



南京邮电大学

mmSpoof:基于反射阵列的毫米波雷达的 弹性欺骗



汇报人: 韩科爽



指导教师: 张品昌

参考文献: mmSpoof: Resilient Spoofing of Automotive Millimeter-wave Radars using Reflect Array

Published in: [2023 IEEE Symposium on Security and Privacy \(SP\)](#)

Date of Conference: 21-25 May 2023



目录



南京邮电大学
Nanjing University of Posts and Telecommunications



第一部分

研究背景



第二部分

FMCW雷达



第三部分

mmSpooF



第四部分

实验结果



第五部分

总结与展望



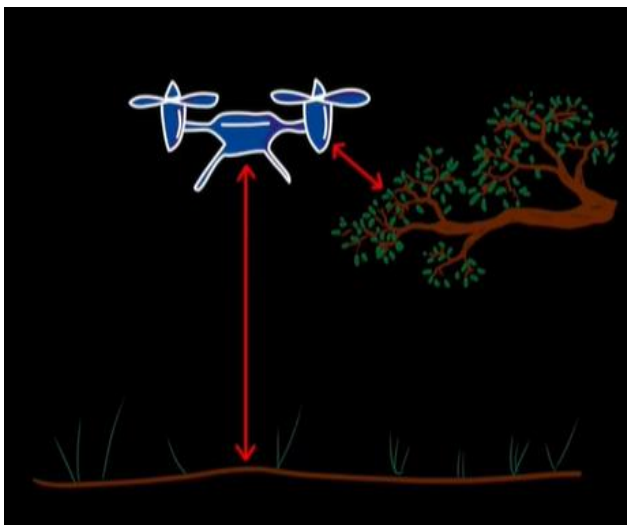
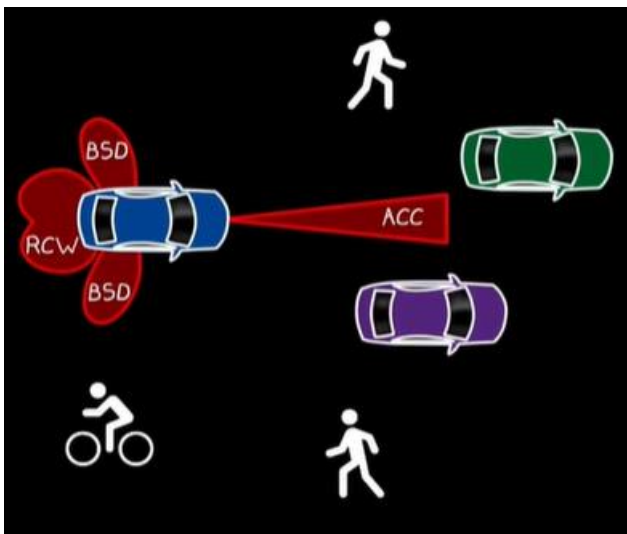
南京邮电大学
Nanjing University of Posts and Telecommunications



第一部分 研究背景



1.研究背景

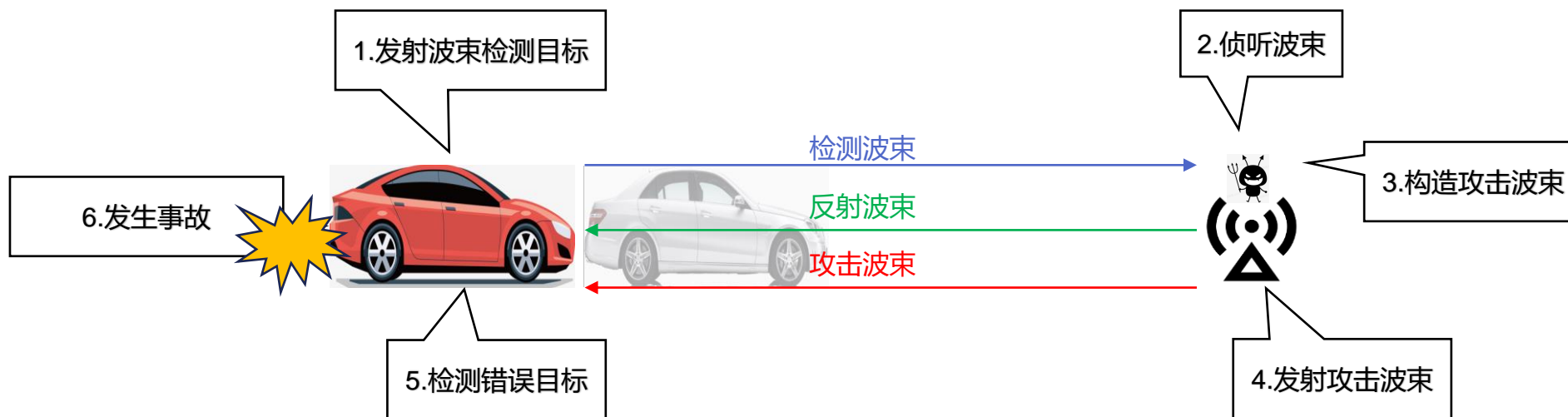


在当前环境下，自动驾驶和无人机等工具的**安全系统**依赖**雷达**实时侦测的数据维持其正常运行。

为了实现这样的功能，系统需要雷达具有**低成本、小尺寸、低开销和鲁棒性好**等特点。毫米波调频连续波雷达（FMCW）如今被应用到许多系统之中，因为它即使在其他光学传感器（如相机和激光雷达）发生故障的雾和弱光等**恶劣条件下**也能提供**稳健**的目标检测，它们已经在现代辅助驾驶系统（ADAS）中发挥着重要的作用。



FMCW雷达容易遭受欺骗攻击，攻击者往往通过侦听等手段获取雷达参数的**先验信息**，再**主动构造**欺骗波束，将其发射给雷达完成欺骗。

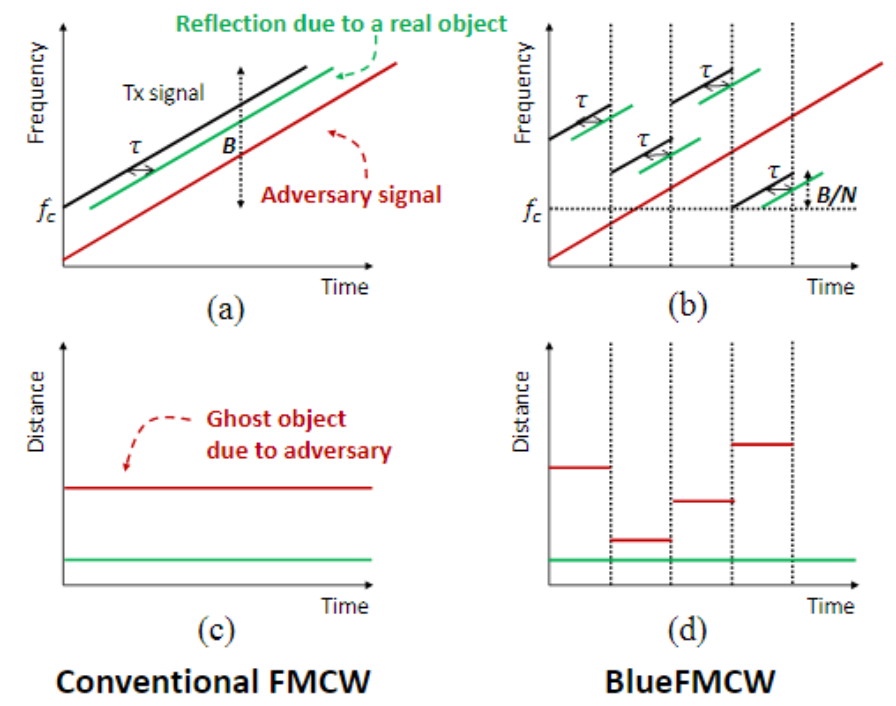
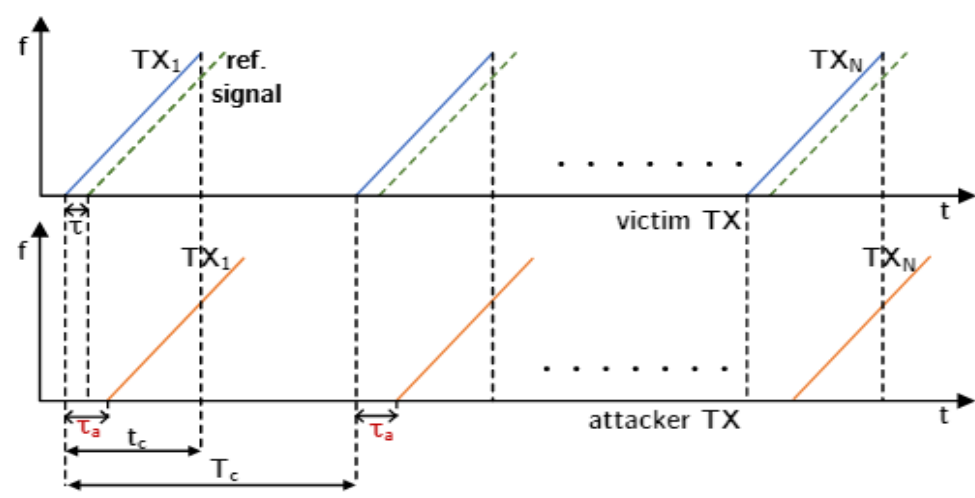




