used together to generate electromagnetic waves at 77 GHz.

Experiment Setup. The setup is similar to Figure 8, except that the distance between the equipment and car is increased for evaluation.

6.3.2 Results

The results of jamming attack is very prominent. At first a car is detected by the Radar system and shown, when the RF output (jamming) is turned on, the car disappears at once. When it is turned off, the car can be detected again. Moreover, we have found the attack to be more practical when Tesla is in Autopilot mode by increased attack distance and less angle restriction. We assume this is because of threshold changes for tracking objects in Autopilot mode. Results are shown in Figure 9.

6.4 Spoofing Attack

By modulating signals the same way as the automotive Radar, we were hoping for some spoofing results. Due to the low ratio of working time over idle time, signal injection at the precise time slot is very unlikely as we expected. Nevertheless, by tuning ramp slope back and forth in a higher value range on the signal generator, we happened to observe periodic distance change displayed in the Tesla.

6.5 Relay Attack

A more delicate attack would be to relay the received signal at the harmonic mixer to the transmitter, and send back to the Radar to emulate a farther ghost target. Because the relayed signal closely follows the authentic one, it could be accepted with less suspicion, therefore making deception easier. Unfortunately, we only had one horn antenna at the time of experiments and wouldn't be able to do so.

7. ATTACKING CAMERAS

Data from radars, LiDAR, ultrasonic sensors, GPS, and many other sensors are not enough for safe automated driving, especially on highways and city streets where many rules and regulations are applied. For an autonomous car sharing traffic with human drivers, necessary information needs to be acquired visually from road signs and lanes. Onboard camera system handles visual recognition of the surroundings in automated driving technology. Recognition includes lane lines, traffic signs and lights, vehicles, and pedestrians. After fusing data with other sensors, the driving behavior and routes can be better and more safely planned. On Tesla for example, a forward facing camera is used to recognise lanes and road signs. Features based on this technology include automatic lane centering and changing, lane departure warning, and speed limit display.

Cameras are passive light sensors. From our daily experience, they can be blinded or fooled in many ways. To validate the attack on vehicle cameras, we carried out blinding attacks in different scenarios, observed and recorded the camera output. This section will present the experiments on blinding the vehicle camera with lights of different wavelengths generated by off-the-shelf, low-cost light sources. Our major finding is:

- Automotive cameras do not provide enough noise reduction or protection, and thus can be blinded or permanently damaged by strong light, which will further lead to failure of camera-based functionalities.

7.1 System Model

As shown in Figure 10, cameras collect optical data by CCD/CMOS devices through filters, generate images in the camera module, and send them to the MCU for further processing and calculation. The recognition results will be sent to the ADAS ECU from the CAN bus. ADAS processor makes driving decisions and send commands to actuators, e.g., hydraulic steering wheel and control panel. Some systems further provide the driver with video outputs on the screen for reference.

7.2 Blinding Attack

Our attack is based on the assumption that CMOS/CCD sensors can be disturbed by malicious optical inputs, and will produce unrecognizable images. The broken images will further influence the decision of ADAS unit and indirectly affect vehicle control. As a consequence, it will lead to the car's deviation, or an emergency brake, which could all possibly cause crashes.

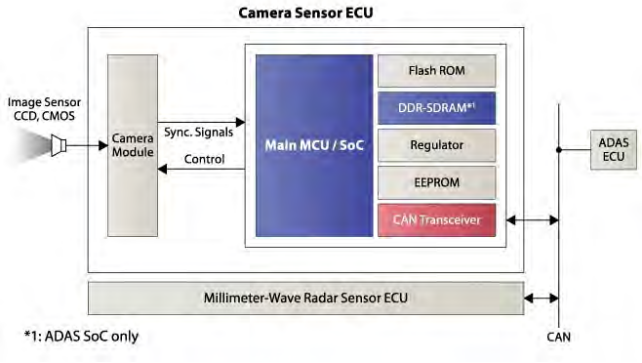


Figure 10: Forward-looking camera system block diagram [20].

