NDSS SYMPOSIUM

MetaWave: Attacking mmWave Sensing with Meta-material-enhanced Tags

Xingyu Chen*, Zhengxiong Li*, Baicheng Chen*,

Yi Zhu, Chris Xiaoxuan Lu, Zhengyu Peng, Feng Lin,
Wenyao Xu, Kui Ren, Chunming Qiao

University of Colorado Denver · UC San Diego · University at Buffalo · THE UNIVERSITY of EDINBURGH · 浙江大學 ZHEJIANG UNIVERSITY

Introduction

- Millimeter Wave (mmWave) Sensing

Autonomous Vehicle

Delivery Robot

Automated Forklift

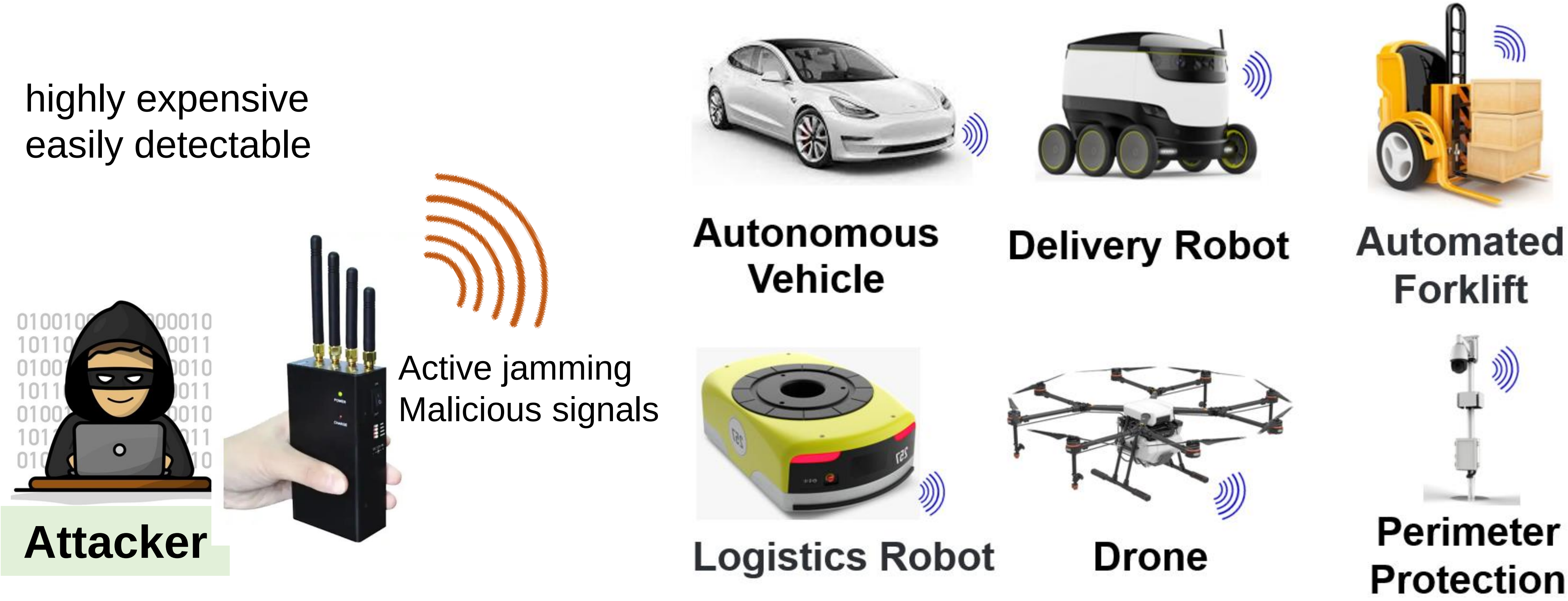
Logistics Robot

Drone

Perimeter Protection