1.研究背景



在之前的研究中，研究者往往采用主动构造的方式进行欺骗，这种方式需要获悉雷达参数的先验知识，并且需要和雷达进行一定程度的同步，这种攻击方式鲁棒性差，一旦雷达改变参数就会失去作用。



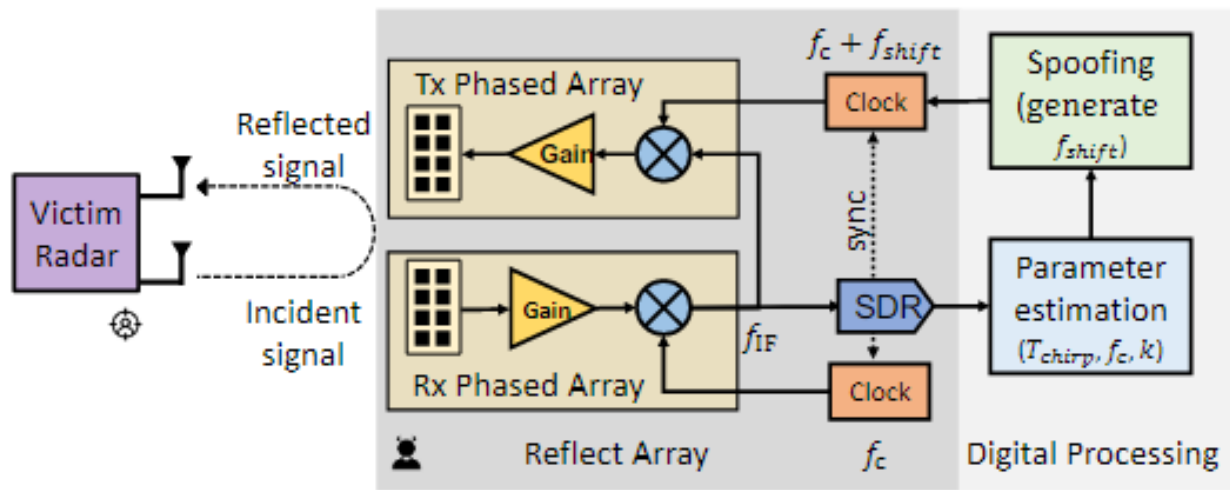


1.研究背景



本文提出一种基于反射阵列的欺骗方式可以进行无需同步、鲁棒性好的弹性欺骗。

与之前的主动攻击相比，本文的方法以受害者**发射波束**为攻击波束主体，**不需要进行数据帧的构造和对齐**，只需**修改频率**即可进行攻击，对于抗攻击策略具有**鲁棒性**





南京邮电大学
Nanjing University of Posts and Telecommunications



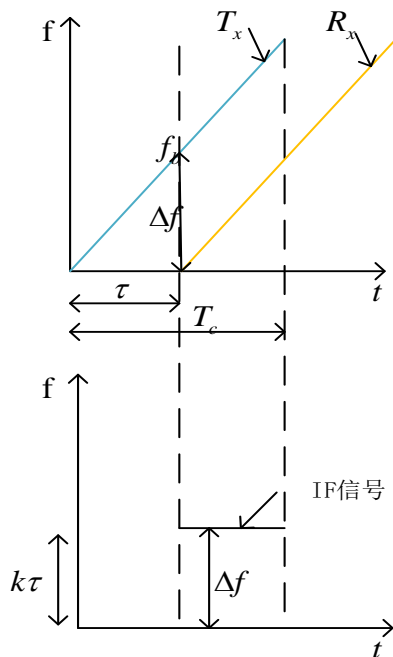
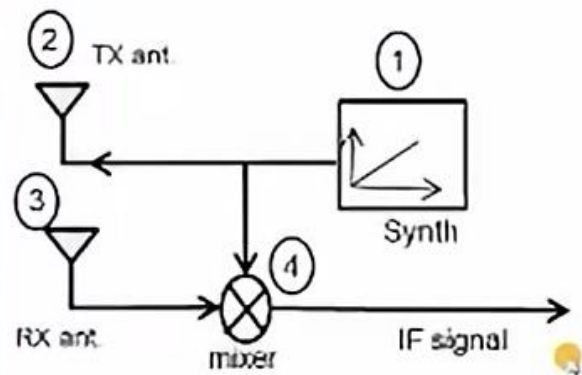
第二部分