7.2.1 *Description*

A common method to attack video equipments is laser blinding. Photoelectric sensors are very sensitive to the intensity of light. With a peak adsorption coefficient at generally 10^3 to 10^5, most of the laser energy at the sensor can be absorbed. The time necessary for damaging photoelectric sensor is one to several orders of magnitude less than the time for harming human eyes. Under laser exposure, the surface temperature will rise rapidly due to the thermal stress caused by non-uniform temperature field. Avalanche breakdown of semiconductor materials can cause irreversible damage to the photoelectric devices. Camera exposure to laser radiation for vehicles running on the road can happen when LiDARs are nearby. LEDs can also be used to generate bright light against cameras. In our experiment, we used three kinds of light sources, i.e., LED, visible laser, and infrared LED.

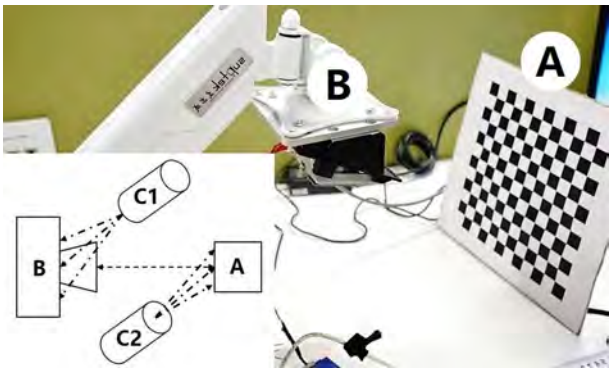
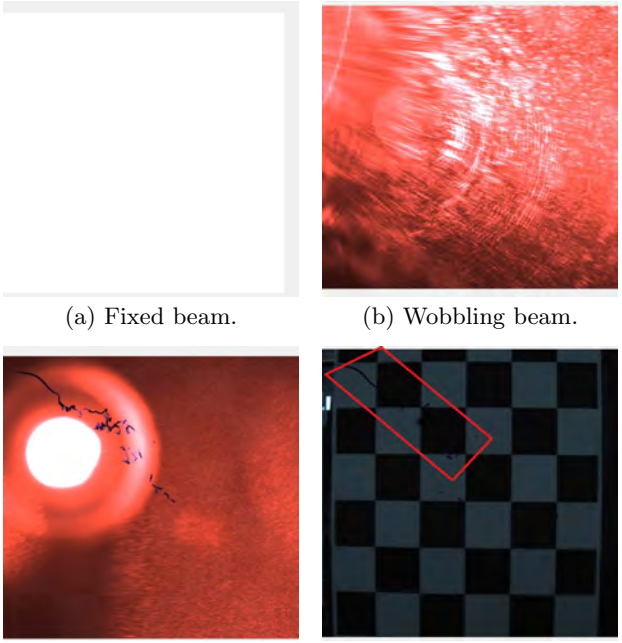


Figure 11: Setup of camera blinding experiment. A is a calibration board, B is a camera, C1 and C2 are laser emitters.

Experiment setup for blinding attack is illustrated in Figure 11. A calibration board A is positioned 1 meter in front of camera B; laser sources are either pointed at the camera or at the calibration board as C1 and C2. C1 is of 15° to the axis of A–B, and C2 of 45°. We have tested with 650nm red laser, 850 nm infrared LED spot, and LED spot of 800 mW power respectively, observed the camera image output, and measured the change of tonal distribution.

(a) Toward board. (b) Toward camera. (c) Tonal distribution.

Figure 12: Blinding camera with LED spot.



(a) Fixed beam. (b) Wobbling beam.

(c) Damage caused by laser. (d) Damage is permanent.

Figure 13: Blinding camera with confronted laser.

