Secure FMCW LiDAR Systems with Frequency Encryption

Marziyeh Rezaei
marziyeh@uw.edu
University of Washington
Seattle, WA, USA

Liban Hussein
libanh@uw.edu
University of Washington
Seattle, WA, USA

Sajjad Moazeni
smoazeni@uw.edu
University of Washington
Seattle, WA, USA

Abstract

Robust and secure ranging is among the most vital capabilities demanded by future autonomous vehicles and robotics for precise navigation and avoiding collisions. Light detection and ranging (LiDAR) is a promising 3D imaging technology for this aim. However, the security vulnerabilities of LiDAR systems can impose critical threats to human safety and security, similar to other types of sensors. While LiDARs are becoming a standard technology for self-driving cars, their security aspects have not yet been studied well so far.

In this paper, we will first summarize various security attack scenarios against different LiDAR types. We focus on beam steering and frequency modulated continuous wave (FMCW) LiDAR systems as they have been considered the most secure LiDAR systems proposed so far. We will show that an attacker can reverse engineer the victim's LiDAR system and build a spoofing system using commercially available electro-optical components. To do so, we will develop an electro-optical co-simulation framework in MATLAB Simulink and use that to study the feasibility of the spoofing attack in today's FMCW LiDAR systems. Finally, we propose the frequency encryption technique as a countermeasure to mitigate the possibility of spoofing FMCW beam-steering LiDAR systems. The proposed approach can ensure the security of future FMCW LiDAR systems without compromising functionality or accuracy.

CCS Concepts: • **Security and privacy → Security in hardware**; **Embedded systems security**; **Hardware attacks and countermeasures**.

Keywords: LiDAR, FMCW, beam-steering, spoofing attack, frequency encryption

ASHES '22, June 03–05, 2018, Woodstock, NY

ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/XXXXXXX.XXXXXXX

ACM Reference Format:
Marziyeh Rezaei, Liban Hussein, and Sajjad Moazeni. 2018. Secure FMCW LiDAR Systems with Frequency Encryption. In *Proceedings of Make sure to enter the correct conference title from your rights confirmation emai (ASHES '22).* ACM, New York, NY, USA, 9 pages. https://doi.org/XXXXXXX.XXXXXXX

1 Introduction

Self-driving cars and robots are becoming ever more autonomous with the advent of artificial intelligence (AI). However, their limited sensing and imaging capabilities do not yet satisfy human interaction's reliability and safety standards. One of the significant technologies answering this need is light detection and ranging (LiDAR), which is widely deployed in today's autonomous vehicles. Despite their great success in navigation and preventing accidents, LiDAR systems can be hacked in many ways due to their security vulnerabilities [8, 23, 31]. These vulnerabilities impose threats to both human safety and security. Although these systems are vulnerable to cyber-attacks and can be hacked in the digital processing and software domains [1, 10, 20], real safety threats can occur by jamming or spoofing the LiDAR front-end [23]. In the most malicious scenarios, an attacker sends a spoofing signal to the victim's LiDAR that cannot be differentiated from the actual reflected light, as illustrated in Fig. 1. By doing so, the attacker can overwrite the actual signal since the spoofing signal has less free-space loss than the actual signal. Eventually, the attacker can trick the victim by hiding or misrepresenting its real location.

While LiDAR systems are on the verge of commercialization [2, 3], attack scenarios as described above are unavoidable even in state-of-the-art LiDARs, and prevention techniques have not been yet well studied. In this paper, we study

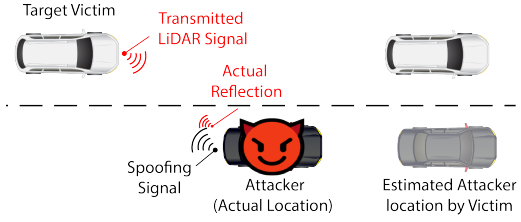

Figure 1. Security risks of today's LiDAR systems for autonomous vehicles (spoofing attack scenario).

and discuss security vulnerabilities of today's LiDARs with a focus on frequency modulated continuous wave (FMCW) beam-steering systems. This type of LiDAR is proved to be the most promising technology as it can operate for long ranges (>150m) with minimal sensitivity to background light and interference [21]. Beam-steering FMCW LiDARs have always been considered both spatially and temporally secure as they perform coherent detection using highly directional optical antennas (or lenses). This is despite the fact that the risks of spoofing in the FMCW ranging systems has been previously investigated and demonstrated for mmWave Radars [16, 17].

In this paper, we study the spoofing vulnerability of beam-steering FMCW LiDARs for the first time. Since currently no such system is commercially available for experimental demonstrations, we have developed a MATLAB Simulink framework for our study. All optoelectronic components are modeled based on realistic parameters of commercial items. Our results show that for a fixed chirp rate, FMCW LiDARs can be hacked. To avoid spoofing in this case, we will propose a new counterattack method based on frequency encryption (FE). This approach does not require any extra laser modules or laser wavelength tunability, unlike frequency hopping schemes that have been proposed for FMCW Radars [15, 17].

The paper is organized as follows. Section 2 summarizes the main categories of today's LiDARs, including the operation principles of beam-steering FMCW LiDARs. Section 3 details the impacts of jamming and spoofing attacks in a LiDAR. We will describe a plausible, realistic spoofing scheme in Section 4, which is verified by a MATLAB Simulink model. In Section 5, a countermeasure against the manipulation will be proposed based on random chirp-rates. The capability and the limitation of the proposed attack and countermeasure will also be discussed. Finally, we conclude the paper and summarize the results in Section 6.

2 LiDAR Systems

LiDAR systems detect an object's distance by transmitting the light and probing the reflected light to estimate the distance by measuring the time-of-flight (ToF). We can classify LiDAR implementations using two key criteria: object illumination methods and modulation/demodulation schemes [11] as described below:

2.1 Object Illumination Methods

Fig. 2 depicts two types of illumination schemes: (a) flash illumination and (b) beam-steering. In flash illumination, the entire field-of-view (FOV) is illuminated at once, and the reflection is spatially resolved using imaging optics followed by a detector array. However, alternatively one can concentrate the laser beam into a single pixel instead of the whole scene, which makes it a point-wise measurement system [11]. In doing so, the beam is scanned through the entire FOV to form a full 3D depth image. This approach is called beam-steering or scanning LiDAR, which achieves a higher signal-to-noise ratio (SNR) suitable for long-range applications at moderate frame rates.