FMCW雷达



2.1 工作原理

FMCW雷达发射频率随时间线性增长的啁啾信号，在接收到反射回来的信号后，将发射信号与接收信号混合成IF信号，进行参数分析。



FMCW雷达

距离估计

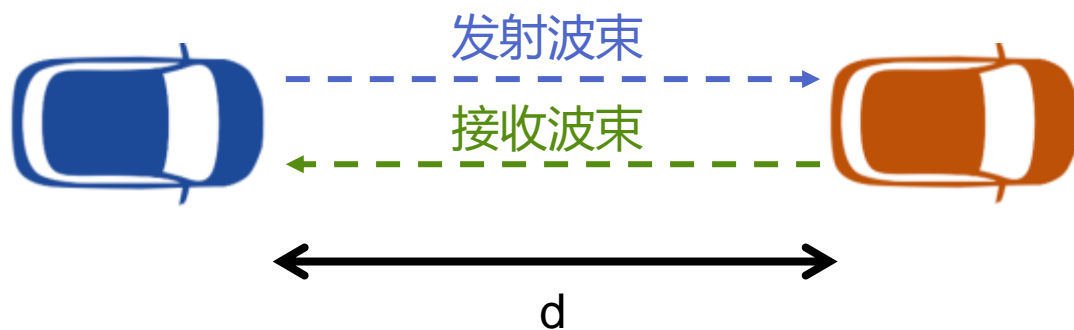
速度估计

角度估计



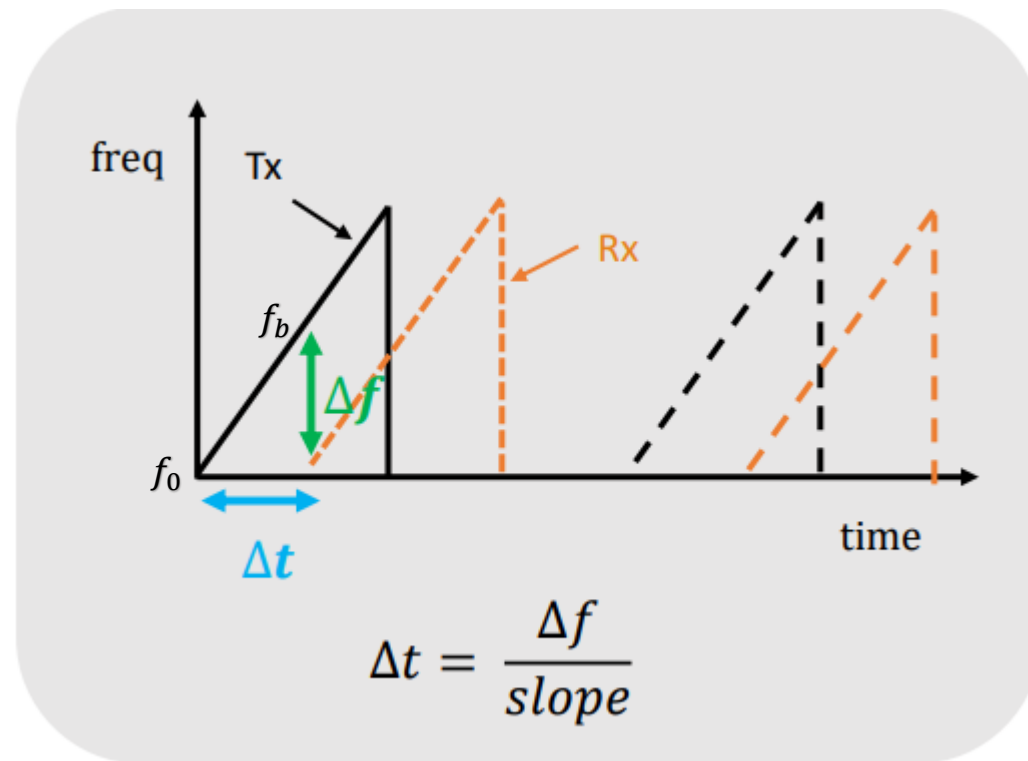
2.2 距离估计

雷达波束往返共经历 $2d$ ，历时 Δt 。在 f - t 图中，反射波束到达雷达时**频率差**为 $\Delta f = f_b = slope * \Delta t$ ，即可以根据频率差计算时间 Δt 从而计算距离 d 。



雷达估计的距离 d

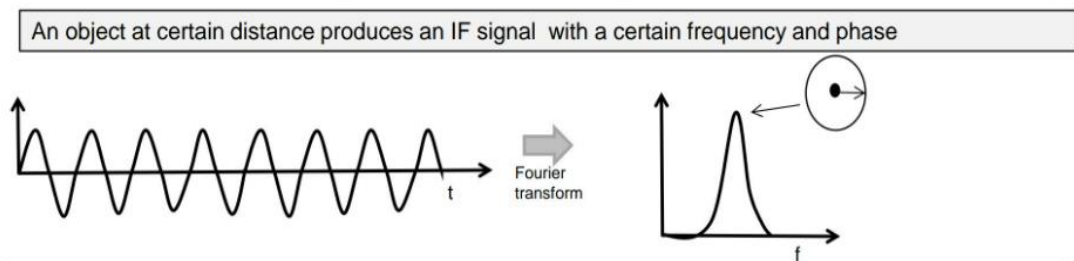
$$d = \frac{c\Delta t}{2} = \frac{c}{2} * \frac{\Delta f}{slope}$$





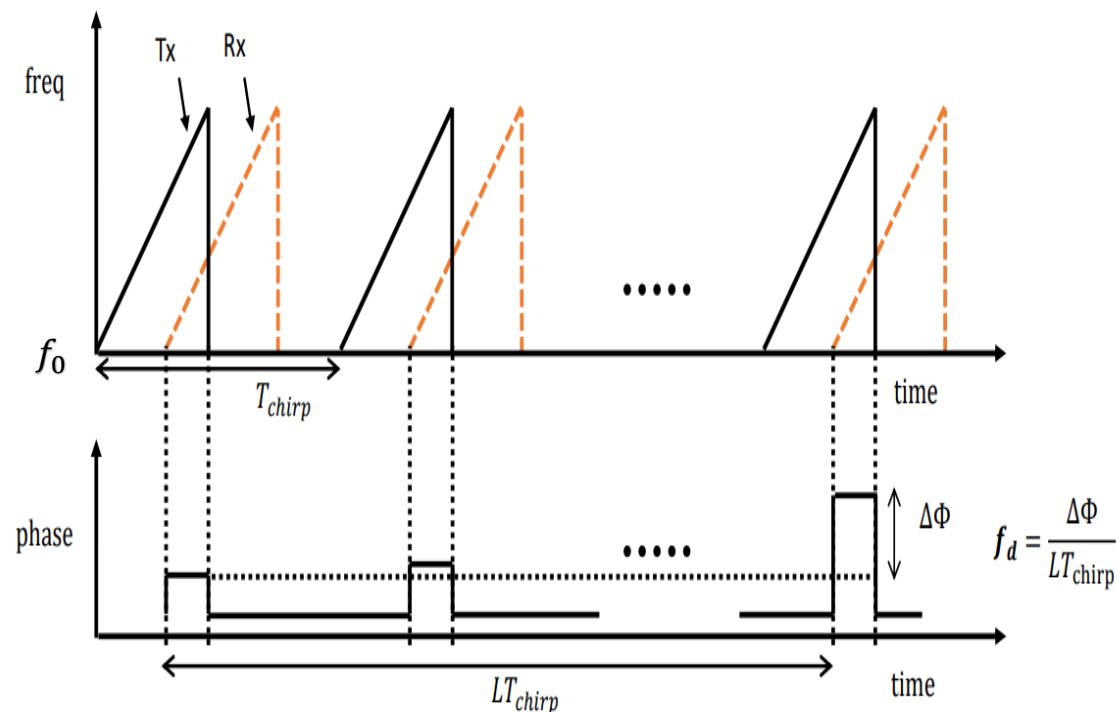
2.3 速度估计

雷达通过**多普勒频率**计算速度，可由相位变化率定义，即 $f_d = \frac{d\Phi(t)}{dt} = \frac{2f_0}{c} v$ 。
在离散域中可以用**相位差**与时间的比值表示，即 $f_d = \frac{\Delta\Phi}{LT_{chirp}}$ 。