7.2.2 *Results*

LED. Aiming LED light at the calibration board leads to increased tonal value in the center area, thus information in this area can be fully concealed, and recognition will no longer be possible. Aiming LED light directly at the camera will induce significantly higher tonal values, and cause complete blindness all over the image. There is no way the camera system can acquire any visual information. The blinding time is relevant to camera refresh rate, as well as the distance between light source and camera. The results are shown in Figure 12.

Laser. Pointing laser beam at the calibration board have almost no effect on the camera. However, pointing directly toward the camera will lead to complete blindness for approximately 3 seconds, during which the recognition will be impossible. We further did another experiment with wobbling laser beam to emulate handhold attacks or unintentional scenarios. As shown in Figure 13(b), it can also cause failure of camera image recognition, though the tonal values are not as high due to shorter exposure time at one spot of CMOS/CCD chip.

Permanent Damage. When laser beam is directly radiated at the camera within 0.5 meter and for a few seconds,

irreversible damage can be caused to the CMOS/CCD chip. The black curve in Figure 13(c) is the evidence. When the laser is turned off, the curve still remains, as in Figure 13(d). Therefore the damage is permanent and irreversible, and can only be fixed by replacing the CMOS/CCD component. Unintentional damage of this kind can possibly be caused by nearby laser radars.

Infrared LED. No effect on the camera has been observed by pointing the infrared LED spot either at the camera or board. We assume it is due to narrow frequency band of filters on the camera, which is a sign of good hardware quality.

8. DISCUSSION

In this section we will discuss the feasibility of our attacks on ultrasonic sensors, MMW Radars, and cameras, from the perspectives of security research and launching real attacks on the road. Based on our experience and limited expertise, we propose countermeasures against these attacks. In the end we conclude the limitations of our work, and calls for new findings in the future.

8.1 Attack Feasibility

We are going to evaluate the feasibility of our attacks by means of influential factors, knowledge threshold, hardware cost, detection by system and driver.

8.1.1 Influential Factors

The attack success rate is affected by many factors including the distance, angle, weather, surroundings, equipment performance, and sensor design after all. We are only going to discuss distance and angle.

Distance. In ultrasonic attacks, jamming is normally kept within 1 meter due to atmospheric attenuation and high jamming noise amplitude required. Spoofing can be done within several meters. The distance can be increased with equipments that generate higher sound pressure and narrower beam pattern. For radar and camera attacks, maximum distance is not measured due to location limitations, which will be discussed later.

Angle. In ultrasonic attacks, best performance is achieved at perpendicular. This is easy to understand because sound is longitudinal wave, and will project most of its energy in the forward direction. However, up to 75° to the sensor perpendicular axis works when spoofing attack aims to create a ghost target. Angle is not tested for camera and Radar attacks.

8.1.2 Knowledge Threshold

To attack a sensor, certain knowledge threshold must be reached, which includes the system model, working principle, relevant physics, and skills to build or operate hardware equipments. Since attack methods on one kind of sensors can hardly be reused when dealing with another kind, learning and researching has to start over, which can be pretty time-consuming. Among the three sensors we studied, ultrasonic is the easiest to approach, and Radar the hardest.

8.1.3 Hardware Cost

For ultrasonic sensors, an Arduino and transducer cost $23, and even cheaper if one makes his own. A laser pointer of a few dollars can cause permanent damage to the camera, no matter it is on or off. However, for MMW Radar, there is no off-the-shelf tools. General equipments like the ones we used cost more than the Tesla Model S.

8.1.4 Detection by System

For all of our attacks described in this paper, no alarm of "malicious attack" or "system failure" from the system is given. Under ultrasonic attacks, the system either displays the spoofed distance, no detection, or no display at all. Interestingly, in [18] it is said that in the presence of ultrasonic noise, "the system responds as *rule* by indicating a fault to the driver or a pseudo-obstacle at a distance that is *less* than potentially real obstacles." Recall that for jamming attack, the distance is falsified to maximum (means no detection), whereas no alarm is given at all. Under radar attack the detected object disappears, but no alarm of radar system error or of any kind is given, and the Autopilot mode is not forced off.

