A Low-Cost Replica-Based Distance-Spoofing Attack on mmWave FMCW Radar

Noriyuki Miura, Tatsuya Machida, Kohei Matsuda, Makoto Nagata
Kobe University
Kobe Hyogo Japan
miura@cs.kobe-u.ac.jp

Shoei Nashimoto, Daisuke Suzuki
Mitsubishi Electric Corporation
Kamakura Kanagawa Japan
suzuki.daisuke@bx.mitsubishielectric.co.jp

ABSTRACT

This paper presents a low-cost distance-spoofing attack on a mmWave Frequency Modulated Continuous Wave (FMCW) radar. It uses only a replica radar chipset and a single compact microcontroller board both in mass production. No expensive and bulky test instrument is required, and hence a low-cost and light-weight attack setup is developed. Even with the limited hardware resource in this setup, the replica radar can be precisely synchronized with the target radar for distance-spoofing capability. A half-chirp modulation scheme enables timing compensation between crystal oscillators on the replica and the target radar boards. A two-step delay insertion scheme precisely controls relative delay difference between two radars at ns-order, and as a result the attacker can manipulate distance measured at target radar with only around ±10m ranging error. This demonstrates potential feasibility of low-cost malicious attack on the commercial FMCW radar as a physical security threat. A countermeasure employing random-chirp modulation is proposed and its security level is evaluated under the proposed attack for secure and safe radar ranging.

CCS CONCEPTS

• Security in hardware • Embedded systems security • Hardware attacks and countermeasures

KEYWORDS

mmWave; FMCW radar; ranging; distance-spoofing attack; security and safety

ACM Reference Format:

Noriyuki Miura, Tatsuya Machida, Kohei Matsuda, Makoto Nagata, Shoei Nashimoto, & Daisuke Suzuki. 2019. A Low-Cost Replica-Based Distance-Spoofing Attack on mmWave FMCW Radar. In *3rd Attacks and Solutions in Hardware Security Workshop (ASHES '19), November 15, 2019, London, United Kingdom.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3338508.3359567

ASHES'19, November 15, 2019, London, United Kingdom

ACM ISBN 978-1-4503-6839-1/19/11…$15.00
https://doi.org/10.1145/3338508.3359567

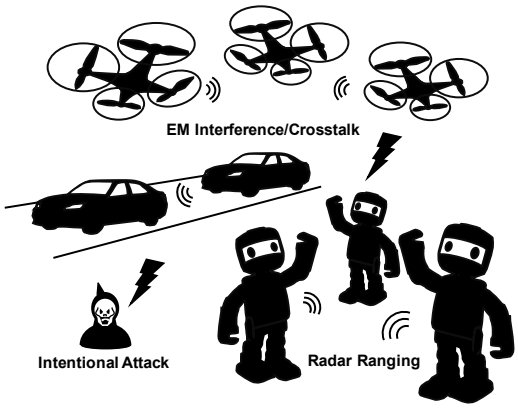

Fig.1 Technical challenge of radar ranging in autonomous CPS services.

1 Introduction

Ranging is one of the most fundamental functions for realizing purely autonomous Cyber-Physical-System (CPS) services, such as automatic driving, robot nursing, and drone guard (Fig.1), where physical moving objects directly actuate our physical world based on the information obtained from the environment surrounding them. A radar is one of the best options as a cost-effective ranging solution with widely scalable spatial resolution depending on its radio frequency. One of the biggest technical issue is the security and safety of the radar in applying to such advanced CPS services where malfunction of the ranging even causes fatal death. The situation is especially severe in those CPS applications. The ambient Electro-Magnetic (EM) interference and crosstalk are significantly large because the radar needs to co-operate with other multiple radars and also noisy mechanical moving parts (e.g. motors) placed close proximity operating at orders-of-magnitude higher voltages. This issue could be screened out by a component-level strict EM regulation compliance with an extensive EM immunity test at a product module. However, there is even a risk of malicious intentional attack to disable or manipulate the ranging functionality. The attack is relatively easier because the radar in CPS operates autonomously in a public open field with limited shield resources due to stringent cost and size constraints of the CPS node. This physical security threat should be covered by a white-hacker approach in this hardware-security community.