Introduction

- mmWave Attacks

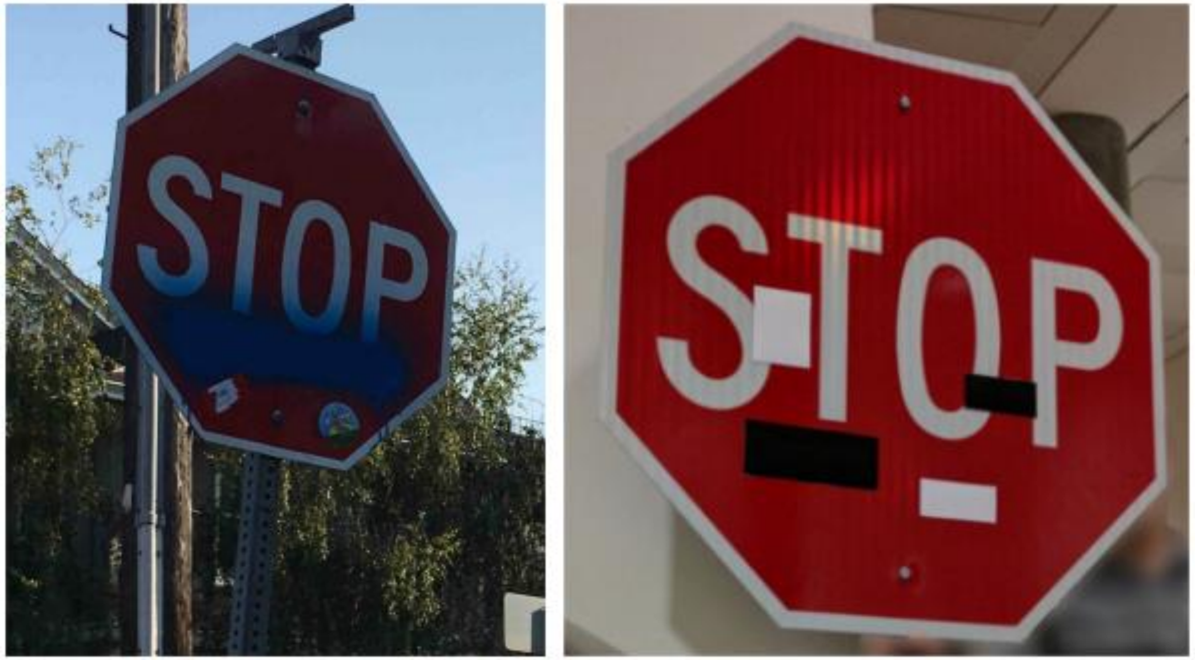


highly expensive
easily detectable

Active jamming
Malicious signals

Introduction

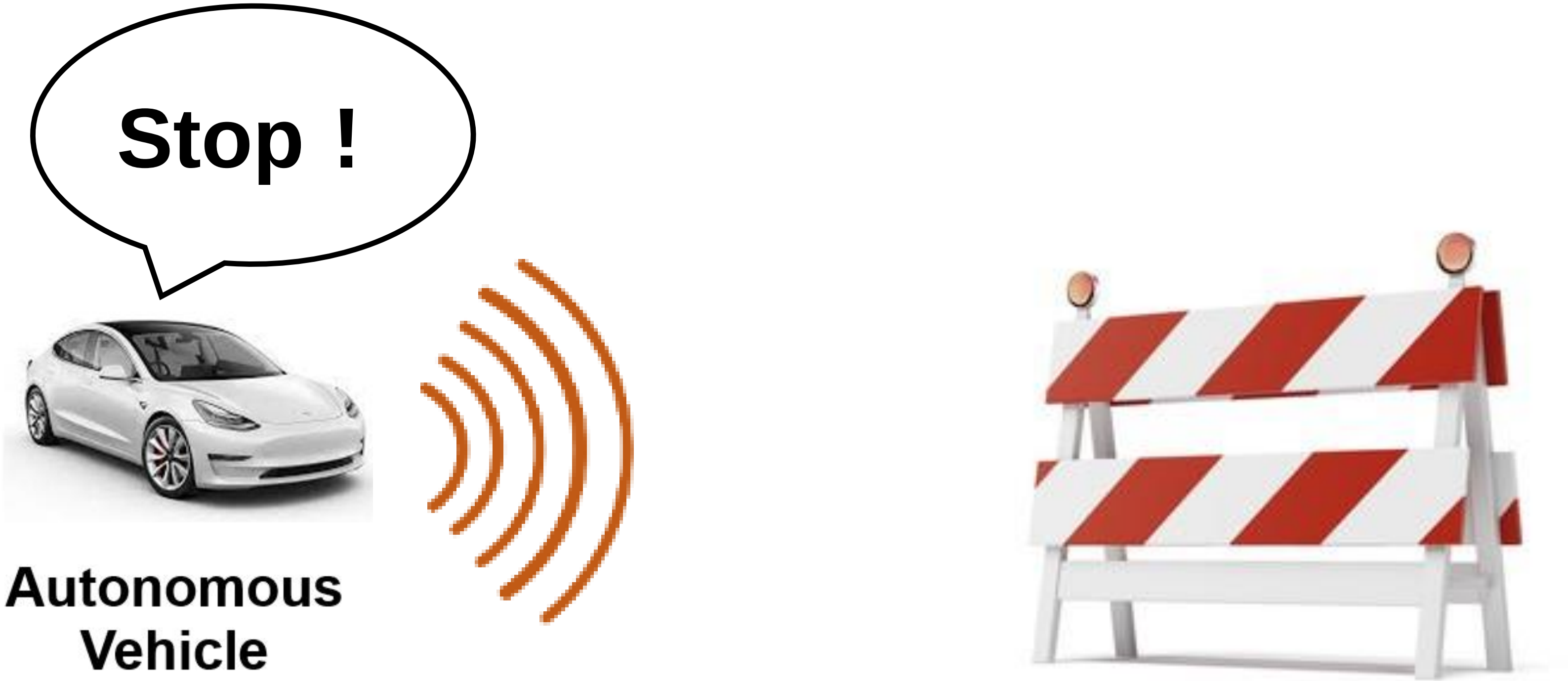
- How to we attack the sensor passively?



* Eykholt, Kevin, et al. "Robust physical-world attacks on deep learning visual classification", CVPR 2018

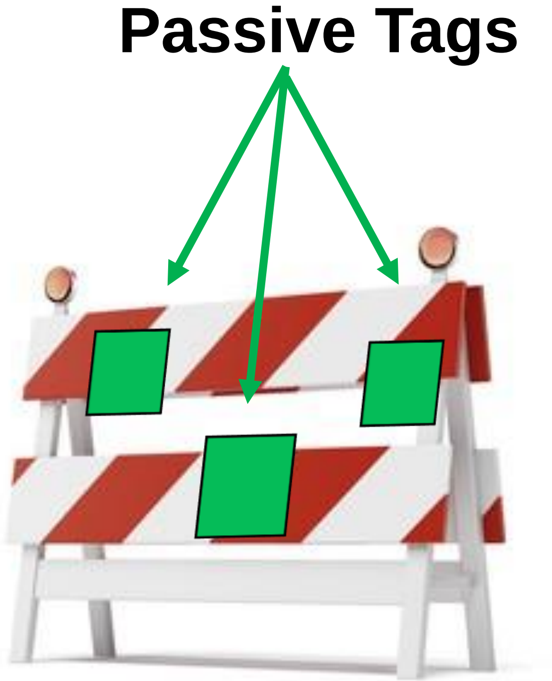
Introduction

- How to we attack the sensor passively?



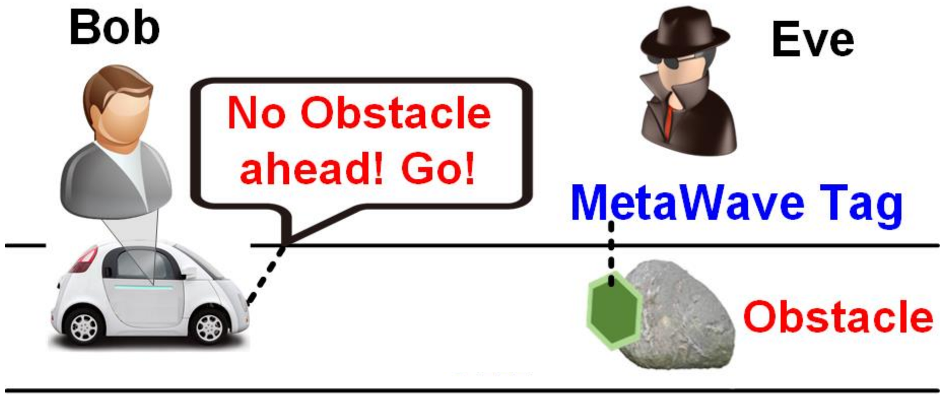
Introduction

- How to we attack the sensor passively?

