Spoofing Attacks Against Vehicular FMCW Radar

Rony Komissarov

School of Electrical Engineering

Tel Aviv University

Ramat Aviv, 69978. Israel

ronykom@gmail.com

Avishai Wool

School of Electrical Engineering

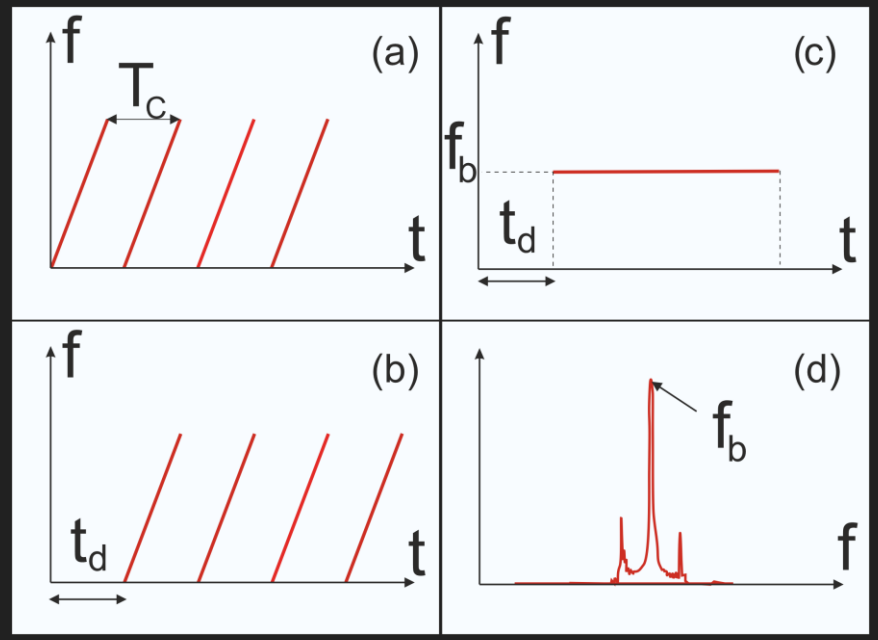
Tel Aviv University

Ramat Aviv, 69978. Israel

yash@eng.tau.ac.il

