3rd URSI AT-AP-RASC, Gran Canaria, 29 May – 3 June 2022

Automotive FMCW radar spoofing device based on a low-cost backscatter tag

A. Lazaro(1), A Porcel(1), M.Lazaro(1), R. Villarino(1) and D. Girbau(1)
(1) Department of Electronics, Electrics and Automatic Control Engineering, Rovira i Virgili University, 43007 Tarragona, Spain, Email: antonioramon.lazaro@urv.cat

Modern advanced driver assistance systems (ADAS) are progressively equipped with millimeter-wave radar technologies. These automotive radars are based on frequency-modulated continuous-wave (FMCW) radars that can measure both the velocity and range of targets. Since this technology is rapidly growing, interferences and radiofrequency attacks that will become a major security issue that will need to be addressed. Consequently, since the radars constitute an essential part of the vehicle, among other aspects with regard to safety issues, the cyber-attacks that may occur in it must be carefully treated, in order to preserve the safety of the occupants of the vehicle and especially in autonomous vehicles that will soon be a reality.

The purpose of this work is to present a low-cost spoofing device based on a modulated backscatter to generate a ghost capable of confusing a 24 GHz mmWave FMCW radar installed inside the vehicle (Figure 1.a). The modulated backscatter consists of two patch antennas, with two 3D-printed PLA dielectric lenses on top of each (Figure 1.b) to increase the gain up to 17.5 dB. Antennas are interconnected by two MMIC LNAs (LNA-24-04 from Silicon Radar) with a typical gain of 17 dB at 24 GHz and a current consumption of 5.6 mA at 3.3 V per amplifier. The modulation of the backscatter is produced by switching the gain of the amplifiers to achieve a sufficiently high differential RCS, comparable to that of a car at 24 GHz. The victim radar detects a beat frequency shift associated with the backscatter modulation frequency resulting in a false target. The modulation frequency to generate spoofing targets at different distances and velocities is configured by a low-power microcontroller. The theory has been verified with simulations and measurements performed with the spoofing device at 24 GHz and a FMCW radar (EVAL-DEMORAD from Analog Devices). Figures 1.b-c show some measured range-Doppler maps where two false targets have been introduced in range and velocity. Countermeasures to detect a potential spoofing using backscattered devices have also been proposed. They are based on random variation in radar sweep parameters such as the sweep slope or the duration of the chirps.

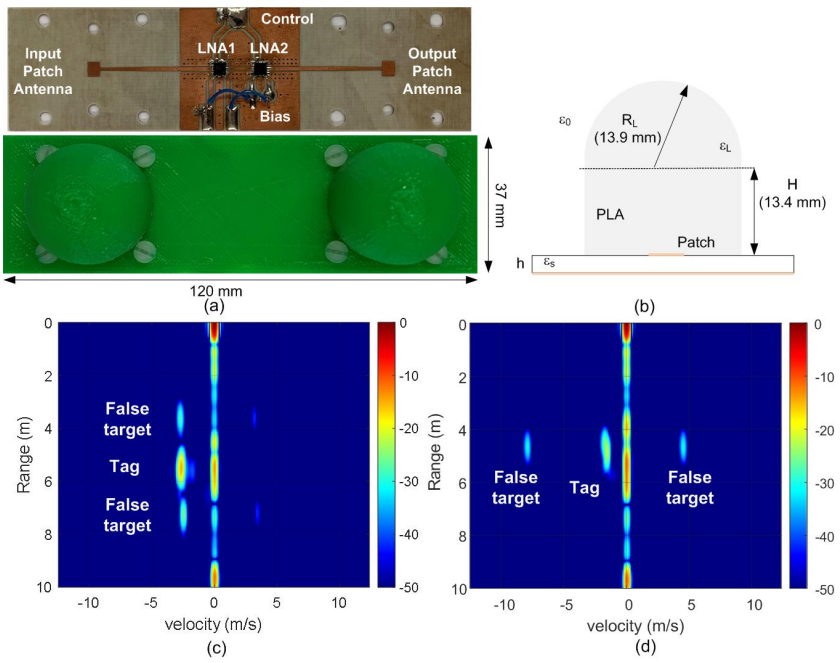

Figure 1. (a) Prototype photography. (b) Detail of the lense over the patch. (c) Measured range-Doppler map including two false targets at 2.5 m with the spoofing device (tag) moving approaching the radar. (d) Measured range-Doppler map including two false targets generated with a Doppler frequency shift of 1000 Hz with the tag approaching the radar.