2.2 Modulation/Detection Methods

In direct-detection or pulsed LiDAR systems, the intensity of a laser source is modulated to transmit an optical pulse, and the ToF is directly measured by comparing the intensity patterns of transmitted (Tx) and received (Rx) light in the time domain (i.e., photon arrival times) as shown in Fig 2c. In coherent LiDAR systems, the transmitted light's phase/frequency is modulated while the intensity is held constant. The Rx light is then coherently mixed with a certain portion of the Tx light in the optical domain. Finally, the ToF is inferred from the spectrum of the photo-current at the optical mixer output [11]. FMCW LiDAR is a widely used variant of coherent detection, where the frequency of the laser is linearly modulated, as shown in Fig. 2d. While direct detection is mainly used in today's commercial systems due to their lower complexity, coherent LiDARs are being used for long-range LiDARs as they are less sensitive to ambient light and can achieve higher SNR due to lower bandwidth requirements for the electrical receiver front-end [11].

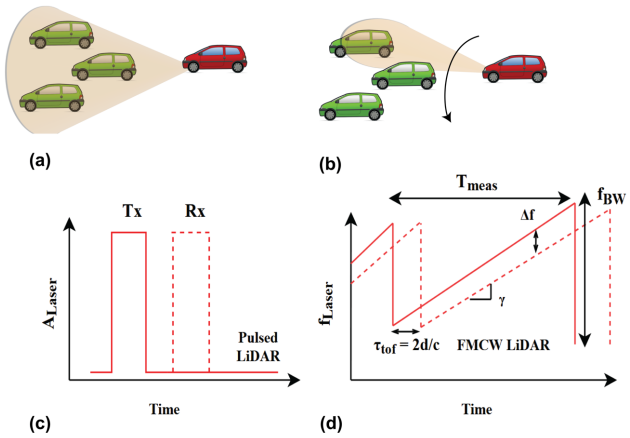

Figure 2. Illumination Methods: (a) Flash illumination, and (b) Beam-steering illumination; Detection Methods: (c) Direct detection/pulsed LiDAR, and (d) FMCW coherent detection.

2.3 Beam-Steering FMCW LiDAR

In this work, we focus on FMCW beam-Steering LiDARs as they are the most promising LiDAR systems demonstrated so far. These LiDAR systems have been considered to be difficult to be hacked for two reasons. First, the attacker can only manipulate a beam-steering victim's LiDAR when the victim's LiDAR is pointing at the attacker. This effect significantly reduces the time window the attacker can exploit to jam or spoof the LiDAR. Second, the attack signal must be highly coherent (i.e., same phase and frequency) with

the victim's laser source to impact an FMCW LiDAR. Any non-coherent signal will be rejected in the optical front-end of the LiDAR. Therefore, these LiDARs can be considered to be "spatially" and "temporally" secure. In Section 4, we will show that a multi-step attack scenario can still be devised to breach these two major security walls and spoof a beam-steering FMCW LiDAR in practice. In order to understand this attack mechanism, we need to first briefly describe system-level requirements and details of FMCW LiDARs.

Standard long-range LiDAR systems should be able to measure distances up to the range of $100m$ to $200m$ with a lateral angular resolution of $\sim 0.1°$-$0.2°$ (about $1milli$ radian) and a ranging precision of $\sim 1cm$ [28]. To meet these requirements, a chirp signal with a bandwidth (f_{BW}) of a few GHz and a measurement time (T_{meas}) of $100\mu s - 1ms$ is required to achieve an acceptable SNR range of $> 10dB$ using $1cm^2$ Rx aperture size. The required frame rate is $20Hz$ which determines the frame length (T_{frame}) of $50ms$.

Range Measurement in an FMCW Beam-Steering LiDAR: An example of FMCW transmitted and reflected signals are shown in Fig. 2d. A popular hardware implementation block diagram is illustrated in Fig. 3. For the range measurement, Tx light (E_{Tx}) is transmitted to the object of interest through the beam scanner, hits the object ,and bounces back to the LiDAR's receiver after the ToF. At the receiver side, the reflected light (E_{Rx}) beats with a portion of the transmitted light (E_{LO}) using an optical coupler and a balanced photodetector (PD). The product is a photocurrent signal (I_{Rx}) that should have ideally a single-tone frequency linearly proportional to the ToF (τ_{ToF}):

$$f_{beat} = \gamma \tau_{ToF} \tag{1}$$

where γ is the chirp rate (f_{BW}/T_{meas}) of the modulated Tx light. Hence, we can determine the ToF by estimating the frequency of I_{Rx} using either fast Fourier transform (FFT) or zero-crossing (ZC) methods [5]. Typically a trans-impedance amplifier (TIA) and an analog-to-digital converter (ADC) is used to amplify and digitize the I_{Rx}, respectively. Eventually, the distance to the target (d) can be measured from $d = c\tau_{ToF}/2$, where c is the speed of light.

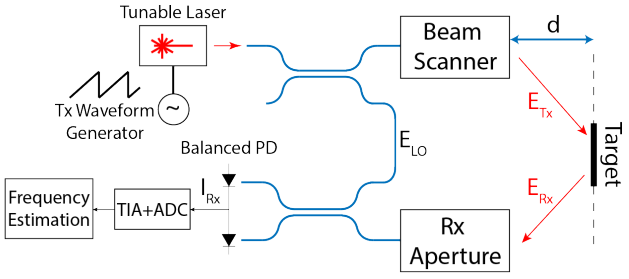

Figure 3. System-level block-diagram of a beam-steering FMCW LiDAR system.

3 Adversarial Attacks on LiDAR Systems

Taking into account the LiDAR system-level requirements detailed before, it can be seen that the most malicious attacks against a LiDAR system can occur at the hardware front-end during measurements [23, 31]. We can generally classify these attacks into two main categories described below:

3.1 Jamming Attacks

Jamming attacks can be referred to as any means of defecting or breaking the LiDAR functionality. A well-known jamming attack scenario is the case in which the attacker transmits an optical beam with a very high optical power to saturate the victim's LiDAR receiver. Direct detection or pulsed LiDARs are highly vulnerable to this type of attack as they rely solely on the optical intensity of the received light for ranging, and a moderately large pulse can surpass the dynamic range of the electrical front-end. However, the impact is less detrimental for FMCW systems since the receiver can only detect the light coherent with its local laser. Hence the only way to jam an FMCW Lidar is to blast a large optical power to damage the front-end PDs.