雷达估计的速度v

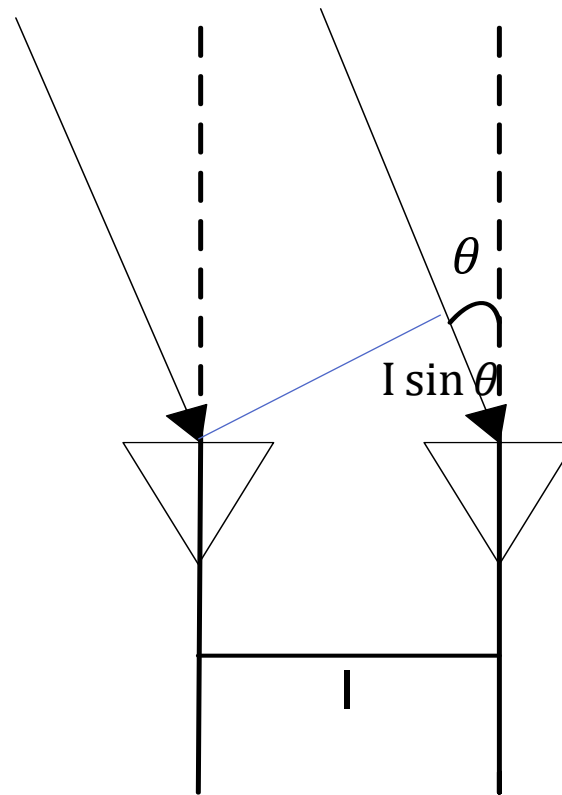
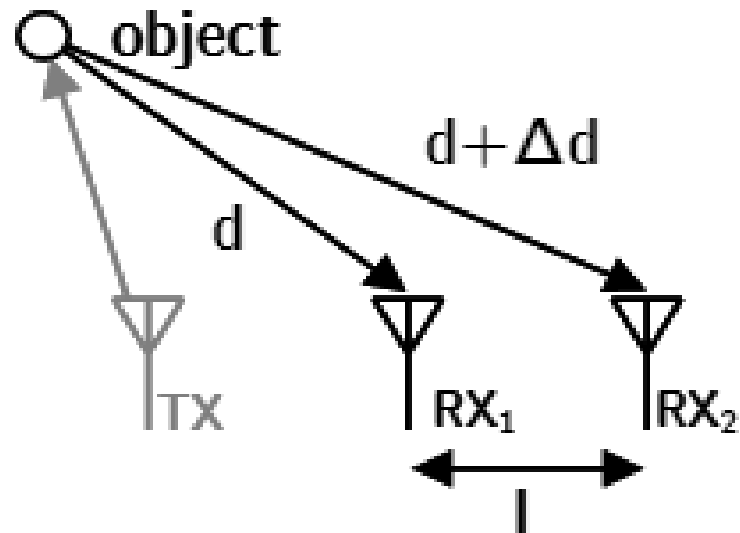
$$v = \frac{c}{2f_0} f_d$$