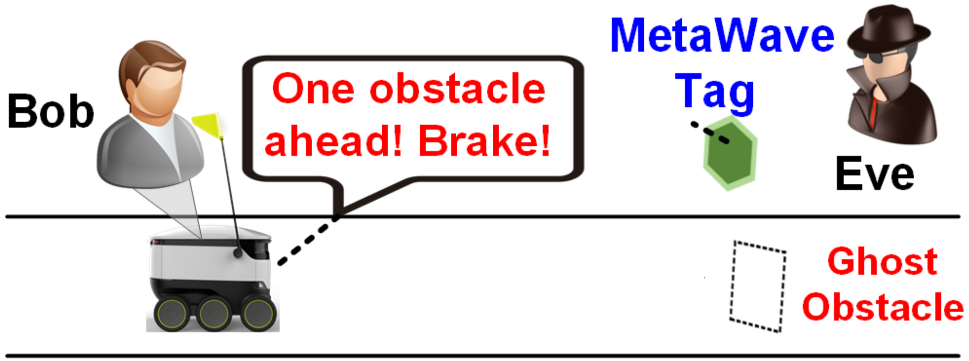


Threat Model

- Vanish Attack



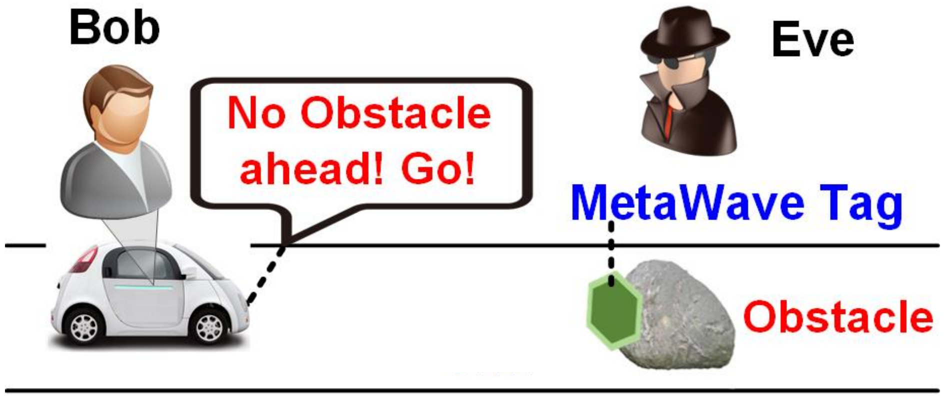
- Ghost Attack



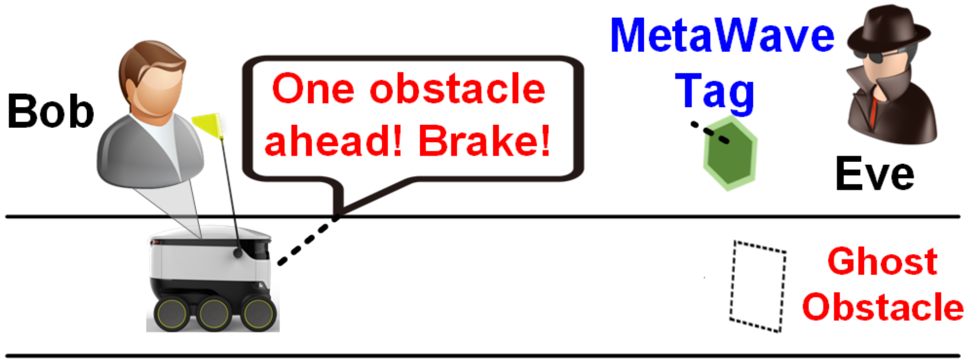
- Passive Attack
  - Security check
  - Prevent suspicious equipment's
- Practical
  - No access or modification the victim's hardware
- Black Box
  - No access to the details of the sensing algorithms

Threat Model

- Vanish Attack



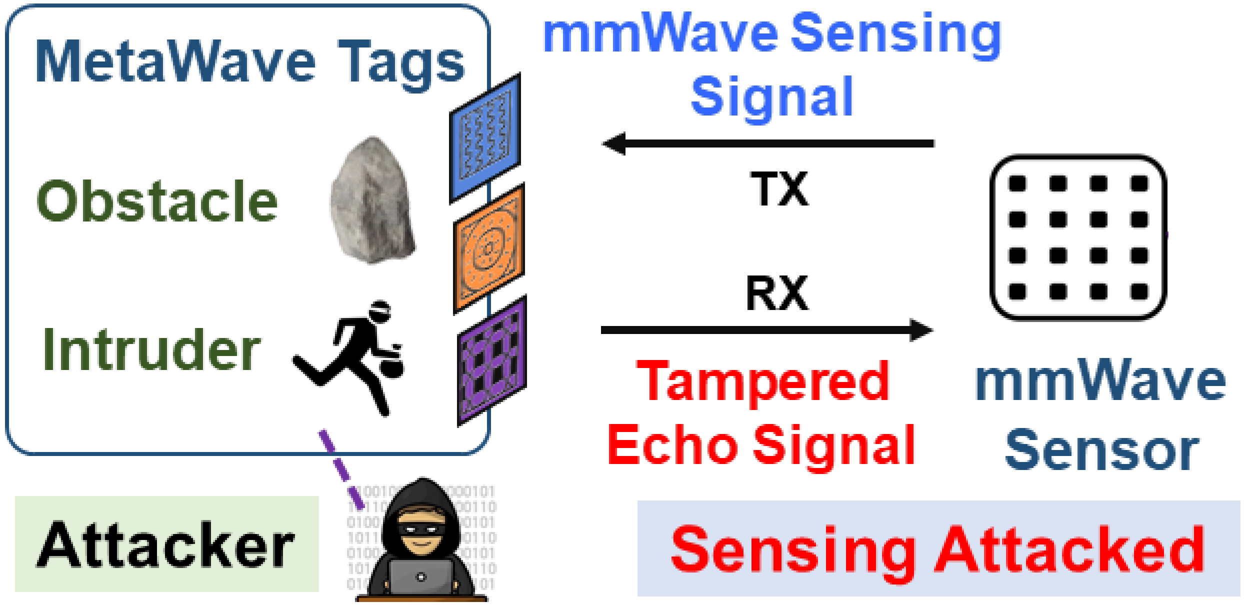
- Ghost Attack



- Passive Attack
  - Security check
  - Prevent suspicious equipment's
- Practical
  - No access or modification the victim's hardware
- Black Box
  - No access to the details of the sensing algorithms