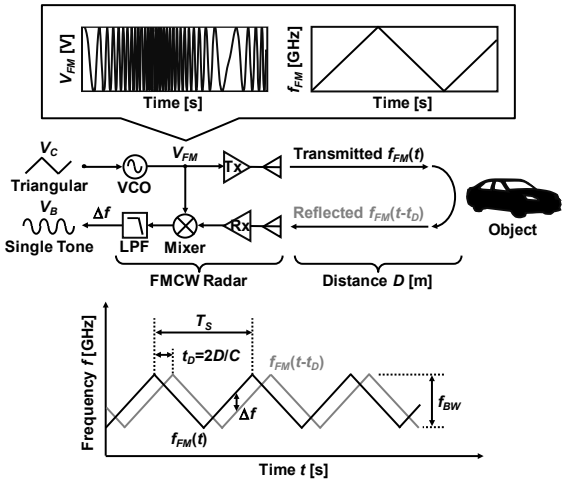

Fig.2 Operation principle of FMCW radar.

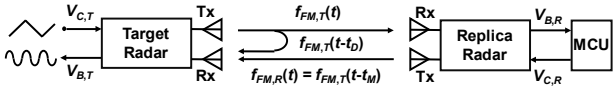

Fig.3 Overview of proposed replica-based distance-spoofing attack setup.

This paper presents a low-cost distance-spoofing attack on a mmWave Frequency Modulated Continuous Wave (FMCW) radar, one of the most commonly-used low-cost ranging radar with an appropriate ranging accuracy for the CPS applications. In this attack, instead of using any expensive and bulky test instruments, an identical replica of the target radar is utilized. This replica scheme significantly reduces its cost and thus demonstrates the practical feasibility of the proposed attack. It requires only the replica radar and one additional small Micro-Controller Unit (MCU) board for low-cost and compact setup, enabling a standalone field operation. Under the real-time MCU control, the replica-radar quickly synchronizes with the target radar to provide distance-spoofing capability. This kind of radar spoofing attack has been studied so far only in either simulations or low-frequency model-based studies [1-3]. Other related works [4, 5] only focus on how to make object electro-magnetically invisible by using an EM absorber. A Software-Defined Radio (SDR) approach might be considered as another attack scenario. However, an extremely high-end mmWave SDR hardware is needed which is not easily available to civilians. To our best of knowledge, the proposed attack setup, for the first time, demonstrates the feasibility of the real-time distance-spoofing attack on a mmWave FMCW radar by using commercially-available mass-products.

The rest of the paper is organized as follows. Next, in Section 2, the operation principle of the FMCW radar will be briefly reviewed. In Section 3, the detail of the proposed replica-based attack scheme will be described. In Section 4, a prototype attack setup comprised of commercial module products will be explained and the prototype demonstration will be presented with measured distance-spoofing capability. In Section 5, a countermeasure against the manipulation will be proposed and the protected radar will also be evaluated by the prototype. The capability and the limitation of the proposed attack and countermeasure will also be discussed. Finally, in Section 6, concluding remarks will be drawn.

2 FMCW Radar

The FMCW radar is one commonly-used ranging scheme to capture physical positioning information into a cyber domain. Compared to a Time-of-Flight (ToF) radar [6], a finer resolution with higher noise tolerance can be obtained. A distance is calculated based on a frequency-domain calculation instead of direct time-difference measurement such as in ToF.

Figure 2 depicts the operation principle of the FMCW radar. The radar transmits EM wave V_{FM} whose frequency $f_{FM}(t)$ is continuously modulated by controlled voltage V_C of Voltage-Controlled Oscillator (VCO), typically in a triangular shape. This so-called chirp signal is reflected back to the radar with a propagation delay t_D depending on the distance D between the radar and a target object. In the radar, the reflected signal therefore gives the time-shift frequency $f_{FM}(t-t_D)$, which is then down converted by self-mixing with the transmitted signal. A stable low-frequency beat signal V_B is obtained by a Low-Pass Filter (LPF). The frequency of the beat signal is given by the temporal frequency difference between the transmitted and reflected signal Δf. The distance D can be calculated by