2.4 角度估计

当与目标距离较远时，反射波束近似一组平行光。雷达通过接收天线之间的波程差（可由相位差计算）计算目标角度。





第三部分

mmSpoof



主要内容



南京邮电大学
Nanjing University of Posts and Telecommunications



3.1

核心思想



3.2

反射阵



3.3

解耦

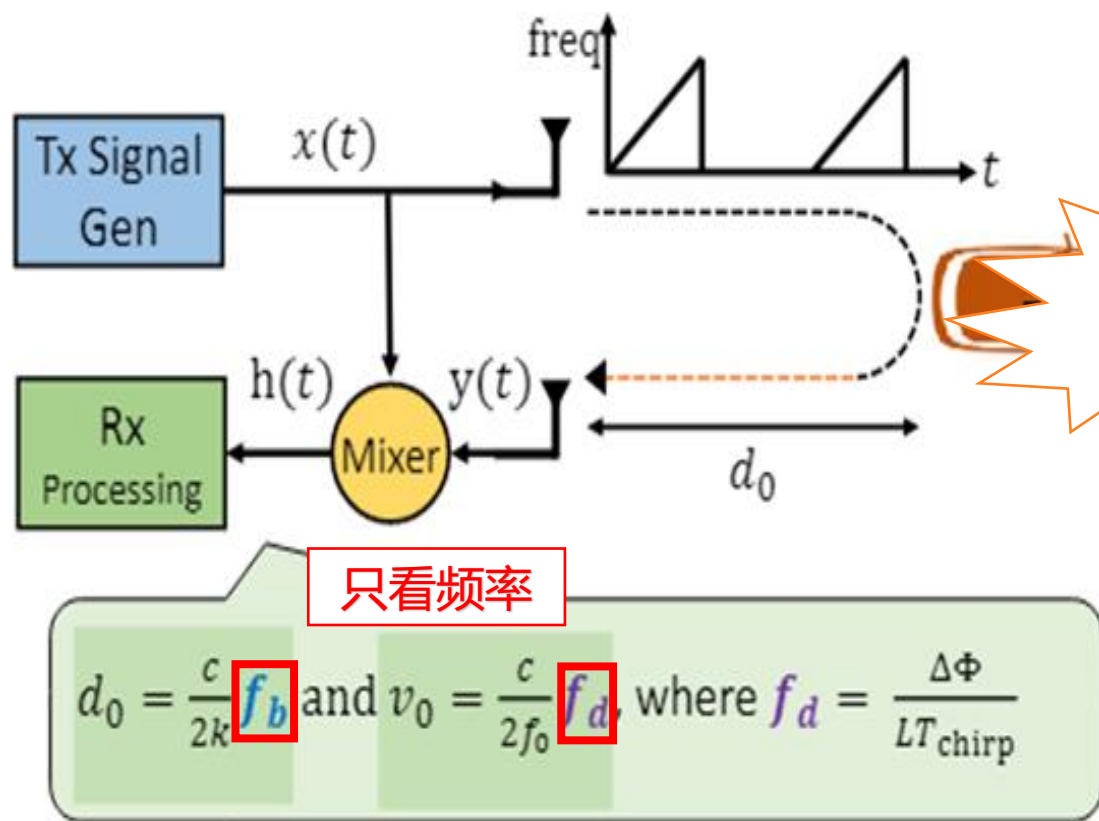


3.4

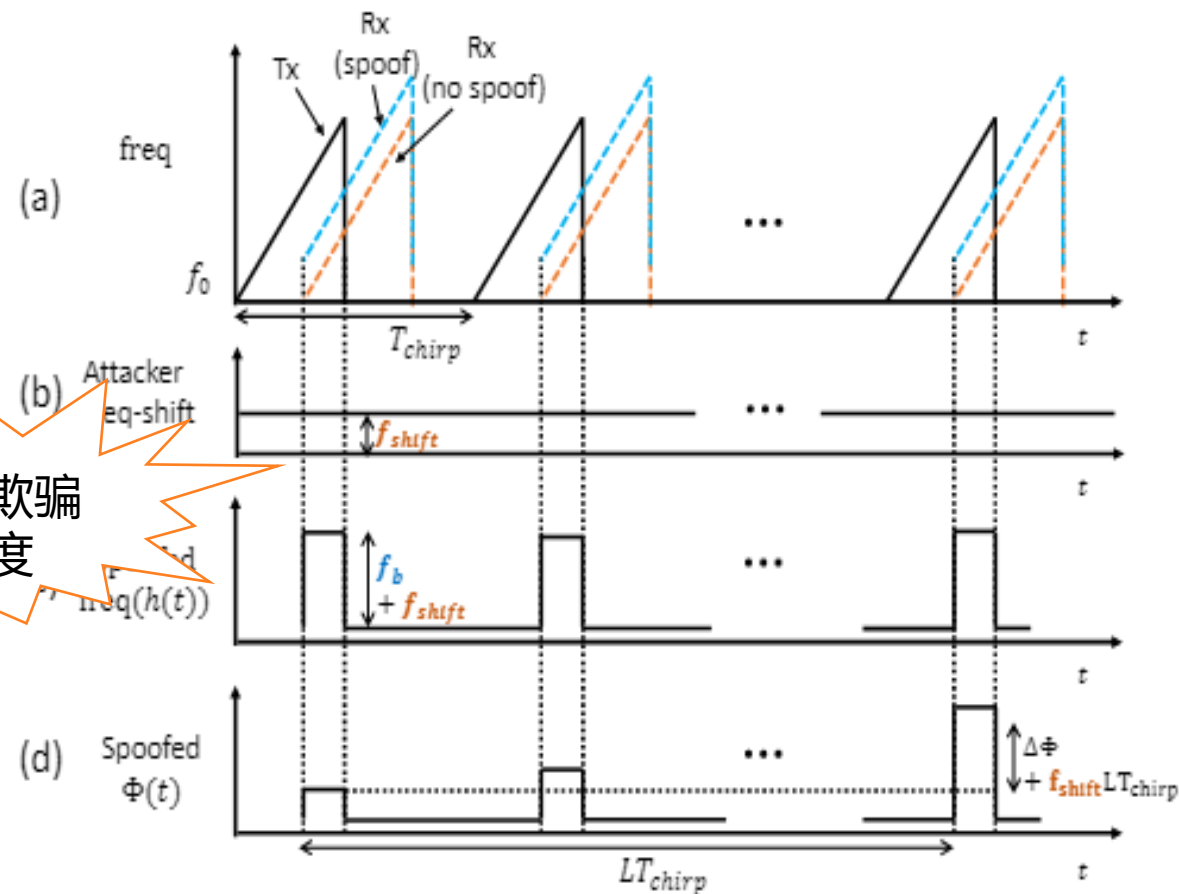
参数估计



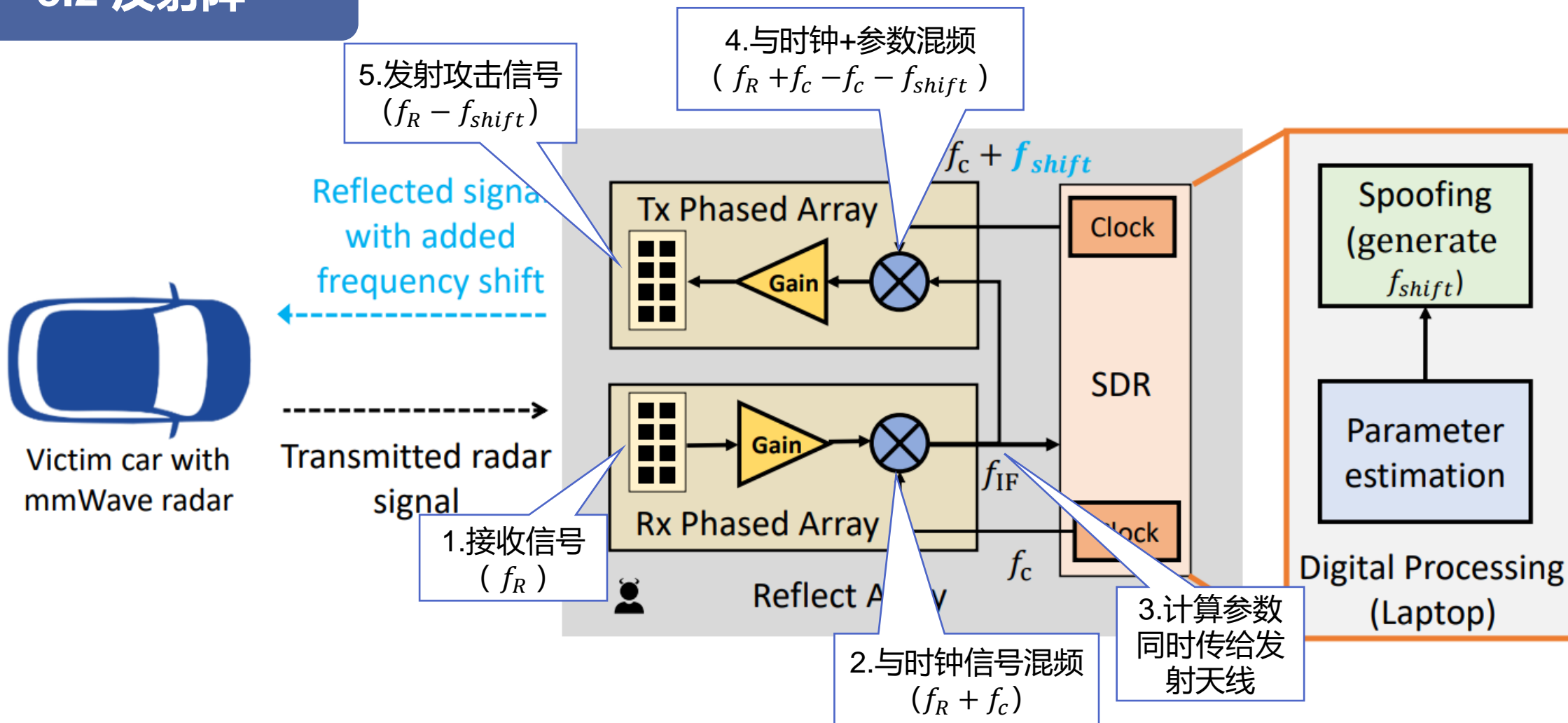
3.1 核心思想



无法欺骗
角度



3.2 反射阵