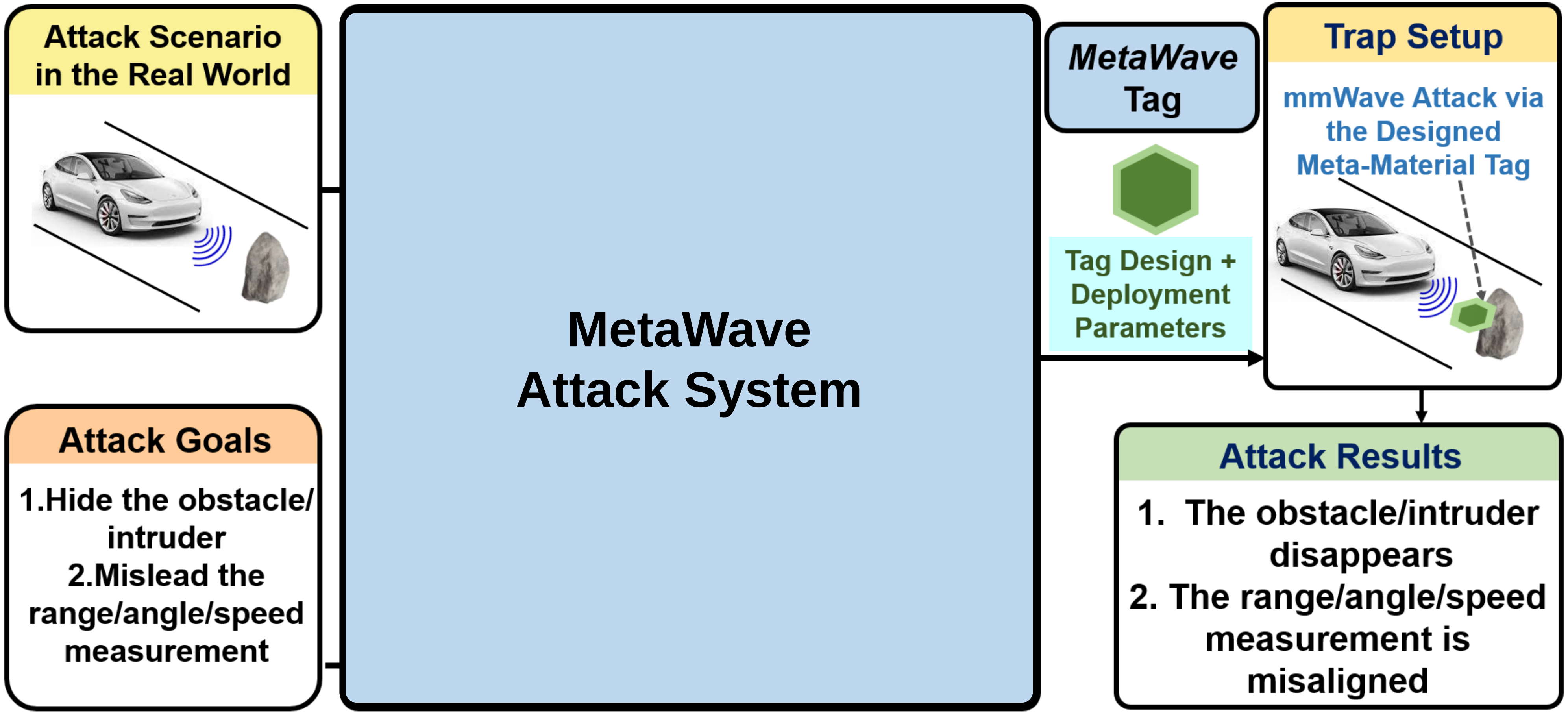
Introduction

- mmWave Attack using passive meta-material tags



Introduction

- mmWave Attack using passive meta-material tags



Attack Scenario in the Real World

Attack Goals

1.Hide the obstacle/ intruder

2.Mislead the range/angle/speed measurement

MetaWave Attack System

MetaWave Tag

Tag Design + Deployment Parameters

Trap Setup

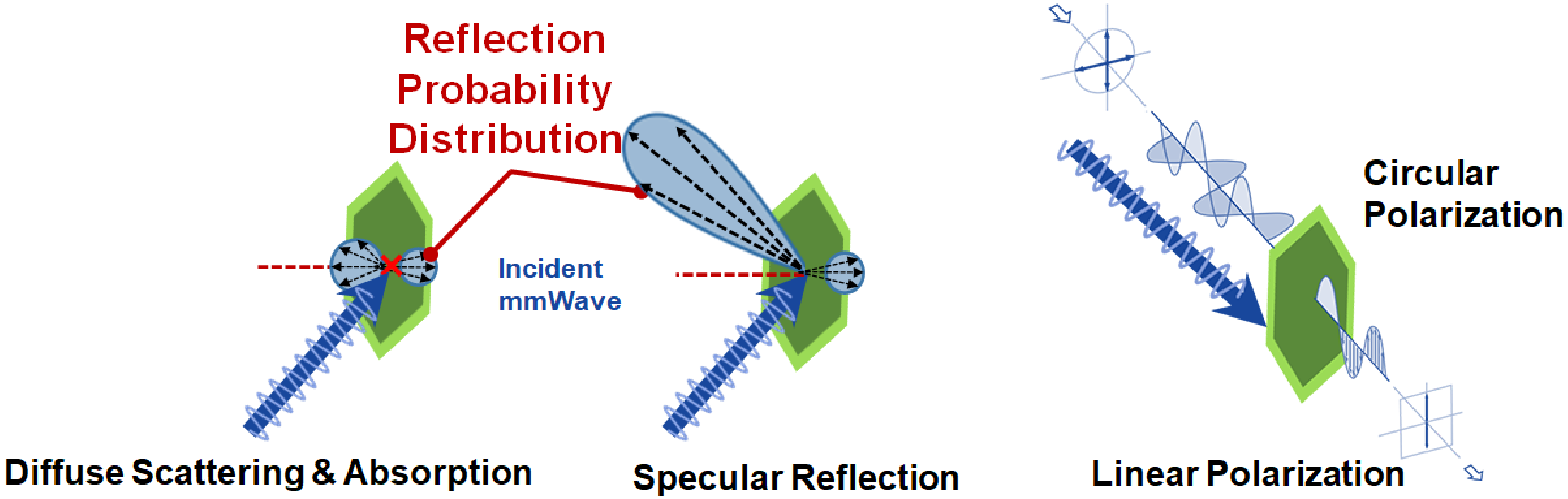
mmWave Attack via the Designed Meta-Material Tag