From the illumination perspective, beam-steering LiDARs are more robust and secure against jamming attacks. This is due to the fact that the attacker's signal will be only detected by the victim's LiDAR over T_{meas} time, while in a flash illumination LiDAR this time will be T_{frame}. This means that to have an equal jamming optical power on a beam-steering LiDAR, the attacker needs more than 50× larger optical power. In practice using narrow-band optical filters can reduce the risk of jamming attacks for all LiDAR types.

3.2 Spoofing Attacks

Spoofing attacks are the most dangerous forms of security breaching since the attacker can trick the victim's LiDAR to miscalculate the actual distance between them or see nonexistent obstacles. These attacks cannot be detected by the sensor unlike most of jamming attacks. Pulsed LiDARs can be easily spoofed by detecting the victim LiDAR's transmitted pulse to trigger a fake spoofing pulse with an additional delay [8]. The possibility of the spoofing in FMCW systems has been also shown for mmWave Radars [13, 16], but here for the first-ever study we argue that an FMCW LiDAR can be also spoofed even under stringent signal considerations discussed in this section.

Fig. 4a shows transmitted (E_{Tx}) and actual reflection (E_{Rx}) signals in an FMCW LiDAR. In order to spoof this system, a signal mimicking the E_{Rx} should arrive with an extra delay (τ_{Att}). This spoofing signal should have precisely the same frequency range (f_{Min} and f_{Max}) and the chirp rate as the victim LiDAR signals to create an additional beat frequency of f_{Sp} in the spectrum of the received signal. If the power of f_{Sp} tone is sufficiently larger than the actual beat signal (f_{beat}), then the frequency estimation block will be tricked

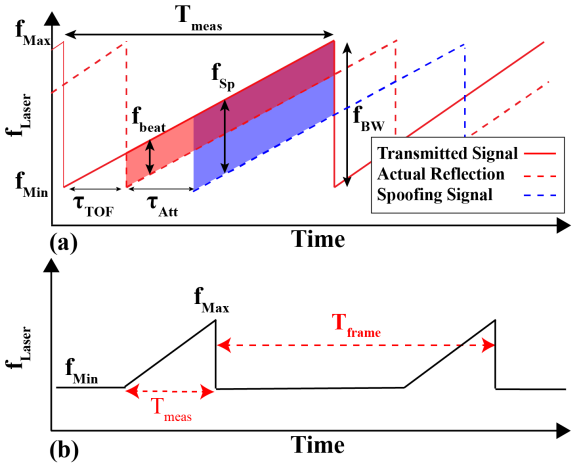

Figure 4. (a) Tx and Rx signals at a victim's LiDAR under the spoofing attack, (b) the E_{Tx} signal detected by the attacker.

and the estimated distance will be:

$$d = \frac{c(\tau_{ToF} + \tau_{Att})}{2} = d_{Act} + d_{Sp} \tag{2}$$

where d_{Act} and d_{Sp} denote the actual and extra spoofing distances, respectively. The τ_{Att} consists of the estimation/preparation time by the attacker plus the actual deliberate spoofing delay (τ_{Sp}). This spoofing attack scenario against a beam-steering FMCW LiDAR can be feasible by considering the following three strict signal requirements:

A. Coherency: The coherent detection method relies on the coherency (i.e., having a precisely exact phase/frequency relationship) between the received light and LiDAR's laser light. In a practical attack scenario, the attacker must generate the spoofing signal from a laser source. This is due to the fact that an all optical approach (effectively "mirroring" the signal) cannot provide sufficient optical power to overwrite the actual reflection signal. Attacker's laser source has to be tuned to be coherent with the victim's laser, otherwise the spoofing signal will not affect the victim's LiDAR.

This requirement leads to a major contrast between spoofing a LiDAR and radar systems. The wavelength of any two laser diode sources even from the same vendor and batch can have more than $\pm 0.5nm$ offset. This corresponds to a $125GHz$ frequency offset range in the C-band ($1550nm$) [19]. This frequency offset for two mmWave radar modules is typically much smaller (sub-GHz range). Therefore, techniques such as replica modules [16] will not be effective for LiDAR spoofing. We will describe in the next section, how the attacker can tune its laser frequency to be able to spoof a victim's LiDAR.

B. Attack Time: Despite the fact that T_{meas} is typically $100\mu s - 1ms$, maximum ToF ($\tau_{ToF,Max}$) is determined by the maximum operating range of the LiDAR. For instance assuming a maximum detection range of $150m$, the $\tau_{ToF,Max}$ is $1\mu s$. Any signal with the arrival time beyond $\tau_{ToF,Max}$ can be easily filtered out at the victim's LiDAR by limiting the bandwidth of the receiver to the maximum f_{beat} (this can be done at the analog front-end). This means $\tau_{ToF} + \tau_{Att}$ should be less than $\tau_{ToF,Max}$ in a successful spoofing attack.

Furthermore, since the beam-steering technique uses a point-wise measurement, victim's LiDAR is only facing the attacker during one signal chirp in each frame. Thus, the actual signal that the attacker sees will be similar to Fig. 4b. This further complicates the attacker's job to spoof the LiDAR.

C. Optical Power: Finally, the power of the spoofing signal should be sufficiently higher than the actual reflection. The attacker has a significant advantage over the victim in terms of optical power if attacker also uses a beam-steering technique. Transmitted light by the victim does not experience a significant loss in the forward path due to its directionality. However, the actual reflected light will be back propagated isotropically after hitting the object. Hence, the free space loss for the victim's LiDAR can be calculated from the following equation [11]:

$$Loss_{Act} = \frac{P_{Rx,Act}}{P_{Tx}} = \frac{A_{Rx}}{\pi d_{Act}^2}\eta \tag{3}$$

where $P_{Rx,Act}$ and P_{Tx} are signal powers of the received light and transmitted light for the victim's LiDAR, respectively. Maximum P_{Tx} is normally limited to $10mW$ due to the human eye safety standards at $1550nm$ [11]. A_{Rx} is the receiver's aperture size and η is the reflection coefficient which counts for effective object reflectivity, absorption, etc. Assuming $A_{Rx} = 1cm^2$, and $\eta = 10\%$, the corresponding loss is around $90.5dB$ for an arbitrary distance (d_{Act}) of $60m$. Since the attacker can also exploit the directional optical antennas (lenses), the spoofing signal loss can be calculated from the following equation:

$$Loss_{Att} = \frac{P_{Rx,Sp}}{P_{Sp}} = \frac{A_{Rx}}{\pi(\tan(\theta/2)d_{Act})^2} \tag{4}$$

where $P_{Rx,Sp}$ is the power of the received spoofing signal by the victim's receiver and P_{Sp} is the power of the transmitted light by the attacker. The denominator is equal to the illumination spot size, where θ is the beam-scanner's angular resolution (beam width) in radian. Assuming θ is $2milli$ radian, the corresponding spoofing signal loss will be only $20.5dB$. Atmospheric losses can be also included in these calculations, but typically they are negligible [11]. Now, if we assume both victim and attacker can access to a similar laser sources ($P_{Sp} = P_{Tx}$), the spoofing signal can be up to $\sim 70dB$ larger than the actual reflection at the victim's LiDAR.