$$D = CT_S\Delta f/4f_{BW}, \quad (1)$$

where C is the velocity of the light, T_S and f_{BW} is a sweep cycle and bandwidth, respectively. A relative velocity between the radar and the target could also be measured by Doppler frequency shift in the reflected signal. This paper focuses only on the distance ranging just for simplicity (our proposed system covers also velocity manipulation capability). The target range is 10~1,000m which corresponds to the propagation delay t_D of 10~1,000ns order. In a commercially-available ranging radar, f_{BW} of mmWave band (24GHz in this paper) is utilized. In this condition, T_S and Δf typically becomes ms and kHz order, respectively.

3 Attack Scheme

Figure 3 depicts the overview of our proposed attack setup. A target radar is attacked by its own identical replica radar and a compact MCU module. This replica-based configuration can fully cover the target mmWave frequency band with the minimum hardware resources. The MCU module controls the VCO in the replica radar through the control voltage $V_{C,R}$ to emit full-band mmWave EM interference to the target radar. In addition, by synchronizing with the target radar, the attacker can exhibit distance-spoofing capability. The replica radar in the attack setup can autonomously obtain the frequency-domain timing information of the target radar $f_{FM,T}(t)$ through the received signal $V_{B,R}$ for synchronization. A replicated signal with precise delay t_M can be generated as $f_{FM,R}(t)=f_{FM,T}(t-t_M)$ for the distance spoofing. By increasing the signal power of $f_{FM,R}(t)$ against that of an actual

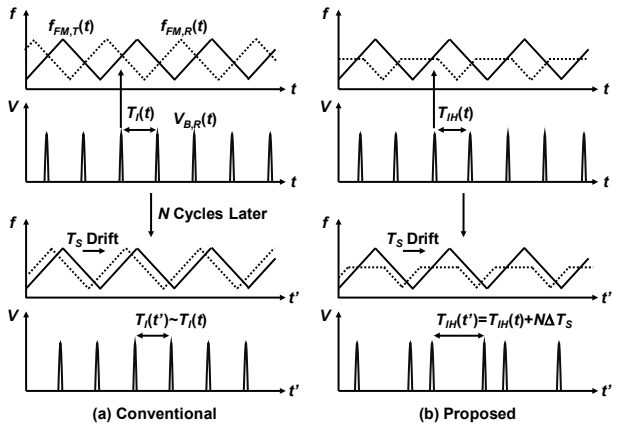

Fig.4 Operating waveforms of (a) conventional and (b) proposed Half-Chirp Modulation (HCM) scheme for timing calibration.

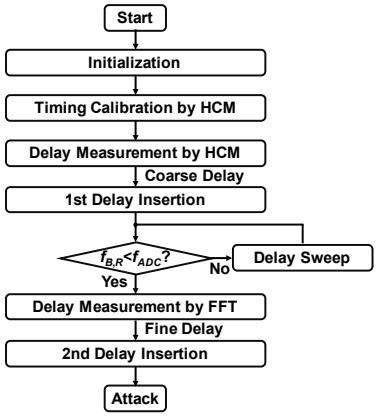

Fig.5 Attack flow chart with two-step delay insertion scheme.

reflected signal $f_{FM,T}(t-t_D)$, the target radar miscalculates the distance with a typical peak frequency search in the beat signal $V_{B,T}$. However, a ns-order accurate timing control is needed for distance spoofing of around ±10m errors. This is especially difficult by the compact MCU module with limited hardware resources e.g. Analog-to-Digital Converter (ADC) sampling rate of <1MSample/s and digital signal processing performance at <100MHz system clock. In order to cope with this hardware limitation, a Half-Chirp Modulation (HCM) and two-step delay insertion schemes are proposed in this paper, which are the main contributions of this paper.