8.1.5 Detection by Driver

Detection of ultrasonic attack and radar attack by the driver is not likely due to the imperceptibility of ultrasound and MMW radio. Camera attack using laser is very likely to be discovered, unless the damage has been done in advance. There are chances that the driver become suspicious to the equipments, therefore it is necessary to carefully hide the equipments or reduce their size.

8.1.6 On Road Attack

We think on road attacks are possible. Ultrasonic jammer can be hidden in a fixed cover or held by hand. Radar equipments can be hidden at the roadside for fixed-spot attack, or in the trunk or in a van for mobile attack, and only leave the tiny antenna outside for concealment. Laser pointer or dazzler can be placed similarly.

8.2 Countermeasures

From the sensor side of view, jamming attacks can be easily recognised, especially for ultrasonic sensors and radars, because there are very few sources of ultrasonic and MMW radio noise in the working environment, especially with high power that can make measurements impossible. Many sensor applications have been implemented with noise rejection, but are not designed with the security concern of malicious jamming, as well as spoofing.

On the systems side that take sensors as input, we suggest using multiple sensor for redundancy check, such as ultrasonic MIMO system. We also suggest adding randomness into control parameters, taking logic check, confidence priority, and attack detection system into consideration when designing sensor data fusion strategy.

8.3 Limitations and Future Work

For ultrasonic sensors, we hope to increase the attack range by developing equipments with better performance, and carry on the ultrasound cancellation system. For MMW Radars, we were not able to test the attack performance in different distances and angles due the limitation of the test yard. We hope to test further in an open field and when the Tesla is moving. For cameras we hope to research more on the feasibility of spoofing attacks.

Besides, for most of the attacks we were only able to observe the results from the vehicle display rather than from sensors themselves, and therefore not sure where the prob-

lems originate, i.e., from the sensors or the ECUs. We hope to further analyze the automated driving system, and monitor all the states for better comprehension of security on the system level.

9. CONCLUSIONS

This paper exhibits that sensor security is an realistic issue to the safety of autonomous vehicles. Three essential kinds of sensors that Automated Driving Systems rely on and have been deployed on Tesla vehicles with Autopilot are studied and examined, i.e., ultrasonic sensors, Millimeter Wave Radars, and cameras. Jamming attacks and spoofing attacks have been launched against these sensors indoors and outdoors, and caused malfunction in the automotive system, all of which could potentially lead to crashes and impair the safety of self-driving cars.

10. ACKNOWLEDGMENTS

We thank Xin Bi and Keysight Open Laboratory & Solution Center in Beijing for their professional support and for providing access to the radar equipments. We thank Xmyth Team for participating in the ultrasonic research.

11. REFERENCES

[1] Arduino. Arduino and Genuino Project. https://www.arduino.cc/. Accessed: 2016-07-05.

[2] L. Bergmann. The ultrasound and its application in science and technology. 1954.

[3] S. Checkoway, D. Mccoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno. Comprehensive Experimental Analyses of Automotive Attack Surfaces. *System*, pages 1–6, 2011.

[4] H. Chen and C. Chan. Acoustic cloaking in three dimensions using acoustic metamaterials. *Applied physics letters*, 91(18):183518, 2007.

[5] S. A. Cummer and D. Schurig. One path to acoustic cloaking. *New Journal of Physics*, 9(3):45, 2007.

[6] S. J. Elliott and P. A. Nelson. Active noise control. *IEEE signal processing magazine*, 10(4):12–35, 1993.

[7] Google. Google Self-Driving Car Project. https://www.google.com/selfdrivingcar/. Accessed: 2016-07-06.

[8] S. Hall. Elon Musk says that the LIDAR Google uses in its self-driving car 'doesn't make sense in a car context'. http://9to5google.com/2015/10/16/. Accessed: 2016-07-06.