4 Spoofing Attack Scheme on a Beam-Steering FMCW LiDAR

In this section, we propose a detailed spoofing attack procedure against a beam-steering FMCW LiDAR system which can satisfy all three signal requirements described in the

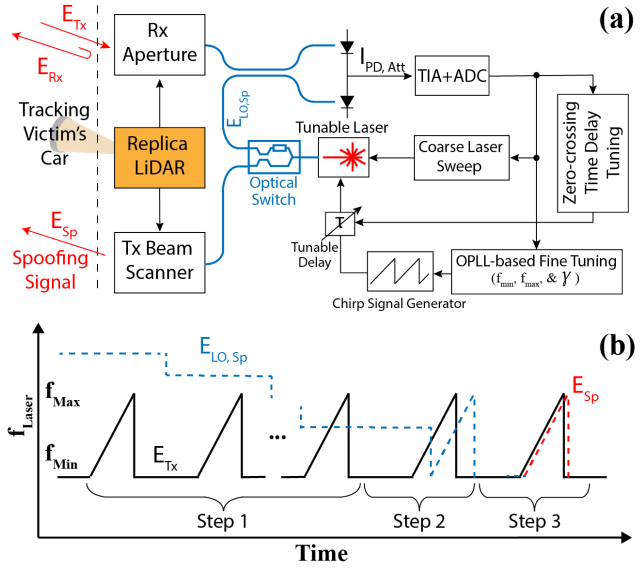

Figure 5. Attacker's system block-diagram (a) and the timing-diagram of FMCW signals (b) for spoofing.

previous section. The practical spoofing attack system block-diagram is illustrated in Fig. 5a. In principle, the attacker can have a replica LiDAR that can be used to track the victim's location and lock its receive and transmit optics front-end (Tx and Rx beam scanners) to the target. Notice that this replica LiDAR cannot be directly used to generate the spoofing signal as explained before (unlike a radar system [16]). Hence, the attacker has to use a coherent detection to measure the frequency offset (beat frequency) between the victim's signal (E_{Tx}) and its own laser ($E_{LO,Sp}$). Using the resultant photocurrent ($I_{PD,Att}$), the spoofing attack can happen in the following three steps as shown in Fig. 5b:

4.1 Step 1: Coarse Wavelength Tuning

The first step is wavelength (frequency) coarse tuning to minimize the frequency offset between the attacker's and victim's lasers such that the frequency difference can be measured by a PD in Step 2. This step is necessary since the initial offset between two lasers can be much larger than a high-speed PD bandwidth which is about $40GHz$ [12]. To do so, the attacker needs to have a tunable wavelength laser to sweep the wavelength across the entire offset range. This can be done using a Distributed Bragg Reflector (DBR) laser and tuning the laser cavity mirror current [4, 29] or a Distributed Feedback (DFB) laser using thermal tuning [25]. Once the frequency offset is within the PD bandwidth, the electrical front-end can detect the photocurrent ($I_{PD,Att}$) in Fig 5. This process can be done using a simple detect threshold current for the $I_{PD,Att}$. Since coarse wavelength tuning can be a slow process (typically kHz range [24]), this process can take place over multiple frame cycles. For instance, if PD bandwidth is $40GHz$ and maximum wavelength offset range is $\pm 0.5nm$ (this can be estimated with extra margin from the brand/type of victim's LiDAR laser), coarse tuning requires $125GHz/40GHz \approx 3$ steps which needs about $0.15s$ at $20fps$.

4.2 Step 2: Fine Frequency Tuning & Chirp rate Estimation

After performing the first step, detected $I_{PD,Att}$ can be used to finely tune the attacker's laser parameters (including f_{Max}, f_{Min}, and γ). In order to precisely track and lock two laser sources, the attacker can utilize a custom optical phase-locked loop (OPLL) [22]. Fig. 6a shows the block-diagram of such an OPLL, where the victim's laser is used as the reference signal, and the attacker's laser is modeled as a tunable current-controlled oscillator and the balanced PD current ($I_{PD,Att}$) is used to measure the optical phase difference. Laser control current can be injected in the phase section of a DBR laser to have large modulation bandwidth [30]. This current is provided by a laser driver that converts the control voltage to the current suitable for driving the laser. Similar to a conventional PLL, an OPLL has a loop filter that controls the stability and bandwidth of the loop.

We have modeled and simulated the OPLL in MATLAB Simulink using linear s-domain models as shown in Fig. 6b. All electro-optical components are modeled using realistic parameters reported in [27]. The laser is modeled with a center frequency of f_0 and a full width half max (FWHM) of h_0 to model the phase-noise. The laser modulation bandwidth shows the frequency dependency that directly affects the loop bandwidth and can be modeled by a low pass filter with a pole at (w_f), and K_f represents the laser current to frequency conversion gain. We have used a 2nd-order loop filter to stabilize the OPLL. The inherent loop delay due to the optical components and routing is denoted by τ_{Loop}, which is a limiting factor for loop bandwidth [27]. All the parameters used in our simulation setup including FMCW signal metrics and OPLL parameters are listed in Table 1 and Table 2, respectively. We have intentionally picked a large f_{BW} to study the OPLL locking mechanism for large chirp rates.