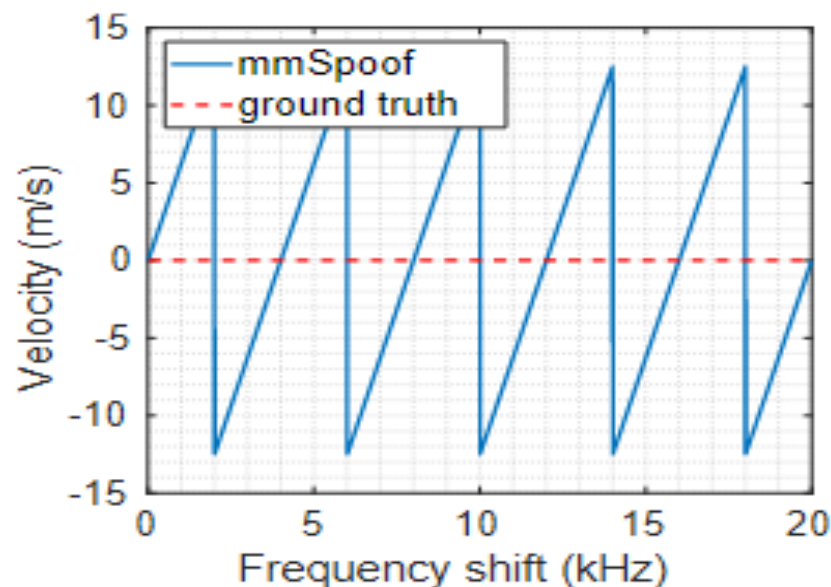




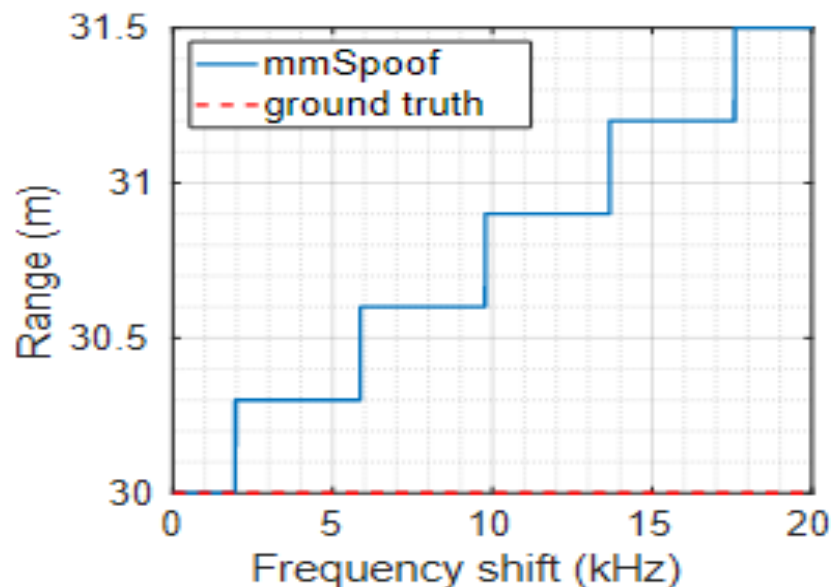
3.3 解耦

f_{shift} 同时影响 v 和 d ，如果想进行有效攻击，需要解除速度和距离之间的耦合，独立地欺骗速度和距离。

$$\Delta v = \frac{c}{2f_0} f_{shift}$$



$$\Delta d = \frac{c}{2k} f_{shift}$$



距离分辨率需要
 $\Delta f > \frac{1}{T}$

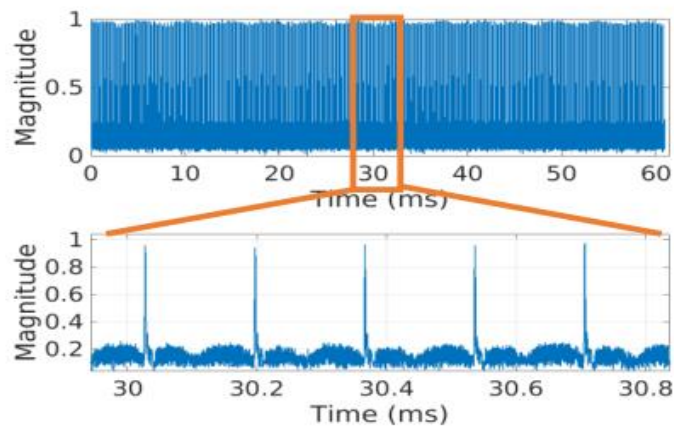
令 $f_{shift} = n \frac{1}{T}$ ，当 n 在两个整数之间变化时，只有 Δv 变化，当 n 为正整数时， Δd 跳变