3.1 Half-Chirp Modulation (HCM) scheme

The first technical challenge is how to keep synchronization between the replica and the target radar. Even though the identical replica is employed in the attack setup, there exists a slight timing variation between source crystal oscillators in the target and replica radar. The timing variation is typically around only 100ppm however this finally causes a significant timing error in the ns-order precise synchronization, which is required in this attack. The error can be seen as a sweep cycle T_S drift ΔT_S as described in Fig.4 (a). ΔT_S is typically as small as a few 10s of μs which is however unignorably large because the ns-order accurate timing control is needed for distance-spoofing capability. The timing error can be calibrated by measuring this ΔT_S through the beat signal in the replica radar $V_{B,R}$. The $V_{B,R}$ signal becomes a periodic spike signal generated at the cross point of the frequency chirp due to the mixer and LPF topology in the radar. LPF only produces when the beat frequency becomes near zero. The interval between these spikes $T_I(t)$ essentially contains the ΔT_S information. However, in a conventional chirp signaling (Fig.4 (a)), it is very difficult to directly extract ΔT_S from $T_I(t)$ due to limited ADC timing resolution of <1Msample/s. The direct measurement of the interval $T_I(t)$ by the ADC contains about ±1μs timing error which is far beyond the target accuracy. In the proposed Half-Chirp Modulation (HCM) scheme (Fig.4 (b)) where the frequency modulation is performed for only a half cycle, ΔT_S can be accumulated in the spike interval $T_{IH}(t)$ over the multiple cycles N as

$$T_{IH}(t')=T_{IH}(t)+N\Delta T_S. \quad (2)$$

The accumulated $N\Delta T_S$ can be captured even by the ADC with the limited timing resolution.

3.2 Two-step delay insertion scheme

The second technical challenge is how to insert after the timing calibration a ns-order accurate delay offset for the distance spoofing. In order to precisely adjust the delay, the relative delay between the target and the replica radar must be measured precisely. However, as described above, due to the limited ADC timing resolution of <1Msample/s, the relative delay measurement by ADC contains around ±1μs error. This is again far beyond the target accuracy. To solve this problem, the two-step delay insertion scheme is proposed. Figure 5 describes the operating flow chart: At the first step, the relative delay is coarsely measured by ADC. The HCM signal is again utilized and the spike interval $T_{IH}(t)$ is measured to calculate the delay. A coarse delay is first inserted to reduce the delay between the target and replica radar. Both the $f_{FM,T}$ and $f_{FM,R}$ chirps almost overlap with around ±1μs error. Small delay sweep is performed to guarantee the beat frequency obtained in the replica radar $f_{B,R}$ to be within the ADC bandwidth f_{ADC} of <500kHz. Fast Fourier Transform (FFT) is then processed to measure $f_{B,R}$ and calculate a precise delay based on the same principle of FMCW ranging (Fig.2). Finally, a fine delay is inserted including time difference required for the distance spoofing. Note that both the timing calibration and delay measurements are performed only by using the radar receiver and the local VCO. The radar transmitter is disabled and there is no unnecessary EM transmission during this sequence, the target radar therefore cannot notice the attack. In addition, the timing and delay calibration is needed only once at the startup, the replica radar after the synchronization can track and update the relative delay by every FFT calculations. The proposed attack can be thus applied to real-time moving objects.

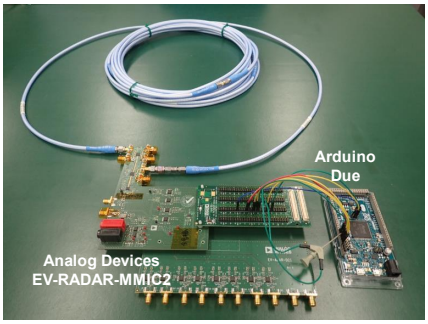

Fig.6 Prototype setup for attack.

4 Prototype Demonstration

Figure 6 presents the prototype attack setup. A commercial 24GHz mmWave FMCW radar module, Analog Devices Inc. EV-RADAR-MMIC2 [7], is selected for the demonstration. The radar module consists of VCO ADF5901 [8], a triangular wave generator ADF4159 [9], and a down conversion mixer ADI ADF5904 [10]. A compact MCU module, Arduino Due [11], is employed for the attack control. It incorporates ADC operating at <1Msample/s and a 32-bit ARM core operating at an 84MHz clock. The MCU module controls the replica radar in real-time providing the digital control code for the triangular wave generator through a common Serial-Peripheral Interface (SPI) link. All required components are commercially available mass products and the total cost of this setup is only less than $1,000.