f_{BW}	T_{meas}	T_{frame}	Ranging Resolution
$10GHz$	$100\mu s$	$50ms$	$2.67cm$

Table 1. FMCW beam-steering LiDAR system requirements

K_f	w_f	f_0	h_0	w_{PD}	τ_{Loop}
$10GHz/mA$	$10MHz$	$5GHz$	$50kHz$	$40GHz$	$10ns$

Table 2. OPLL Simulink model parameters

Fig. 6c shows the phase error from the OPLL simulation results, and it can be seen that the locking time (τ_{Lock}) is $\sim 1.4\mu s$. Notice that this lock time is much larger than the available attack time of $\tau_{ToF,Max} \approx 1\mu s$ (see Section 3.2). So, although attacker's laser can precisely mimic the victim's LiDAR signal (have the same frequency and chirp rate) after

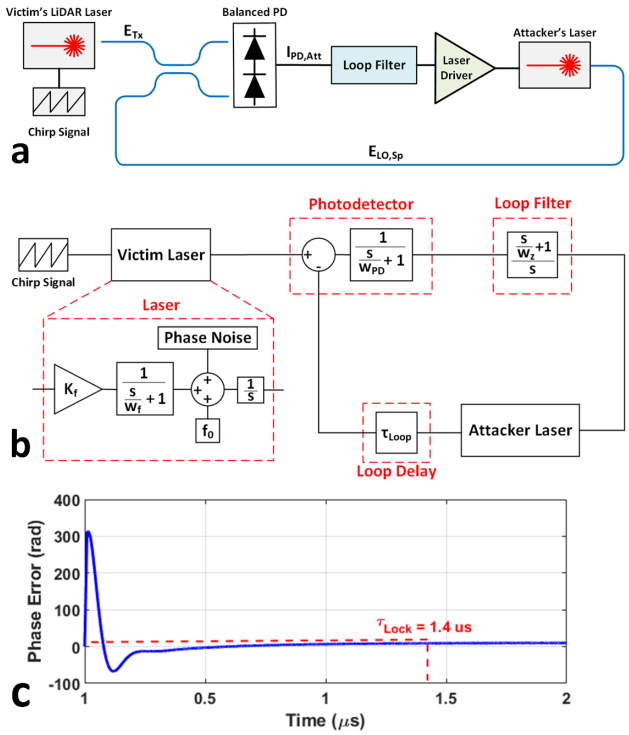

Figure 6. (a) OPLL's block-diagram, b) linearized s-domain model in Simulink, c) locking time results.

the lock time, the attacker cannot initiate the spoofing attack due to the relatively large locking time. However, the OPLL settings (f_{Max}, f_{Min}, and γ) can be stored [14] and reloaded in the next frame cycle to transmit a spoofing signal.

We note that the locking time is inversely proportional to the loop bandwidth, so a larger loop bandwidth is expected to reduce the locking time. While higher order loop filters can increase the loop bandwidth in electrical PLLs [9], the maximum theoretical loop bandwidth is already achieved in our simulations using a 2nd-order loop filter. This loop bandwidth is limited by the total optical loop delay (τ_{loop}) due to the waveguide/fiber connections between the optical elements [7].

4.3 Step 3: Time Delay Estimation

At this stage, the attacker can use the precisely locked laser to spoof the victim. However, the timing delay between the victim and attacker's laser chirp signals can be arbitrary after Step 2. This is because the OPLL stops working and the delay between attacker's and victim's internal chirp signals can be affected by the distance variations and laser's frequency drifts. So the attacker needs to estimate this time delay within a fraction of the available attack time ($\tau_{ToF,Max}$), adjusts the chirp signal timing, and then transmits the spoofing signal by adding a τ_{Sp} intentional delay. Since the attacker knows the chirp rate in this step, the time delay can be estimated from $\tau_{delay} = f_{beat,Att}/\gamma$, where $f_{beat,Att}$ is the beat frequency calculated from $I_{PD,Att}$. Therefore, a fast frequency estimation method is required to estimate $f_{beat,Att}$. Here we assume the attacker will use a zero crossing algorithm instead of a conventional FFT, since it requires fewer calculations and it is suitable for low-complexity and fast frequency estimation [5].

To estimate the crossing times in ZC, the beat signal will be integrated over a t_{intg} period, and then two sample points, before and after the crossing, are selected as a basis for estimating the location of the crossing [5]. Finally, the frequency of the beat signal is estimated by averaging the differences between two successive zero-crosses using the equations presented in [5]. For a two crossing point ZC ($L = 2$ in [5]), the latency of computations includes 5 summations/subtractions and 5 divisions, which will only takes about a few *ns*-range latency in a typical CMOS process even at high bit precision like FP16/32 [6, 18]. Thus, the delay estimation time is mainly determined by the t_{intg}, which should be in the range of $\sim 100ns$ to have enough margin for successfully spoofing the victim's LiDAR independent of the d_{Act} and d_{Sp}. We note that the time delay calculated above is the summation of the actual delay between the attacker's and victim's chirp signals, and a $\tau_{ToF}/2$ due to the actual distance between the victim and the attacker. However, the later term can be estimated and subtracted using the replica LiDAR on the attacker side with a precision of the original LiDAR. Once the τ_{delay} is estimated, attacker can tune the delay of its chirp signal and redirect the laser's output light from the internal locking loop into the beam-scanner (via an optical switch) to transmit the spoofing signal. The delay of the optical switch can be ignored as it can operate at $+10GHz$ switching speeds.

4.4 Spoofing Attack Simulation Results

Since beam-steering FMCW LiDARs are not yet commercially available, we validate the practicality and feasibility of the described spoofing scenario using a MATLAB Simulink framework. We have modeled a full beam-steering FMCW LiDAR system as the victim, and one attacker system as shown in Fig. 5a. In this framework, we assumed the actual distance between the victim and the attacker (target) is $60m$ ($\tau_{ToF} = 400ns$). For the last step of the spoofing attack, t_{intg} and τ_{sp} are both assumed to be $100ns$. In doing so, the attacker intends to spoof the victim's LiDAR by pretending to be at a $90m$ distance from the victim. Maximum transmitted laser power (for both victim and attacker) is set to $10mW$. As previously discussed, the actual reflection and spoofing signal see a propagation loss of $90.5dB$ and $20.5dB$, respectively. Attacker's transmitted power is adjusted such that received spoofing signal power by the victim will be in the same range as the actual reflection (below $1nW$) to avoid saturating the victim's LiDAR receiver.