Attack Results

1. The obstacle/intruder disappears
2. The range/angle/speed measurement is misaligned

System Design

- Meta-material Tags



(a) Absorption Tag (b) Reflection Tag (c) Polarization Tag

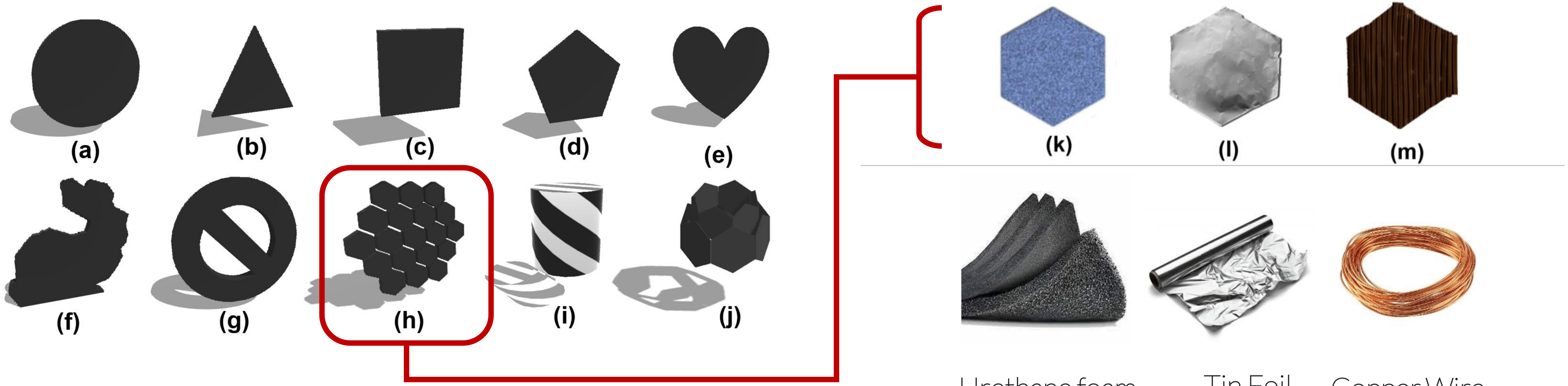
System Design

- ***MetaWave*** Tag Design

Absorption tag

Reflection tag

Polarization tag



Urethane foam

Tin Foil

Copper Wire

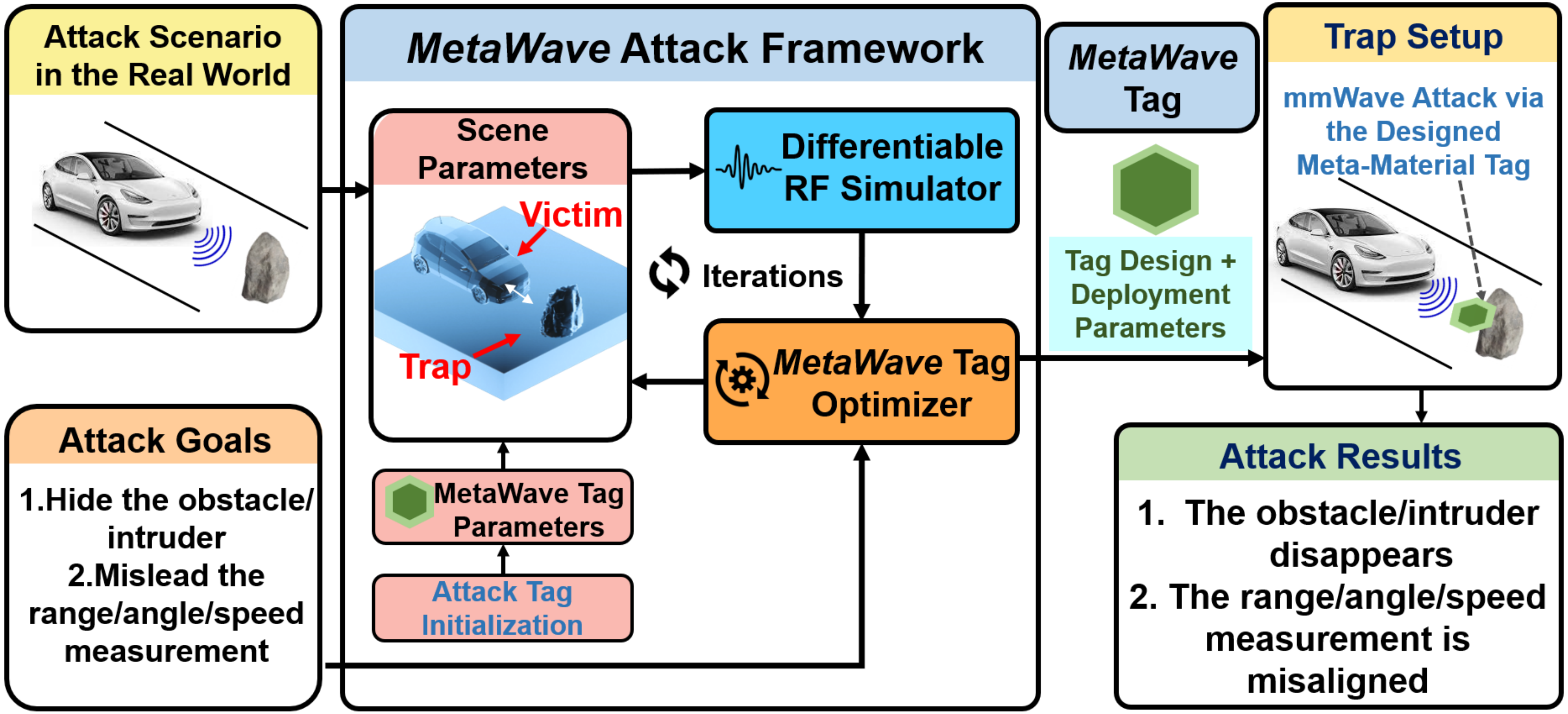
$10-30

$0.02

$9-16

System Design

- ***MetaWave*** Attack Framework Design



Attack Scenario in the Real World

MetaWave Attack Framework

Scene Parameters

Differentiable RF Simulator

Iterations

MetaWave Tag Optimizer

MetaWave Tag Parameters

Attack Tag Initialization

MetaWave Tag

Tag Design + Deployment Parameters

Trap Setup

mmWave Attack via the Designed Meta-Material Tag

Attack Goals

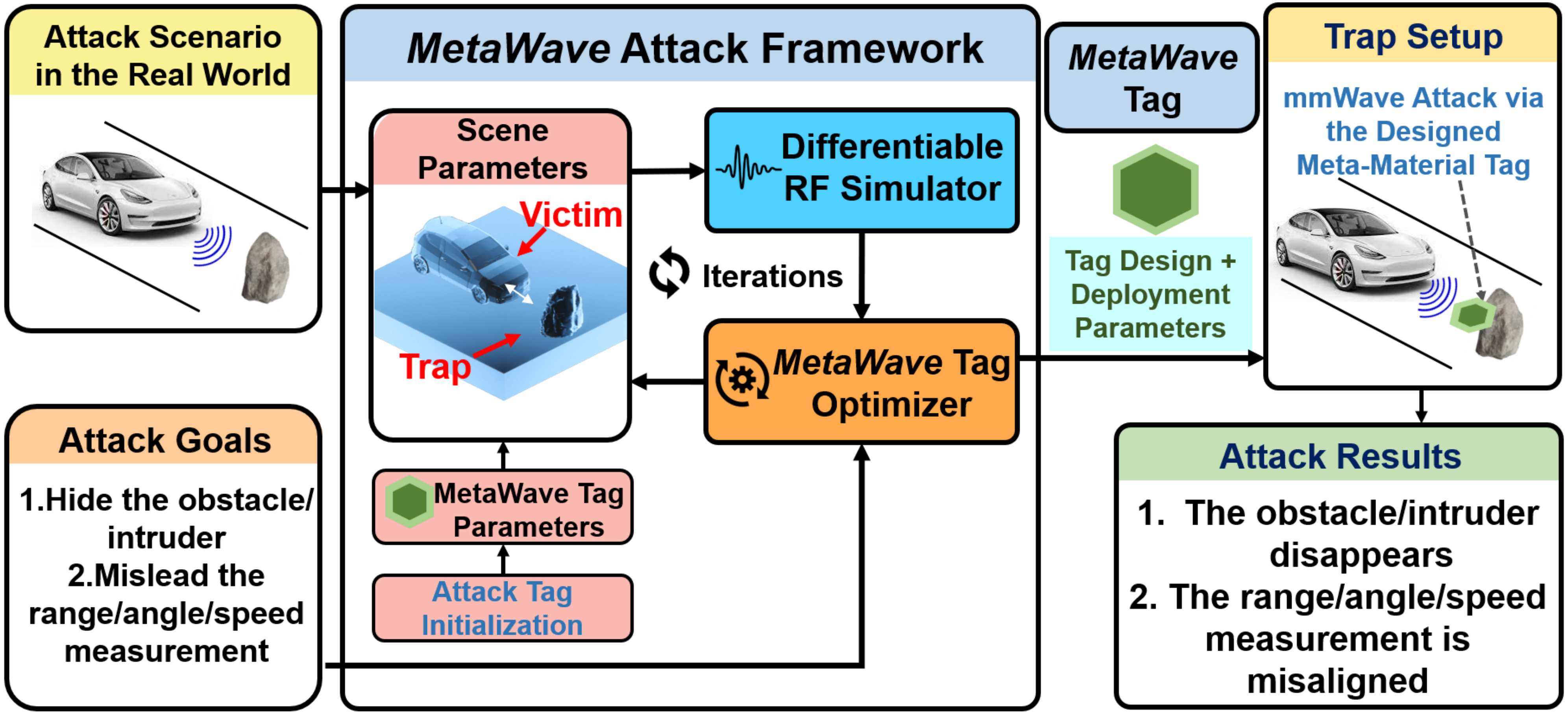
1.Hide the obstacle/ intruder
2.Mislead the range/angle/speed measurement