3.4 参数估计

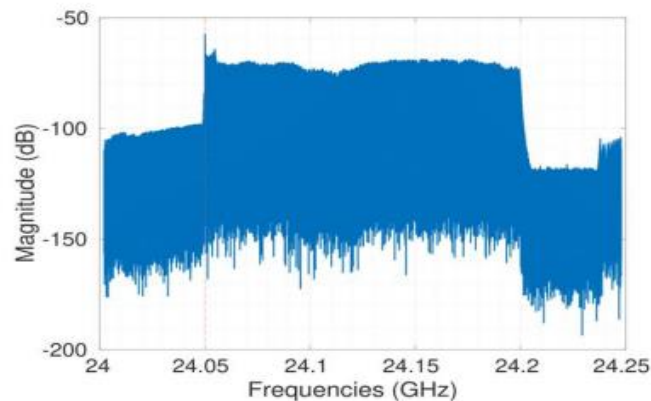
估计雷达的起始频率、斜率和啁啾周期，用于计算 f_{shift} 。

Parameter
estimation

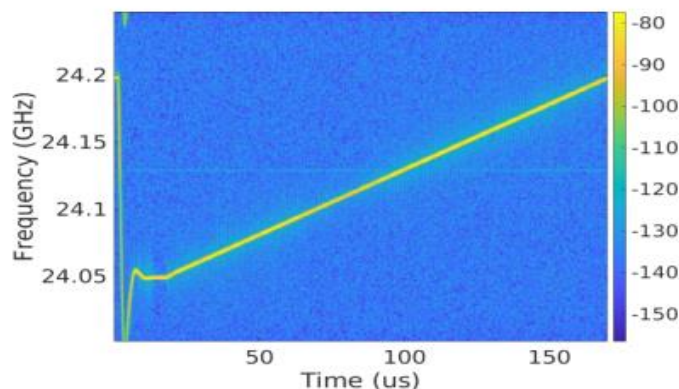
Digital Processing



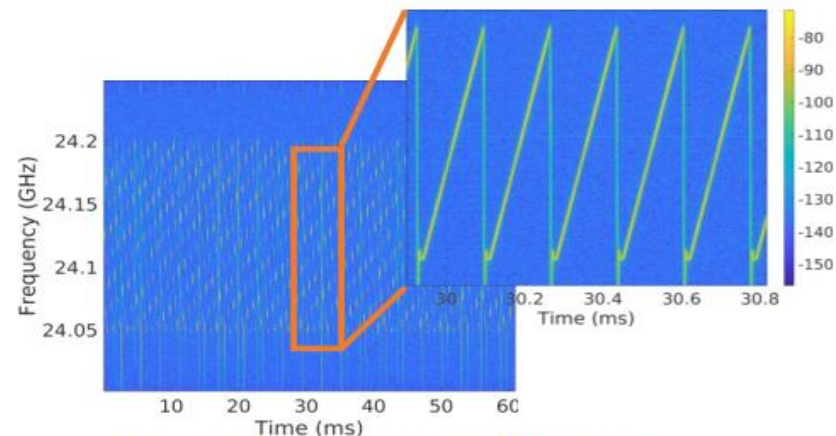
Step3: Chirp time estimation



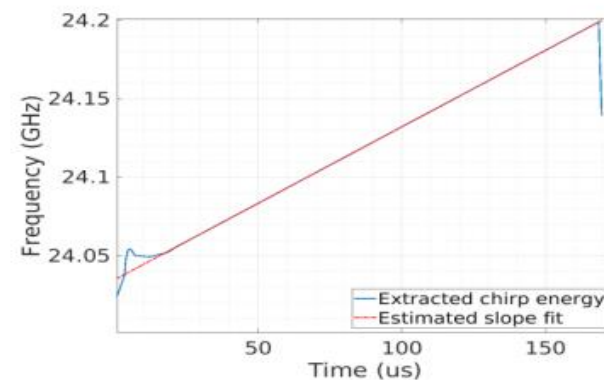
Step1: Start frequency estimation



Step4: Extraction of single chirp



Step2: Extracting FMCW chirps



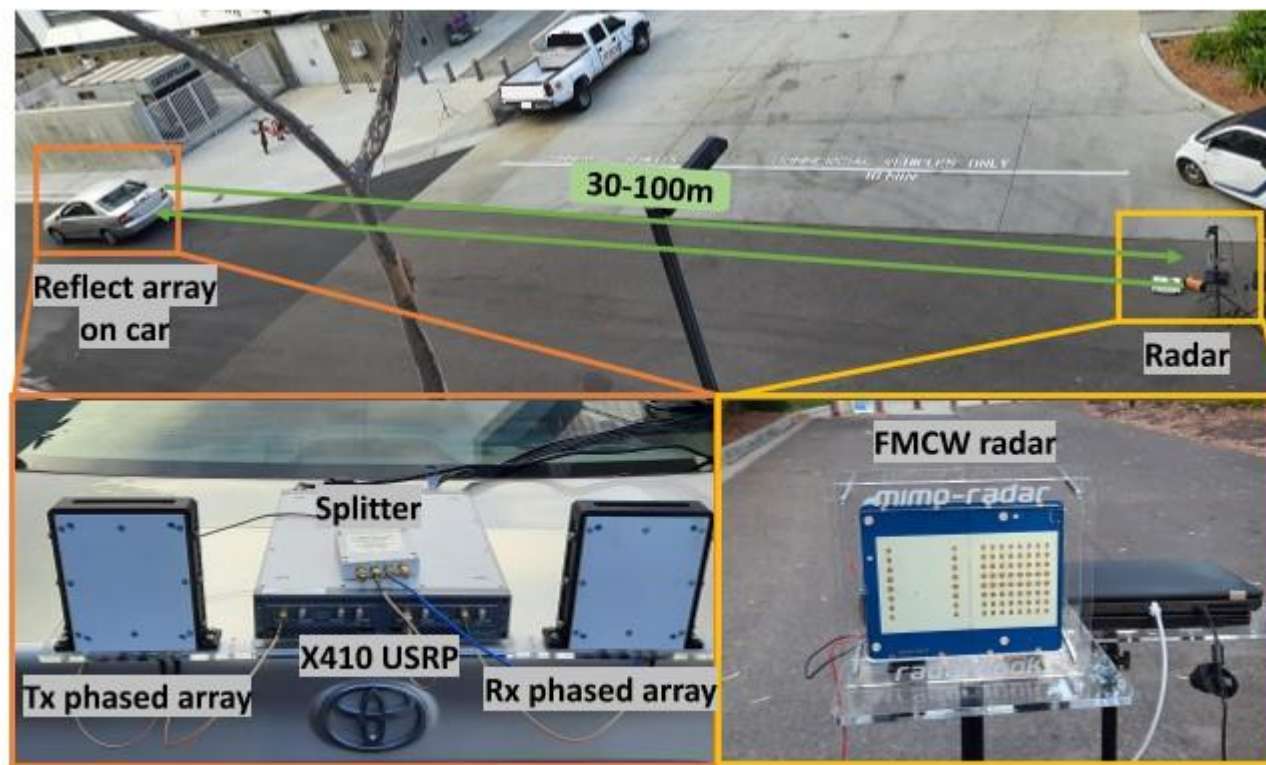
Step5: Slope Estimation



第四部分 实验结果

4.1 实验设置

FMCW雷达固定在原地，反射阵列安装于汽车上，分别进行静态和动态实验。



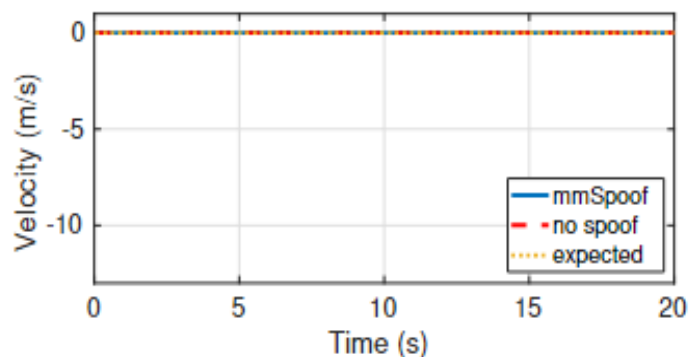
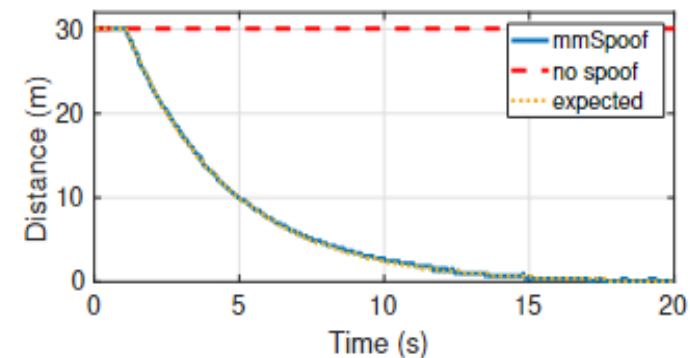


4.实验结果

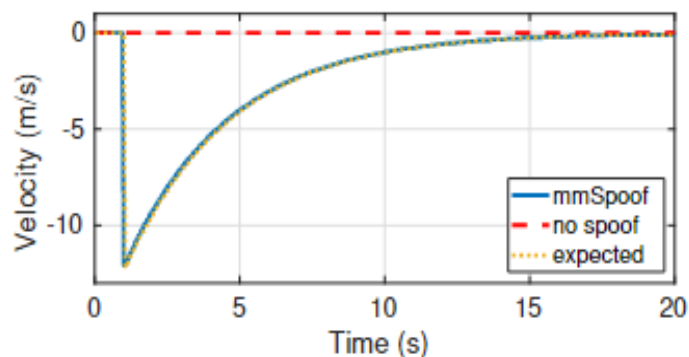
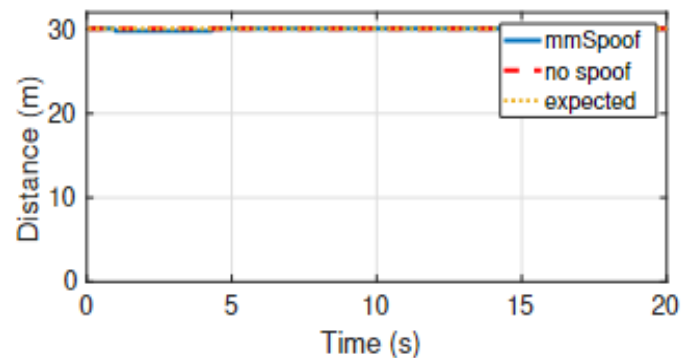


4.2 静态实验

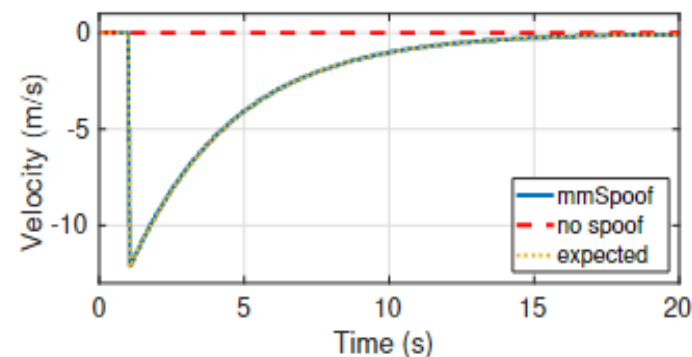
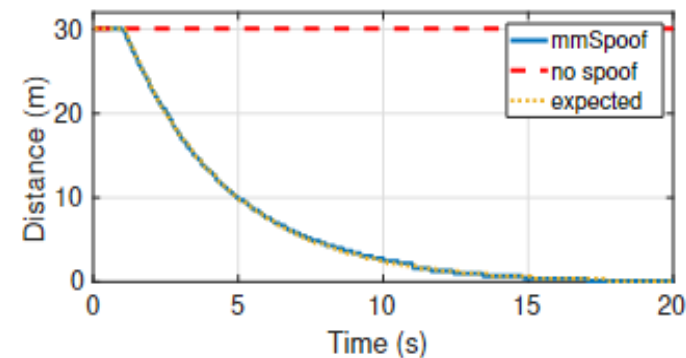
攻击者和受害者之间没有相对速度。