Fig. 7 shows the power spectral density (PSD) of the received photo current (I_{Rx}) at the victim's LiDAR in three

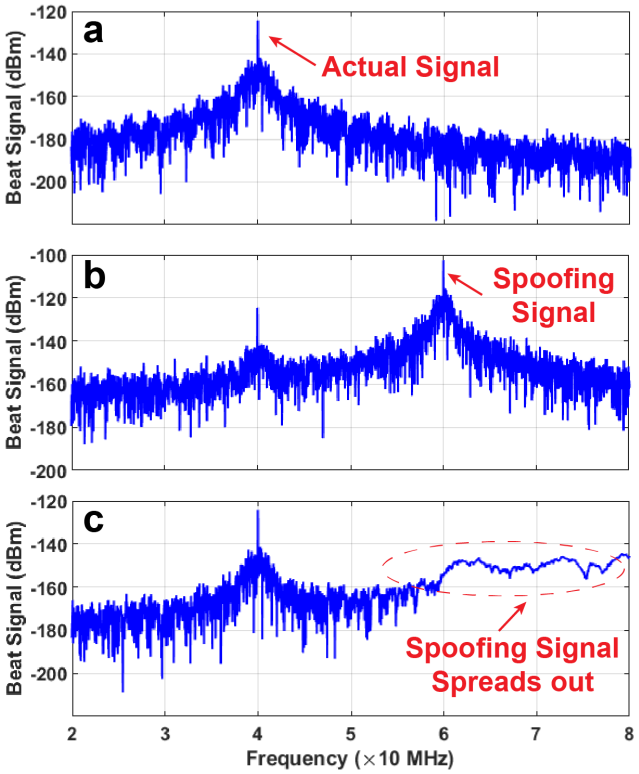

Figure 7. Power spectral density of the beat signal photocurrent at the victim's LiDAR (I_{RX}): (a) without the presence of any spoofing signal, (b) in presence of the spoofing signal with matching chirp rate, (c) in presence of the spoofing signal with a different chirp rate ($\Delta\gamma/\gamma$ = %20)

different scenarios. When there is no attacker, the PSD indicates a single tone at $40MHz$ with $-124dBm$ power (Fig. 7a). In the presence of the attacker, the second tone (spoofing signal) shows up at $60MHz$ with $19dB$ higher power than the actual reflection (Fig. 7b). Hence, the attacker's location will be estimated to be $90m$ instead of $60m$ by the victim. Fig. 7c shows the results with proposed counterattack approach discussed in Section 5.

4.5 Spoofing Attack Precision

In this section, we estimate the accuracy of the proposed spoofing attack mechanism. Assuming that there is a negligible error in fine frequency tuning steps (Step 2), the spoofing attack precision is mainly determined by the time delay estimation accuracy in Step 3. As mentioned in Section 4.3, this delay is calculated based on the time interval between successive crossings using ZC algorithm during the t_{intg} period. If the time interval between two successive zeros is larger than t_{intg}, no crossing can be detected, and the time delay is estimated to be $2t_{intg}$ ($f_{beat} = 1/2\gamma t_{intg}$). Thus, the spoofing distance precision ($\sigma_{d_{Sp}}$) in this case can be calculated from: $\sigma_{d_{Sp}} = ct_{intg}$. However, if the ZC algorithm detects sufficient crossings (at least two) and resolves the delay time,

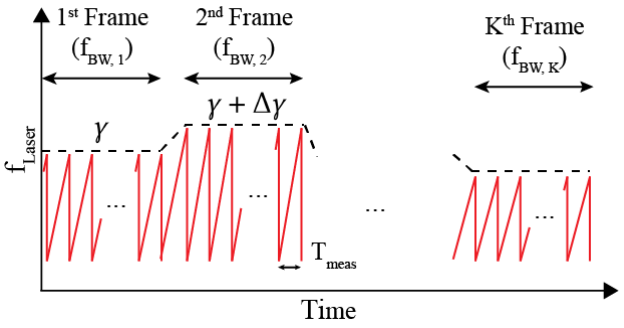

Figure 8. Proposed FE-FMCW approach based on randomly varying chirp rates for each frame ($f_{BW,i}$ is the modulation bandwidth during the i-th frame).

then the ranging precision can be calculated from a theoretical FMCW ranging precision equation [11]. Hence, overall spoofing attack accuracy can be determined from:

$$\sigma_{d_{Sp}} = \max\left(\frac{0.89c}{\gamma t_{intg}}, ct_{intg}\right) \quad (5)$$

Assuming $\gamma = 0.1GHz/\mu s$ and $t_{intg} = 100ns$ in this work, the spoofing ranging precision will be determined from Eq. 5 to be 26.7m.

5 Frequency Encrypted FMCW (FE-FMCW)

We are proposing a novel FMCW technique based on frequency encryption as a counterattack method to avoid the possibility of the spoofing attack described in Section 4. In this approach, the LiDAR uses a randomly generated chirp rate during each ranging frame, as shown in Fig. 8. This can be done by randomly changing the modulation bandwidth for each frame to maintain a fixed frame rate and measurement time.

The spoofing attack scheme described previously will be unsuccessful for the proposed LiDAR since the estimated chirp rate in Step 2 will not be the same as the chirp rate during the attack step (Step 3). This effect has been verified in our simulation results in Fig. 7c, where we assumed the chirp rate has been changed by 20% between two frames ($\Delta\gamma/\gamma$ = 20%). Therefore, the spoofing frequency tone cannot occur and the spoofing signal power is spread across a higher (or lower) frequency span. We will discuss the trade-offs around using a random chirp rate and how much randomness is necessary later in this section.

From the hardware implementation perspective, FE-FMCW can be realized by simply changing the chip-rate in each frame using a random key generator. This can be done using a physically unclonable function (PUF) block to exploit inherent hardware process and mismatch variations to generate a unique chirp-rate sequence code for each LiDAR unit. Note that this random key will be only used to generate FMCW chirp signals (e.g., via an OPLL [7]). Therefore, the key does not need to be communicated to the digital

back-end of the system. This improves the security of LiDAR systems from potential cyber-attacks in both the digital and software domains. Finally, while the chance of interference between multiple beam-steering FMCW LiDAR systems is low in practice, FE-FMCW method can also further mitigate the interference effects.

Related Work: Different approaches have been previously proposed to mitigate spoofing and interference effects in FMCW ranging systems. While all previous works only focused on FMCW Radar systems, proposed methods can be potentially adopted to secure LiDAR systems. However, each method imposes critical limitations compared with our approach due to major differences between mmWave and optical FMCW systems.