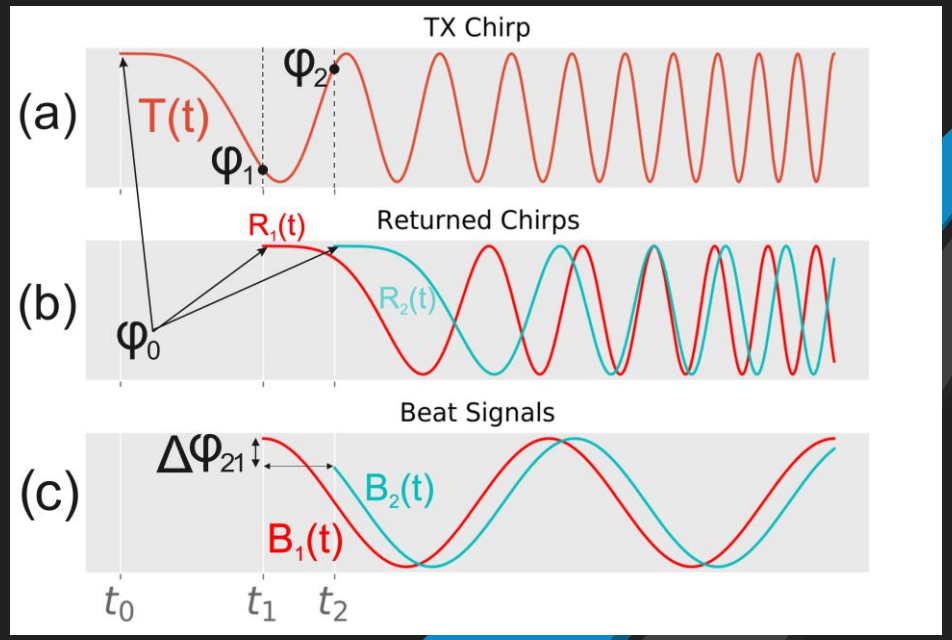
FMCW Radar Technical Background

Range Measurement using Range-FFT



$$d = \frac{c \cdot f_b}{2S}$$

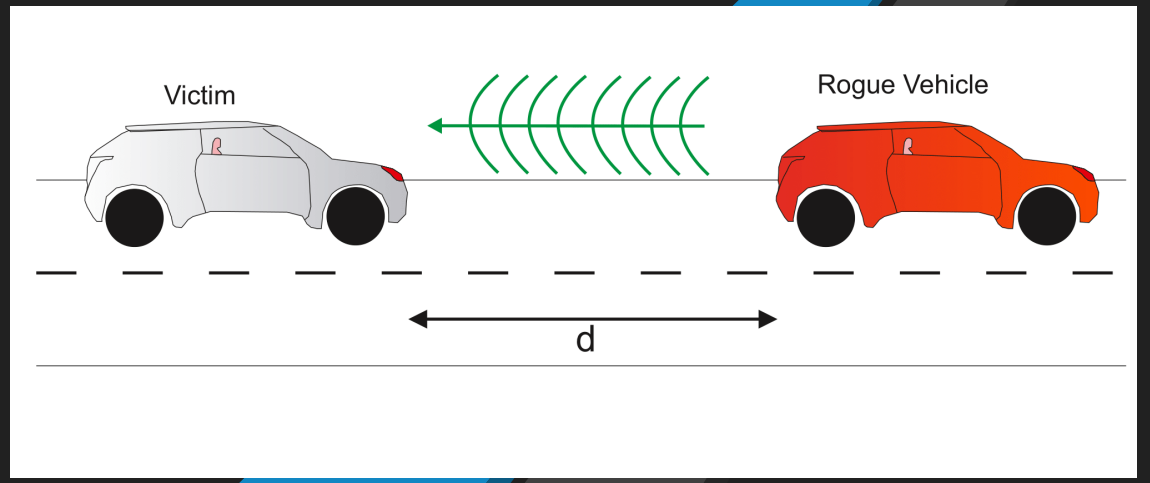
Velocity Measurement using Phase Extraction



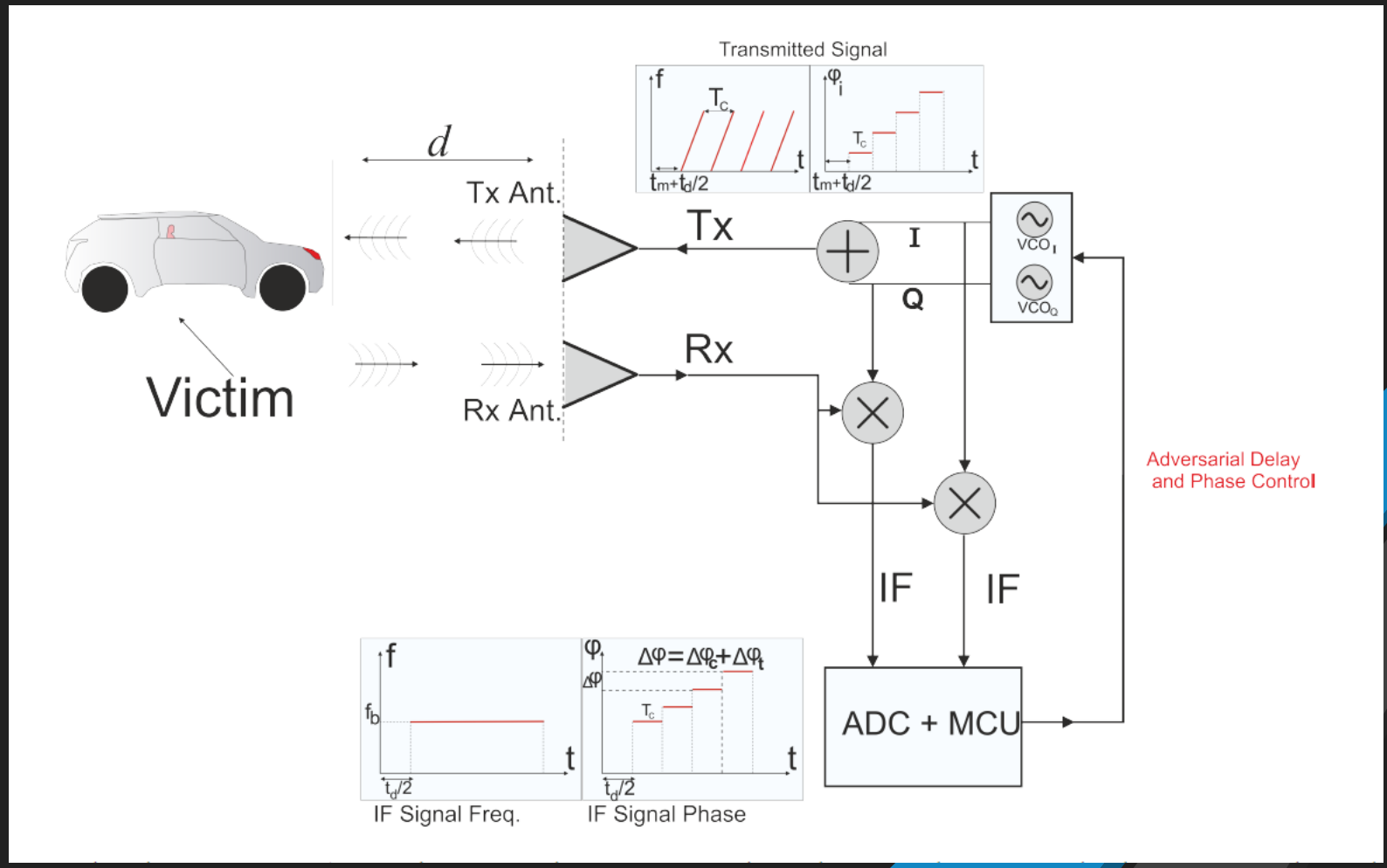
$$v = \frac{\lambda \Delta \varphi_{i+1,i}}{4\pi T_c}$$