In this paper, the distance-spoofing attack is demonstrated with wired connections between the target and replica radar. This is only due to limited test facilities for a wireless test. A standalone field test with a wireless condition would also be possible with this light-weight attack setup configuration. The field test demonstration is now an on-going work. In this prototype setup, the propagation delay is emulated by a long coaxial cable and the reflected wave is generated through an attenuator and a directional coupler where the reflected wave and the replicated wave are combined together and feedback to the target radar. A mixed-signal real-time oscilloscope Keysight MSO9404A is used for monitoring the prototype operation only for the demonstration purposes. The information obtained by the oscilloscope is not utilized in the attack.

Figure 7 presents operating waveform snapshots during the prototype demonstration where the center frequency f_C, sweep bandwidth f_{BW}, and sweep cycle T_S, are 24.125GHz, 200MHz, and 4ms, respectively. At start up, due to large initial delay offset t_{OS} between the target and replica radar, only small periodic spike could be seen in the beat signals at the cross points of the frequency chirp (Fig.7 (a)). In initialization, slight frequency offset between the target and replica radar f_C is calibrated based on the spike interval measurement with down conversion by an unmodulated signal (Fig.8). The offset is calibrated as every spike interval becomes equal. The variation in f_{BW} can also be calibrated similarly. The HCM is then performed for the source clock timing calibration (Fig.7 (b)). In this particular radar pair, the T_S drift ΔT_S was measured to be around 87µs per cycle which is calibrated based on the ΔT_S measurement with HCM. The delay offset t_{OS} between the target and replica radar

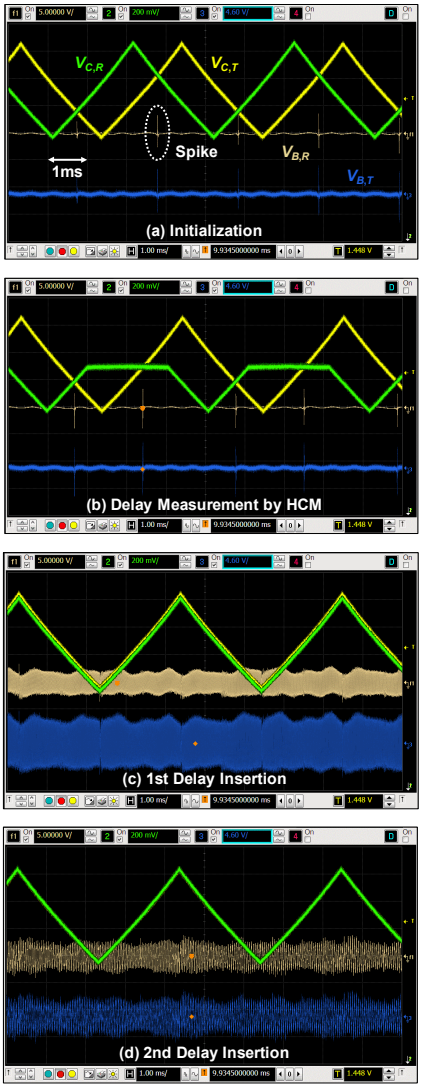

Fig.7 Operating waveform snapshots during attack sequence (a-d).

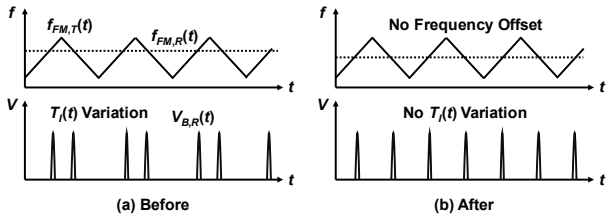

Fig.8 Initial frequency offset calibration waveforms (a) before and (b) after calibration.

is then measured also with HCM. The first coarse delay t_{OS} insertion followed by the delay sweep guarantees the frequency of the beat signal to be within the ADC bandwidth (Fig.7 (c)). As shown in Fig.7 (c), low-frequency beat signals are appeared also in the oscilloscope snapshot. Finally, in the second delay insertion, FFT is one-time executed in the ARM core to measure accurate delay and precisely