The work of [15] introduced an FMCW Radar mechanism based on a random chirp signal. In this work, each pulse is divided into N smaller chirps, while their starting frequencies (f_{Min}) randomly switch. This method sacrifices resolution in favor of hopping the frequency. Another similar work based on random frequency hopping is proposed in [17]. This method suffers from phase discontinuity that affects SNR and precision. Overall, adopting these approaches for a LiDAR system requires a widely and continuously tunable DBR laser to provide a higher tuning range compared with the proposed method. Phase-coded FMCW (PC-FMCW) scheme has been also proposed in [26]. However, this method also suffers from phase discontinuity, and it relies on the amplitude detection which requires unachievable SNR levels in a LiDAR.

Effects of Randomly Changing Chirp Rates: Our proposed design prevents the spoofing attack by randomly changing the chirp rate in each frame. The minimum required $\Delta\gamma$ imposes trade-offs on the SNR, ranging precision and modulation bandwidth. The $\Delta\gamma$ should be sufficiently large enough so that the spoofing signal tone does not show up (similar to Fig. 7). All the γ values should be large enough to provide enough ranging precision ($f_{BW,i} >\sim 1GHz$), while maximum of $f_{BW,i}$ will be limited by the laser modulation range. We can find the minimum required $\Delta\gamma$ to avoid the spoofing attack by measuring the signal to interference and noise ratio (SINR) metric. The SINR is defined using the following equation:

$$SINR = \frac{A_{Rx}^2(T_{meas}/2)}{I+N} \tag{6}$$

where $A_{Rx}^2(T_{meas}/2)$ is the power of the actual reflection signal, I is the attacker (interference) power, and N is a noise power due to the shot noise and laser phase noise. Fig. 9 shows the SINR vs. different chirp rate randomness ($\Delta\gamma/\gamma$) values. This figure shows that as we increase the chirp rate randomness, SINR improves and spoofing signal spreads out more, and SINR asymptotically approaches the ideal (no attacker scenario) SNR value (31.4dB in this paper). This plot also shows that in order to perform FE-FMCW at low $\Delta\gamma/\gamma$, the SINR will be lower in presence of the attacker, and this degrades the ranging precision based on the Cramér-Rao lower bound (CRLB) estimation:

$$CRLB_d = \frac{c}{4\pi f_{BW}}\sqrt{\frac{3}{SNR}} \tag{7}$$

However, we can recover the ranging precision by moderately increasing the modulation bandwidth. For instance, the FE-FMCW approach with $\Delta\gamma/\gamma$ of 60% can achieve the same ranging precision (under spoofing attack) as the ideal FMCW accuracy (under no attack), if we increase f_{BW} by 3.2 times to compensate for the $\sim 10dB$ lower SINR (see Fig. 9).

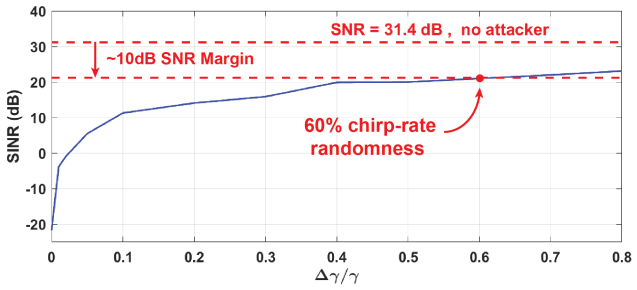

Figure 9. Simulated SINR for different chirp rate randomness values in the proposed FE-FMCW method.

6 Conclusions

In this paper, we have studied the feasibility of the spoofing attacks on beam-steering FMCW LiDARs. For the first time we considered and discussed the effects of beam-steering and optical coherent detection in LiDAR security. Based on our MATLAB Simulink modeling, a realistic spoofing attack system can be implemented using state-of-the-art commercial electro-optics and a custom designed OPLL. A novel counter-attack approach based on frequency encryption and random chirp rates has been proposed and verified. Our approach does not require any major new components (e.g., widely tunable laser, etc.), and it can maintain the ranging accuracy even under the spoofing attack. This approach can be a key to secure the future LiDAR systems for autonomous vehicle, drones, and robotics.

Acknowledgments

This work is supported by the National Science Foundation (NSF) under Grant No. ECCS-2028406.

References

[1] 2017. Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges. *IEEE Transactions on Intelligent Transportation Systems* 18, 11 (2017), 2898–2915. https://doi.org/10.1109/TITS.2017.2665968

[2] 2022. LiDAR firms burn through cash in race to commercialization. https://optics.org/news/13/3/4.

[3] 2022. SiLC Technologies Rolls Out First Commercially Available Chip-Integrated FMCW LiDAR Sensor. https://www.businesswire.com/news/home/20211207005306/en/SiLC-Technologies-Rolls-Out-First-Commercially-Available-Chip-Integrated-FMCW-LiDAR-Sensor.

[4] Y.A. Akulova, G.A. Fish, Ping-Chiek Koh, C.L. Schow, P. Kozodoy, A.P. Dahl, S. Nakagawa, M.C. Larson, M.P. Mack, T.A. Strand, C.W. Coldren, E. Hegblom, S.K. Penniman, T. Wipiejewski, and L.A. Coldren. 2002. Widely tunable electroabsorption-modulated sampled-grating DBR laser transmitter. *IEEE Journal of Selected Topics in Quantum Electronics* 8, 6 (2002), 1349–1357. https://doi.org/10.1109/JSTQE.2002.806677

[5] Belal Al-Qudsi, Mohammed El-Shennawy, Niko Joram, and Frank Ellinger. 2017. Enhanced zero crossing frequency estimation for FMCW radar systems. In *2017 13th Conference on Ph.D. Research in Microelectronics and Electronics (PRIME)*. 53–56. https://doi.org/10.1109/PRIME.2017.7974105

[6] Milad Bahadori, Mehdi Kamal, Ali Afzali-Kusha, and Massoud Pedram. 2016. A comparative study on performance and reliability of 32-bit binary adders. *Integration* 53 (2016), 54–67.