Attack Results

1. The obstacle/intruder disappears
2. The range/angle/speed measurement is misaligned

System Design

- ***MetaWave*** Attack Framework Design



Attack Scenario in the Real World

MetaWave Attack Framework

Scene Parameters

Differentiable RF Simulator

Iterations

MetaWave Tag Optimizer

MetaWave Tag Parameters

Attack Tag Initialization

MetaWave Tag

Tag Design + Deployment Parameters

Trap Setup

mmWave Attack via the Designed Meta-Material Tag

Attack Goals

1.Hide the obstacle/ intruder
2.Mislead the range/angle/speed measurement

Attack Results

1. The obstacle/intruder disappears
2. The range/angle/speed measurement is misaligned

Attack System Integration

Scene Parameters

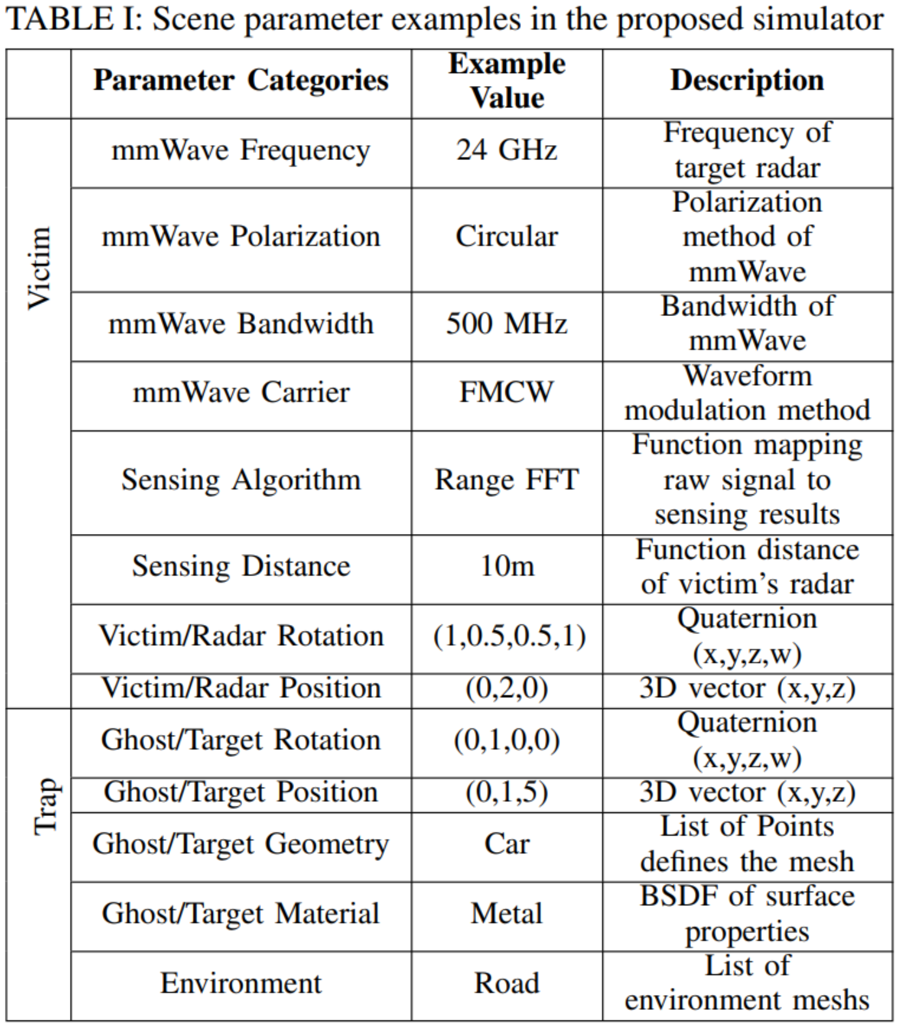


TABLE I: Scene parameter examples in the proposed simulator

	Parameter Categories	Example Value	Description
Victim	mmWave Frequency	24 GHz	Frequency of target radar
	mmWave Polarization	Circular	Polarization method of mmWave
	mmWave Bandwidth	500 MHz	Bandwidth of mmWave
	mmWave Carrier	FMCW	Waveform modulation method
	Sensing Algorithm	Range FFT	Function mapping raw signal to sensing results
	Sensing Distance	10m	Function distance of victim's radar
	Victim/Radar Rotation	(1,0.5,0.5,1)	Quaternion (x,y,z,w)
	Victim/Radar Position	(0,2,0)	3D vector (x,y,z)
Trap	Ghost/Target Rotation	(0,1,0,0)	Quaternion (x,y,z,w)
	Ghost/Target Position	(0,1,5)	3D vector (x,y,z)
	Ghost/Target Geometry	Car	List of Points defines the mesh
	Ghost/Target Material	Metal	BSDF of surface properties
	Environment	Road	List of environment meshs