[9] J. Hasch, E. Topak, R. Schnabel, T. Zwick, R. Weigel, and C. Waldschmidt. Millimeter-wave technology for automotive radar sensors in the 77 ghz frequency band. *IEEE Transactions on Microwave Theory and Techniques*, 60(3):845–860, 2012.

[10] L. He. Development of submarine acoustic stealth technology. *Ship Science and Technology*, 28(s2):9–17, 2006.

[11] R. Katzwinkel, R. Auer, S. Brosig, M. Rohlfs, V. Schöning, F. Schroven, F. Schwitters, and U. Wuttke. Einparkassistenz. In *Handbuch Fahrerassistenzsysteme*, pages 471–477. Springer, 2012.

[12] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Snach??m, and S. Savage. Experimental security analysis of a modern automobile. *Proceedings - IEEE Symposium on Security and Privacy*, pages 447–462, 2010.

[13] H. Kuttruff. *Ultrasonics: Fundamentals and applications*. Springer Science & Business Media, 2012.

[14] J. Li and J. Pendry. Hiding under the carpet: a new strategy for cloaking. *Physical Review Letters*, 101(20):203901, 2008.

[15] C. Miller and C. Valasek. A Survey of Remote Automotive Attack Surfaces. *Defcon 22*, 2014.

[16] C. Miller and C. Valasek. Remote Exploitation of an Unaltered Passenger Vehicle. *Blackhat USA*, 2015:1–91, 2015.

[17] M. Noll and P. Rapps. Ultraschallsensorik. In *Handbuch Fahrerassistenzsysteme*, pages 110–122. Springer, 2012.

[18] M. Noll and P. Rapps. Ultrasonic sensors for a k44das. In *Handbook of Driver Assistance Systems: Basic Information, Components and Systems for Active Safety and Comfort*, pages 303–323. Springer, 2016.

[19] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl. Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR. *Blackhat.com*, pages 1–13, 2015.

[20] Renesas. Front Detection. https://www.renesas.com/zh-cn/solutions/automotive/adas/front.html. Accessed: 2016-07-07.

[21] M. Seiter, H.-J. Mathony, and P. Knoll. Parking assist. In *Handbook of Intelligent Vehicles*, pages 829–864. Springer, 2012.

[22] M. Skolnik. An introduction and overview of radar. *Radar Handbook*, 3, 2008.

[23] 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 *24th USENIX Security Symposium (USENIX Security 15)*, pages 881–896, 2015.

[24] R. Staszewski and H. Estl. Making cars safer through technology innovation. *White Paper by Texas Instruments Incorporated*, 2013.

[25] S. A. D. Team. Welcome. http://driving.stanford.edu/. Accessed: 2016-07-06.

[26] Tesla. A tragic loss. https://www.teslamotors.com/blog/tragic-loss, June 2016.

[27] Tesla Motors. *Tesla Model S Software Release Notes v7.1*, 2016.

[28] C. Valasek and C. Miller. Adventures in Automotive Networks and Control Units. *Technical White Paper*, page 99, 2013.

[29] J. Waanders. Piezoelectric ceramics-properties and applications. philips components. *Marketing Communications*, 1991.

[30] Wikipedia. Teardrop hull. https://en.wikipedia.org/wiki/Teardrop_hull. Accessed: 2016-07-06.

[31] H. Winner. Automotive radar. In *Handbook of Driver Assistance Systems: Basic Information, Components and Systems for Active Safety and Comfort*, pages 325–403. Springer, 2016.

[32] M. Wolf, A. Weimerskirch, and C. Paar. Security in Automotive Bus Systems. *Proceedings of the Workshop on Embedded Security in Cars*, pages 1–13, 2004.

[33] M. Wolf, A. Weimerskirch, and T. Wollinger. State of the art: Embedding security in vehicles. *Eurasip Journal on Embedded Systems*, 2007, 2007.