(a) 只欺骗距离



(b) 只欺骗速度



(c) 同时欺骗

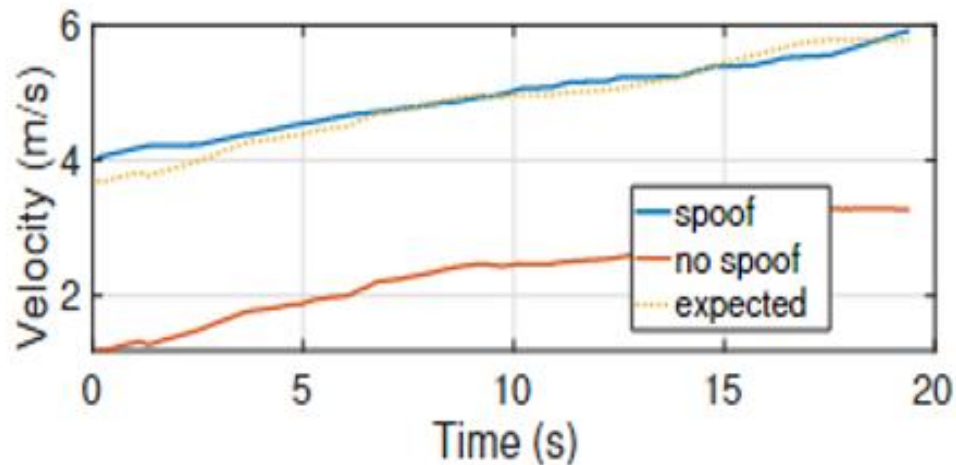
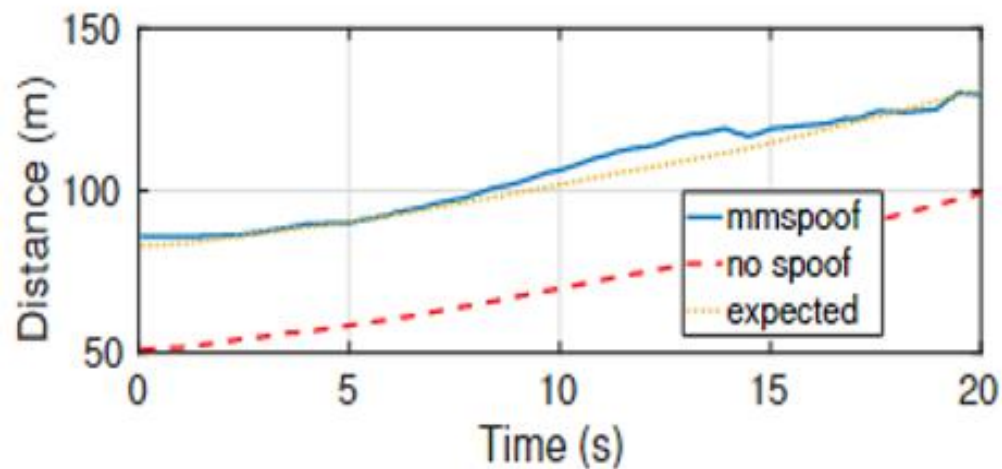


4.实验结果



4.3 动态实验

攻击者和受害者之间存在相对速度。



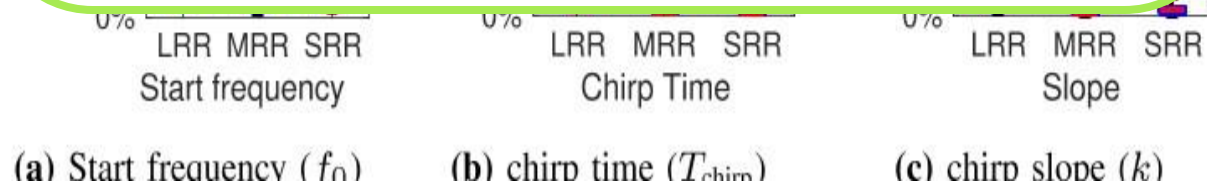
没有相对运动时，相位差可以由相位的累积来近似

$$f'_d = \frac{\Delta\varphi'}{LT_{chirp}} = \frac{\int_0^{LT_{chirp}} f'_b dt}{LT_{chirp}} = \frac{\Delta\varphi + f_{shift} LT_{chirp}}{LT_{chirp}} = f_d + f_{shift}$$

但是存在相对运动时，上式近似结果偏差较大

$$\Delta v = \frac{c}{2f_0} f_{shift}$$

真实的 Δv 与上式之间存在偏差

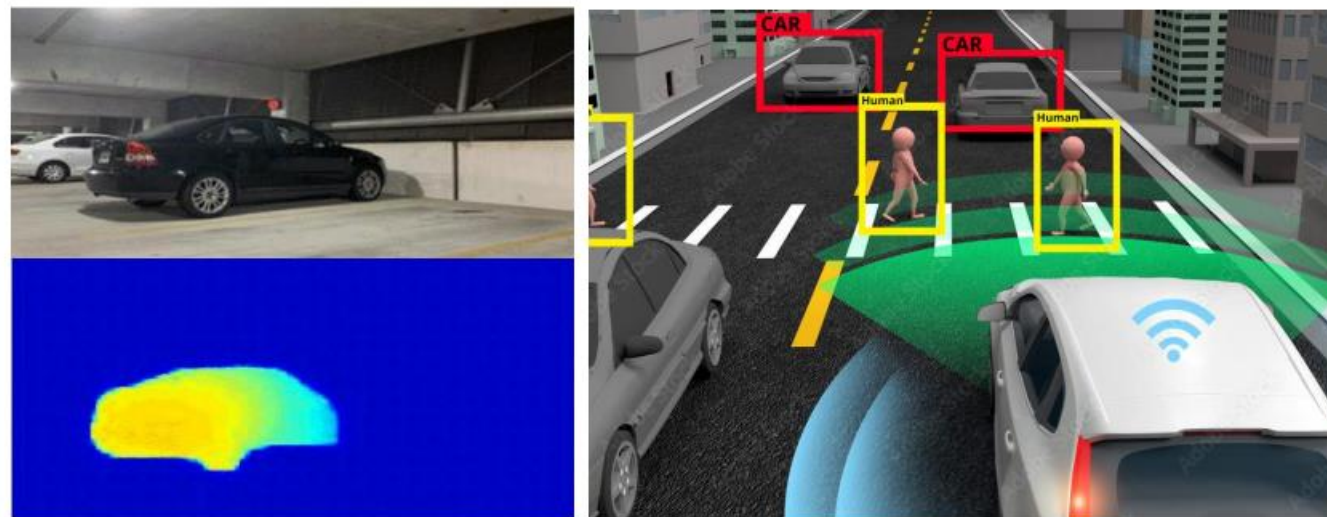




第五部分 总结与展望

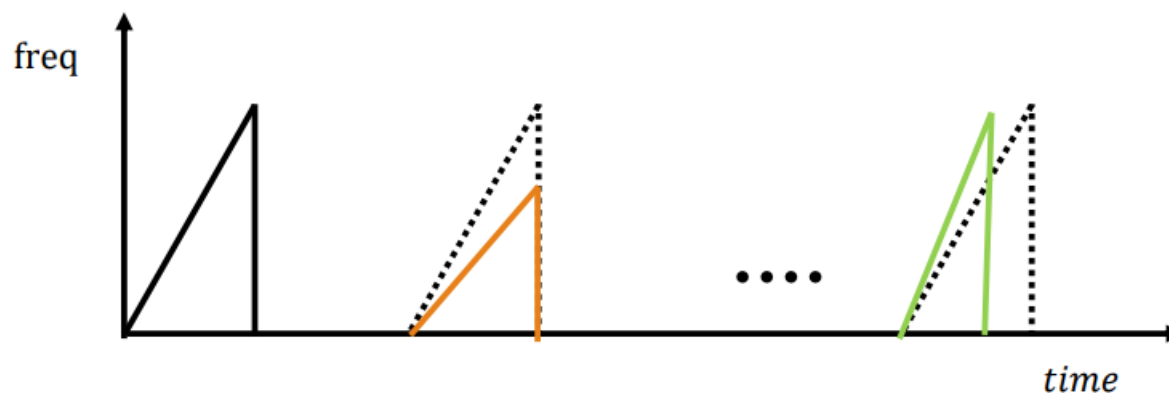


本文提出的基于反射阵列的弹性欺骗方法，只修改了反射信号的频率，能够在没有任何先验知识的情况下进行欺骗，不需要同步，保留了信号调制，对许多抗攻击对策具有鲁棒性。



作者提出的限制或措施：

- 1、**无法欺骗角度**，ghost目标始终在反射阵列的方向上。
- 2、安全系统是一个**多传感器**组成的整体，仅对单一的FMCW雷达欺骗难以欺骗整个系统。
- 3、采用**高分辨率**3D成像雷达，可以识别mmspooof的ghost。
- 4、如果**雷达参数**能以比攻击者参数估计**更快的速度变化**，可以使得mmspooof无效。






南京邮电大学

请各位老师批评指正

 汇报人：韩科爽

 指导教师：张品昌