Tag Parameters

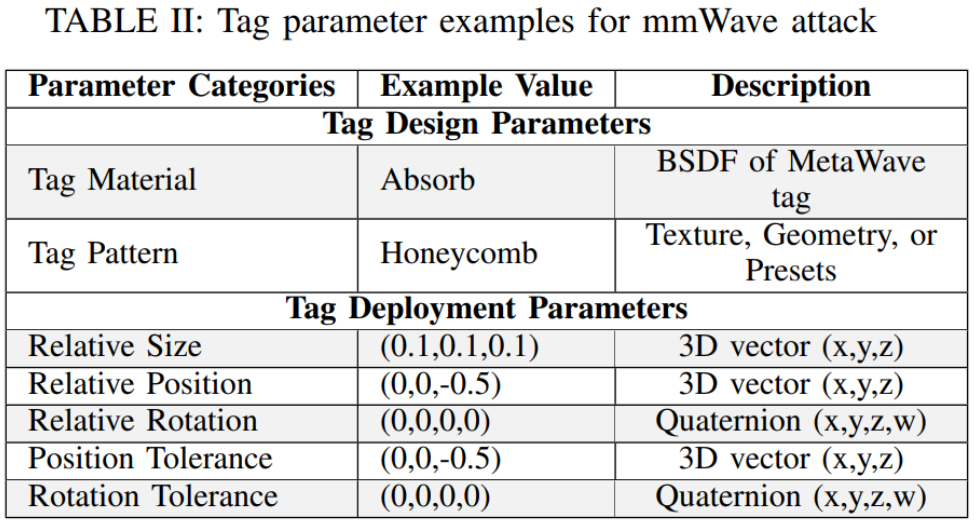


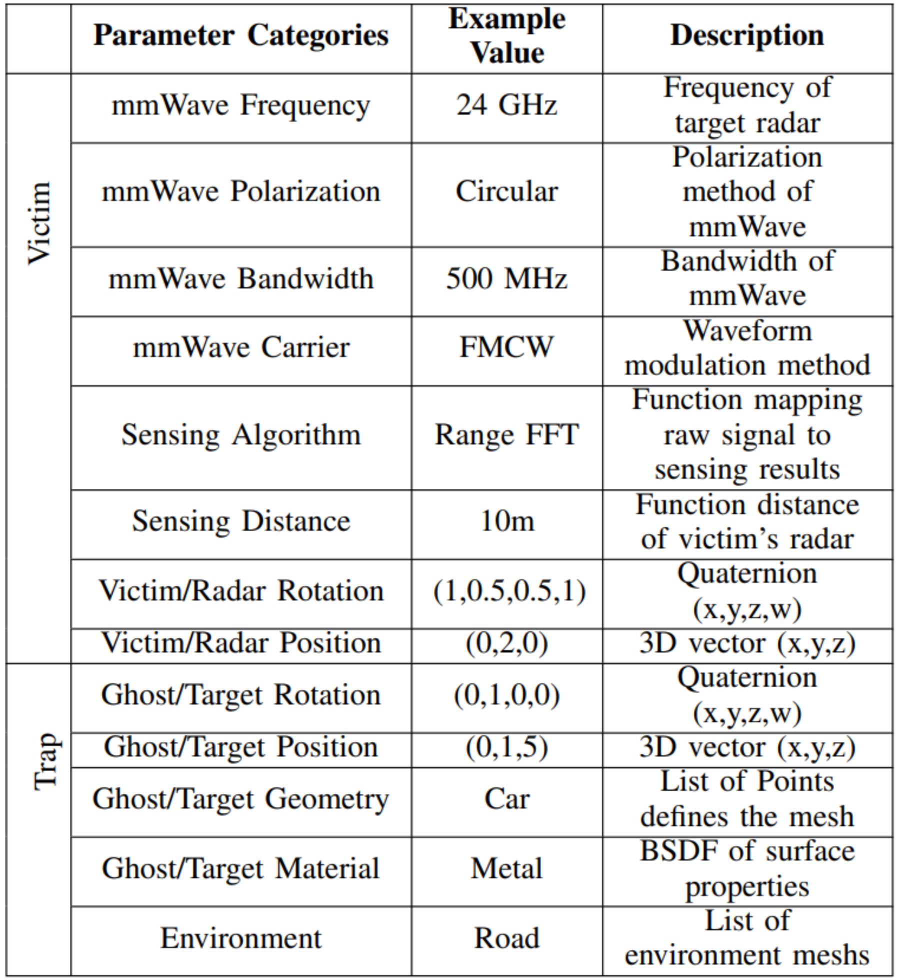
TABLE II: Tag parameter examples for mmWave attack

Parameter Categories	Example Value	Description
Tag Design Parameters		
Tag Material	Absorb	BSDF of MetaWave tag
Tag Pattern	Honeycomb	Texture, Geometry, or Presets
Tag Deployment Parameters		
Relative Size	(0.1,0.1,0.1)	3D vector (x,y,z)
Relative Position	(0,0,-0.5)	3D vector (x,y,z)
Relative Rotation	(0,0,0,0)	Quaternion (x,y,z,w)
Position Tolerance	(0,0,-0.5)	3D vector (x,y,z)
Rotation Tolerance	(0,0,0,0)	Quaternion (x,y,z,w)

Attack System Integration

Scene Parameters

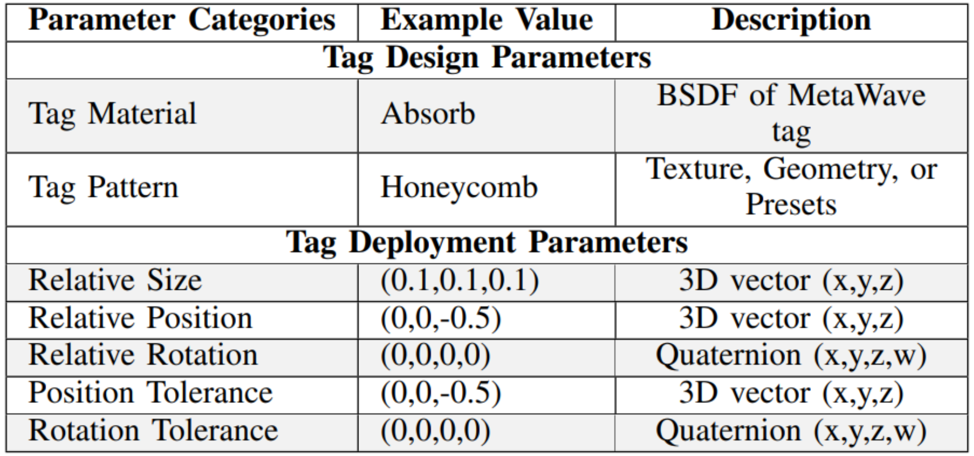
TABLE I: Scene parameter examples in the proposed simulator



	Parameter Categories	Example Value	Description
Victim	mmWave Frequency	24 GHz	Frequency of target radar
	mmWave Polarization	Circular	Polarization method of mmWave
	mmWave Bandwidth	500 MHz	Bandwidth of mmWave
	mmWave Carrier	FMCW	Waveform modulation method
	Sensing Algorithm	Range FFT	Function mapping raw signal to sensing results
	Sensing Distance	10m	Function distance of victim's radar
	Victim/Radar Rotation	(1,0.5,0.5,1)	Quaternion (x,y,z,w)
	Victim/Radar Position	(0,2,0)	3D vector (x,y,z)
Trap	Ghost/Target Rotation	(0,1,0,0)	Quaternion (x,y,z,w)
	Ghost/Target Position	(0,1,5)	3D vector (x,y,z)
	Ghost/Target Geometry	Car	List of Points defines the mesh
	Ghost/Target Material	Metal	BSDF of surface properties
	Environment	Road	List of environment meshs