[7] Behnam Behroozpour, Phillip A.M. Sandborn, Ming C. Wu, and Bernhard E. Boser. 2017. Lidar System Architectures and Circuits. *IEEE Communications Magazine* 55, 10 (2017), 135–142. https://doi.org/10.1109/MCOM.2017.1700030

[8] Yulong Cao, Yimeng Zhou, Qi Alfred Chen, Chaowei Xiao, Won Park, Kevin Fu, Benjamin Cyr, Sara Rampazzi, and Z. Morley Mao. 2019. Adversarial sensor attack on LiDAR-based perception in autonomous driving. In *Proceedings of the ACM Conference on Computer and Communications Security*. 2267–2281. https://doi.org/10.1145/3319535.3339815 arXiv:1907.06826

[9] Alfonso Carlosena and Antonio Manuel-Lazaro. 2007. Design of High-Order Phase-Lock Loops. *IEEE Transactions on Circuits and Systems II: Express Briefs* 54, 1 (2007), 9–13. https://doi.org/10.1109/TCSII.2006.883205

[10] Sasan Jafarnejad, Lara Codeca, Walter Bronzi, Raphael Frank, and Thomas Engel. 2015. A car hacking experiment: When connectivity meets vulnerability. In *2015 IEEE Globecom Workshops, GC Wkshps 2015 - Proceedings*. https://doi.org/10.1109/GLOCOMW.2015.7413993

[11] Taehwan Kim. 2019. *Realization of integrated coherent LiDAR*. Ph. D. Dissertation. UC Berkeley.

[12] S. Klinger, W. Vogel, M. Berroth, Mathias Kaschel, Michael Oehme, and Erich Kasper. 2008. Ge on Si p-i-n Photodetectors with 40 GHz bandwidth. *2008 5th International Conference on Group IV Photonics, GFP*, 188 – 190. https://doi.org/10.1109/GROUP4.2008.4638140

[13] Rony Komissarov and Avishai Wool. 2021. Spoofing Attacks Against Vehicular FMCW Radar. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3474376.3487283

[14] Jri Lee and Mingchung Liu. 2008. A 20-Gb/s Burst-Mode Clock and Data Recovery Circuit Using Injection-Locking Technique. *IEEE Journal of Solid-State Circuits* 43, 3 (2008), 619–630. https://doi.org/10.1109/JSSC.2007.916598

[15] Jiafang Liu, Yunhua Zhang, and Xiao Dong. 2018. High Resolution Moving Train Imaging Using Linear-FM Random Radar Waveform. In *2018 Asia-Pacific Microwave Conference (APMC)*. 839–841. https://doi.org/10.23919/APMC.2018.8617646

[16] Noriyuki Miura, Tatsuya Machida, Kohei Matsuda, Makoto Nagata, Shoei Nashimoto, and Daisuke Suzuki. 2019. A Low-Cost Replica-Based Distance-Spoofing Attack on MmWave FMCW Radar. In *Proceedings of the 3rd ACM Workshop on Attacks and Solutions in Hardware Security Workshop* (London, United Kingdom) *(ASHES'19)*. Association for Computing Machinery, New York, NY, USA, 95–100. https://doi.org/10.1145/3338508.3359567

[17] Thomas Moon, Jounsup Park, and Seungmo Kim. 2022. BlueFMCW: random frequency hopping radar for mitigation of interference and spoofing. *EURASIP Journal on Advances in Signal Processing* 2022, 1 (2022), 4. https://doi.org/10.1186/s13634-022-00838-7

[18] Hooman Nikmehr. 2005. *Architectures for floating-point division*. Ph. D. Dissertation.

[19] Rajiv Ramaswami, Kumar Sivarajan, and Galen Sasaki. 2009. *Optical networks: a practical perspective*. Morgan Kaufmann.

[20] Tim Ring. 2015. Connected cars - The next target for hackers. *Network Security* 2015, 11 (2015), 11–16. https://doi.org/10.1016/S1353-4858(15)30100-8

[21] Christopher Rogers, Alexander Y Piggott, David J Thomson, Robert F Wiser, Ion E Opris, Steven A Fortune, Andrew J Compston, Alexander Gondarenko, Fanfan Meng, Xia Chen, Graham T Reed, and Remus Nicolaescu. 2021. A universal 3D imaging sensor on a silicon photonics platform. *Nature* 590, 7845 (2021), 256–261. https://doi.org/10.1038/s41586-021-03259-y

[22] Naresh Satyan. 2011. *Optoelectronic control of the phase and frequency of semiconductor lasers*. California Institute of Technology.

[23] Hocheol Shin, Dohyun Kim, Yujin Kwon, and Yongdae Kim. 2017. Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Vol. 10529 LNCS. 445–467. https://doi.org/10.1007/978-3-319-66787-4_22

[24] J.E. Simsarian and Liming Zhang. 2004. Wavelength locking a fast-switching tunable laser. *IEEE Photonics Technology Letters* 16, 7 (2004), 1745–1747. https://doi.org/10.1109/LPT.2004.828842

[25] S. Sogaard and J. Henningsen. 2002. Thermal tuning and modulation of a DFB fibre laser with a thin-film heater. *Applied Physics B* 75 (10 2002), 497–501. https://doi.org/10.1007/s00340-002-1002-9

[26] Faruk Uysal. 2020. Phase-Coded FMCW Automotive Radar: System Design and Interference Mitigation. *IEEE Transactions on Vehicular Technology* 69, 1 (2020), 270–281. https://doi.org/10.1109/TVT.2019.2953305

[27] Jacques Van Damme, Bart copromotor (viaf)112158124942814930053 Kuyken, and Guy promotor Torfs. 2019. Design of an Optical Phase Locked Loop. http://lib.ugent.be/catalog/rug01:002786316

[28] Mial E Warren. 2019. Automotive LIDAR Technology. In *2019 Symposium on VLSI Circuits*. C254–C255. https://doi.org/10.23919/VLSIC.2019.8777993

[29] Lintao Zhang and J.C. Cartledge. 1995. Fast wavelength switching of three-section DBR lasers. *IEEE Journal of Quantum Electronics* 31, 1 (1995), 75–81. https://doi.org/10.1109/3.341710

[30] Yaping Zhang. 2020. DBR Tunable Lasers with 10 Gbps RF Direct Modulation. In *2020 22nd International Conference on Transparent Optical Networks (ICTON)*. IEEE, 1–4.

[31] Yang Zhang, Hassan Foroosh, Philip David, and Boqing Gong. 2019. Camou: Learning a vehicle camouflage for physical adversarial attack on object detectors in the wild. In *7th International Conference on Learning Representations, ICLR 2019*.