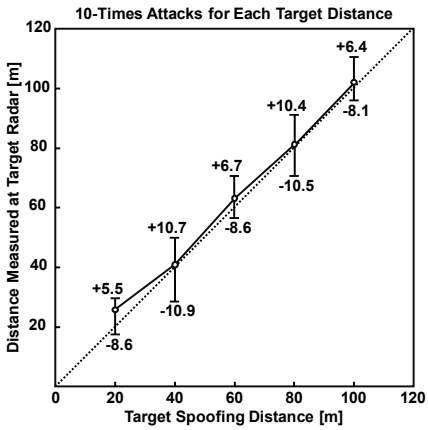

Fig.9 Measured distance vs. target spoofing distance.

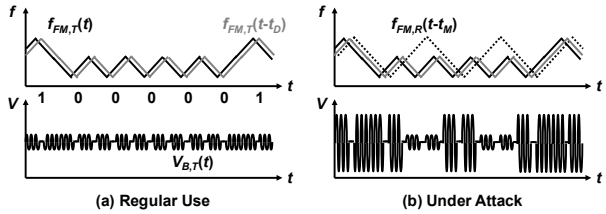

Fig.10 Operating waveforms of proposed random-chirp modulation scheme (a) in regular use and (b) under attack.

adjust the delay for the distance spoofing (Fig.7 (d)). It can be seen in Fig.7 (d) that the frequency of the beat signal is further lowered by the 2nd fine delay insertion. Above attack sequence for the timing synchronization and distance spoofing is performed within 10s by the proposed attack setup. Again, this sequence is only needed once at the startup and after the synchronization the replica radar can track and update the relative delay in real time during the attack.

Figure 9 presents measured accuracy of the distance spoofing. The distance was measured at the target radar by 10 times at each target spoofing distance setting in the replica radar. The bar plot in Fig.9 shows that the distance-spoofing accuracy is measured to be around ±10m. This indicates potential capability of a replica-based low-cost distance-spoofing attack as a physical security threat of the FMCW radar. The accuracy is only restricted by a 10ns limited delay step controllability in Arduino Due [11] and it can be easily improved by employing a higher-performance MCU module in the attack, such as Arduino TRE [12].

5 Discussion on Attack and Countermeasure

The result of the distance spoofing in Fig.9 implies that this kind of controlled replica radar could be exploited as a low-cost attack tool. With only a replica radar and a cheap MCU board (both commercially available products), the attacker can manipulate the distance between the target objects both shorter and longer freely around at least ±10m error. As a countermeasure against this distance-spoofing attack, a random-chirp modulation is proposed.

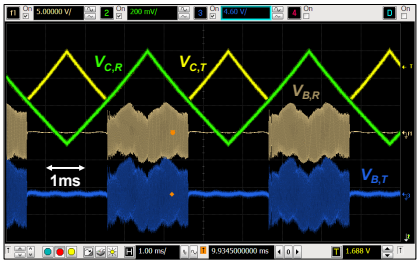

Fig.11 Operating waveform snapshot of random-chirp modulation.

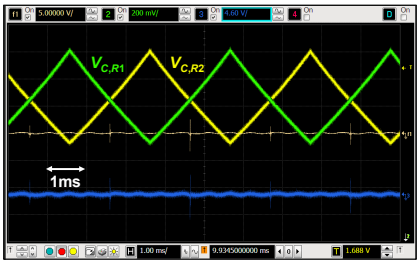

Fig.12 Operating waveform snapshot of dual-chirp signaling.

Figure 10 depicts its operation concept. At every half chirp cycle, the radar changes the chirp signal either going up or down depending on a random code sequence. When the code is "0", down-chirp is generated and up-chirp when "1". In this random chirp modulation, a stable beat signal is obtained in a regular operation with an actual reflected signal (Fig.10 (a)). Under the spoofing attack, the amplitude of the beat signal becomes unstable unless the attacker knows the random code (Fig.10 (b)).