Attack Model

- Victim is behind the attacker's vehicle and has an FMCW radar Installed, facing forward
- The attacker has a modified radar system facing back
- The attacker can sense the victim's FMCW signal, and send much more powerful signal compared to the real reflected signal arriving at the victim



Attack System Architecture

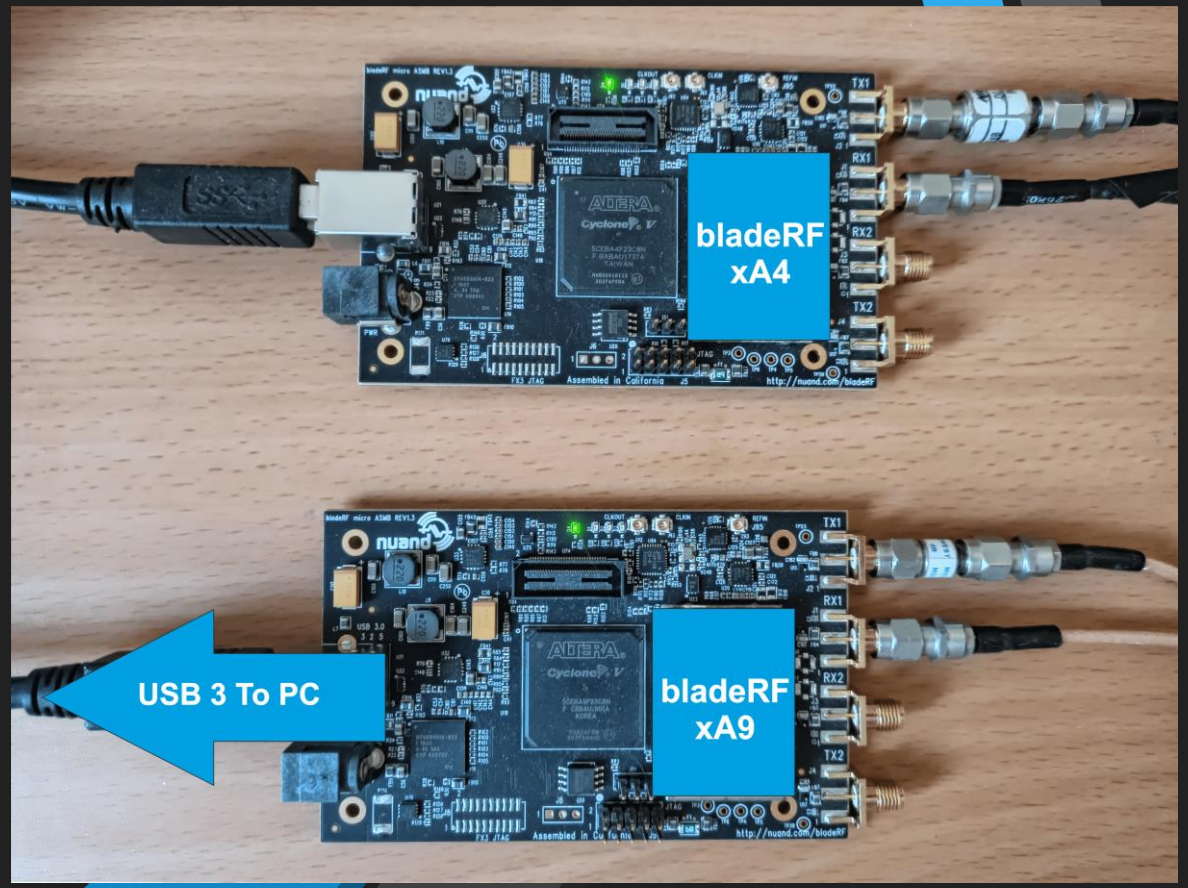


Simultaneous Range and Velocity Spoofing

- Sense victim’s signal, while generating internal chirps
- Use first N to synchronize (we used N=2 out of 100)
- Send fake chirp echoes, control the delay to spoof the distance
- Simultaneously, control the echo's phase to spoof the velocity

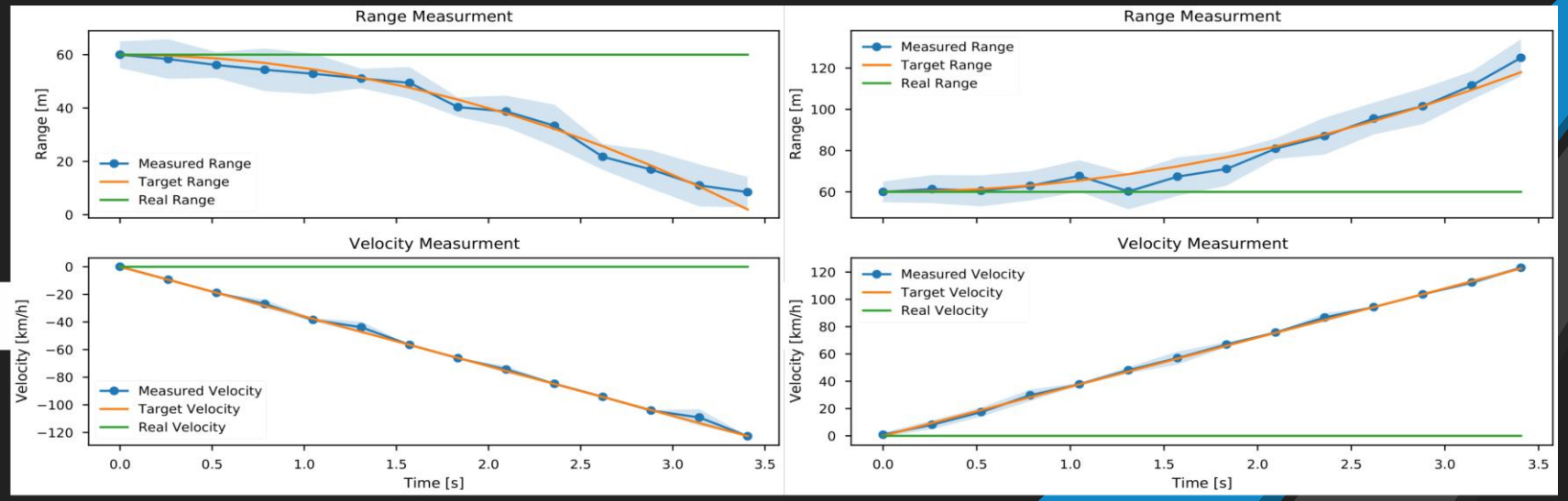
Proof of Concept Setup

- Consists of two Software Defined Radios (SDR), both are bladeRF 2.0 micro
- One is used as the attacker and the other one as the victim
- Connected with cables beyond the photos right margin



Results and Discussion

- Two scenarios – a sudden phantom stop and a sudden phantom acceleration
- Each scenario was simulated 15 times
- Simultaneous spoofing of both range and velocity
- Constant acceleration/deceleration of -+10 m/sec²
- The attack is very difficult for detection, since it matches the laws of mechanics



Thank You!

Rony Komissarov

School of Electrical Engineering

Tel Aviv University

Ramat Aviv, 69978. Israel

ronykom@gmail.com

Avishai Wool

School of Electrical Engineering

Tel Aviv University

Ramat Aviv, 69978. Israel

yash@eng.tau.ac.il