A simple low-frequency envelope detector can be employed as an attack sensor. The protected radar with the random-chirp modulation was evaluated also by the prototype. An operating waveform snapshot in Fig.11 confirms the successful protected operation. The random-chirp modulation is a good low-cost countermeasure with the capability to detect the attack in the low-frequency beat-signal domain. However, by exploiting two replica radars each synchronized by the proposed schemes, both up and down dual chirps $V_{C,R1}$ and $V_{C,R2}$ can be simultaneously generated as shown in Fig.12 and the random-chirp modulation can be disabled by this dual-chirp signaling. This test result indicates the necessity of further sophisticated countermeasure for further advanced security and safety of the FMCW radar. One potential solution is to incorporate a high-bandwidth ADC. By monitoring abnormally-high frequency components in the beat signal, existence of the dual-chirp can be detected. Implementation of this advanced physical countermeasure and demonstration of the effectiveness under the wireless field test condition would be the future works of this research.

6 Conclusion

Hardware security of a ranging radar is an essential requirement for the ranging function in the future advanced CPS services. This

paper presents a replica-based distance-spoofing attack on a mmWave FMCW radar. A half-chirp modulation and a two-step delay insertion scheme enable precise synchronization between the replica and the target radar and hence exhibit distance-spoofing capability even with low-cost and light-weight hardware resources. The distance spoofing with ±10m error was successfully demonstrated on a commercial 24GHz mmWave radar product by using its replica. A random-chirp-based countermeasure against the attack is proposed and evaluated. The attack results indicate the necessity of further advanced countermeasure for a secure and safe FMCW radar.

REFERENCES

[1] A. Ranganathan, B. Danev, A. Francillon, and S. Capkun, "Physical-Layer Attacks on Chirp-Based Ranging Systems," in Proc. the 5th ACM conference on Security and Privacy in Wireless and Mobile Networks (WISEC), pp. 15-26, June 2012.

[2] H. R. Chen, "FMCW Radar Jamming Techniques and Analysis," Naval Postgraduate School Monterey CA, 2013.

[3] R. G. Dutta, X. Guo, T. Zhang, K. Kwiat, C. Kamhoua, L. Njilla, and Y. Jin, "Estimation of Safe Sensor Measurements of Autonomous System under Attack," in Proc. of the 54th Annual Design Automation Conference (DAC), pp. 1-6, June 2017.

[4] R. Chauhan, "A Platform for False Data Injection in Frequency Modulated Continuous Wave Radar," Digital Commons, Utah State University, http://www.ece.usu.edu/grad/reports_theses_disseratations/2014/Chauhan_Ruchir/thesis.pdf

[5] C. Yan, W. Xu, and J. Liu, "Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self Driving Vehicles," DEFCON24, Sept. 2016.

[6] S. Kawahito, I.A. Halin, T. Ushinaga, T. Sawada, M. Homma, and Y. Maeda, "A CMOS Time-of-Flight Range Image Sensor with Gates-on-Field-Oxide Structure," IEEE Sensors Journal, Vol. 7, No. 12, pp. 1578-1586, Dec. 2007.

[7] Analog Devices Inc., "UG-866: EV-RADARMMIC2 User Guide Rev. 0," http://www.analog.com/media/en/technicaldocumentation/user-guides/EV-RADAR- MMIC2_UG-866.pdf

[8] Analog Devices Inc., "ADF5901: 24 GHz VCO and PGA with 2-Channel PA Output Rev. 0," http://www.analog.com/media/en/technicaldocumentation/data-sheets/ADF5901.pdf

[9] Analog Devices Inc., "ADF4159: Direct Modulation/Fast Waveform Generating, 13 GHz, Fractional-N Frequency Synthesizer Rev. E," http://www.analog.com /media/en/technicaldocumentation/data-sheets/ ADF4159.pdf

[10] Analog Devices Inc., "ADF5904: 4-Channel, 24 GHz Receiver Downconverter Rev. A," http://www.analog.com/media/en/technicaldocumentation/data-sheets/ADF5904.pdf

[11] Arduino, "Arduino Due," https://store.arduino.cc/usa/due

[12] Arduino, "Arduino TRE," https://www.arduino.cc/en/Main/ArduinoBoardTre