Tag Parameters

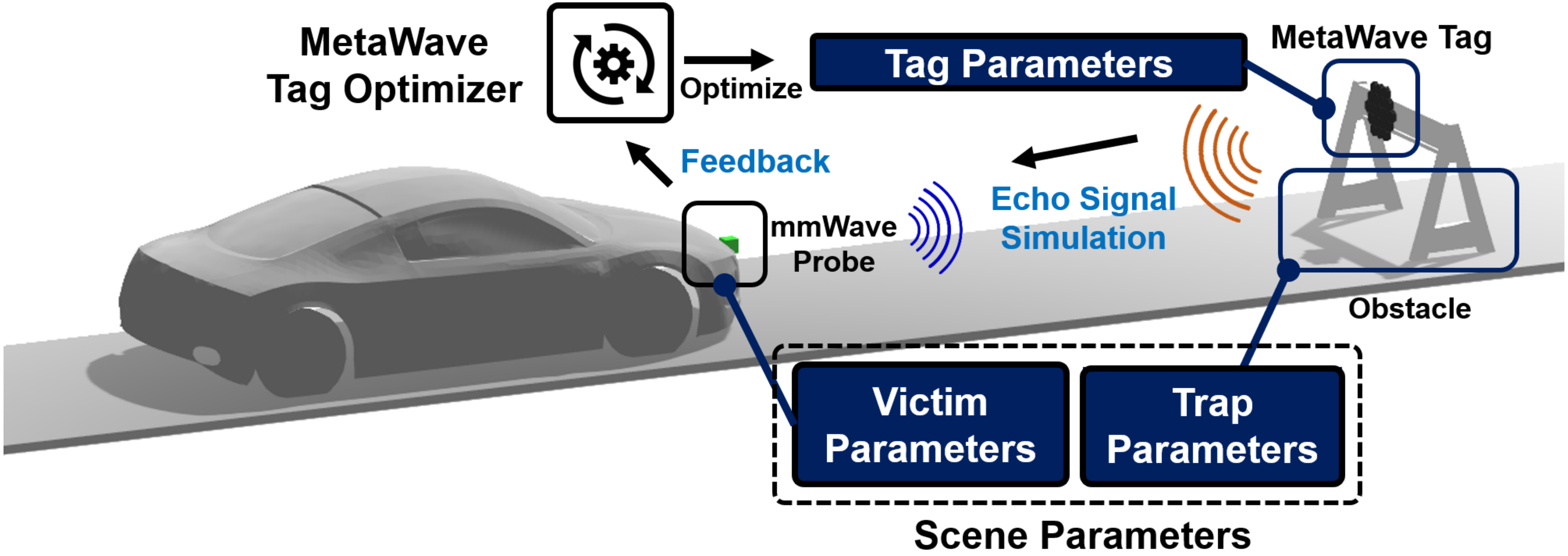
TABLE II: Tag parameter examples for mmWave attack



Parameter Categories	Example Value	Description
Tag Design Parameters		
Tag Material	Absorb	BSDF of MetaWave tag
Tag Pattern	Honeycomb	Texture, Geometry, or Presets
Tag Deployment Parameters		
Relative Size	(0.1,0.1,0.1)	3D vector (x,y,z)
Relative Position	(0,0,-0.5)	3D vector (x,y,z)
Relative Rotation	(0,0,0,0)	Quaternion (x,y,z,w)
Position Tolerance	(0,0,-0.5)	3D vector (x,y,z)
Rotation Tolerance	(0,0,0,0)	Quaternion (x,y,z,w)

Attack System Integration

- ***MetaWave*** Tag Advancement

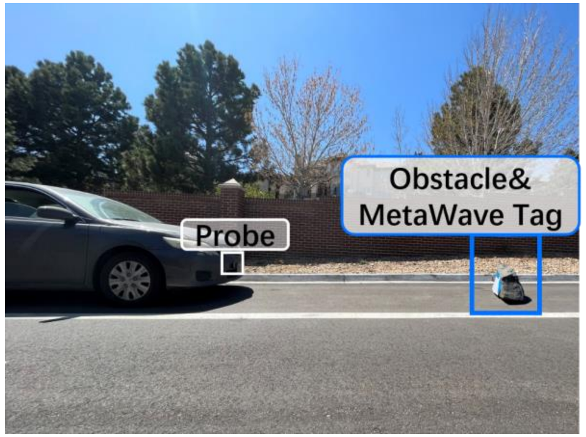


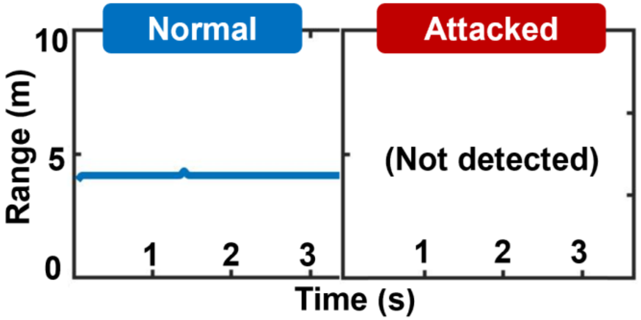
Practicality and Generalization Evaluation

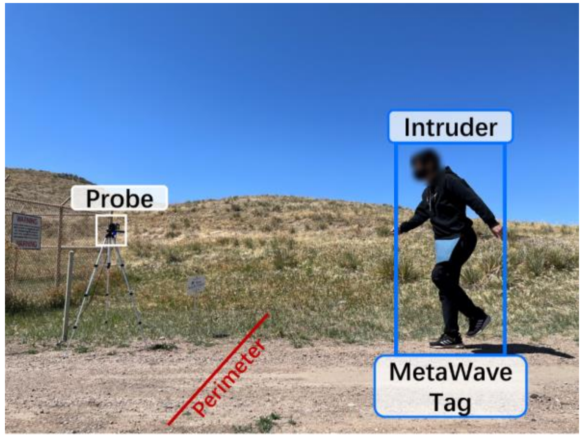
- Overall Performance
  - Attacking **Range** Measurements
    - **97%** attack success rate
  - Attacking **Angle** Measurements
    - **96%** attack success rate
  - Attacking **Speed** Measurements
    - **91%** attack success rate

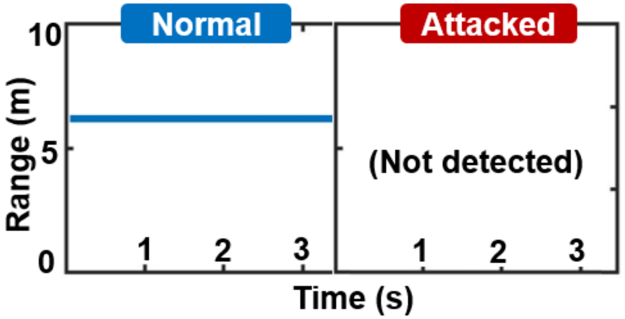
Real-World Attack Evaluation

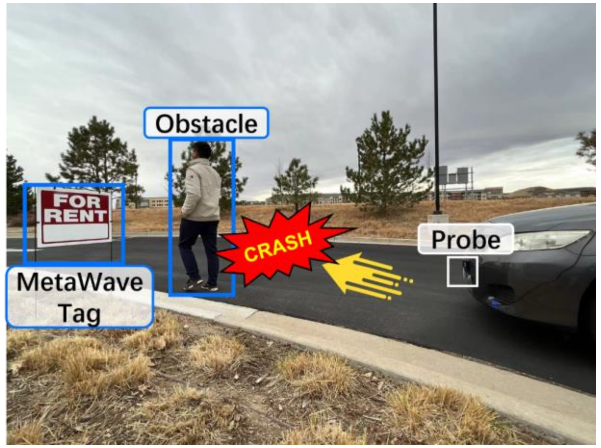
- Real-World Attack Results

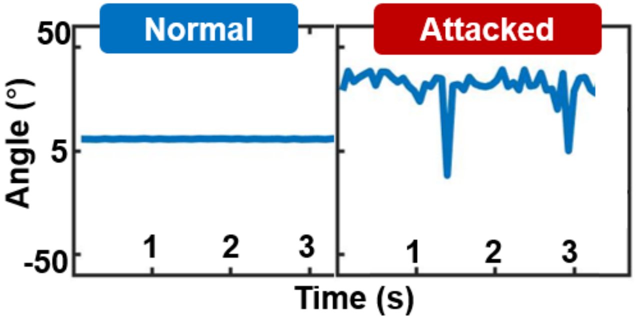


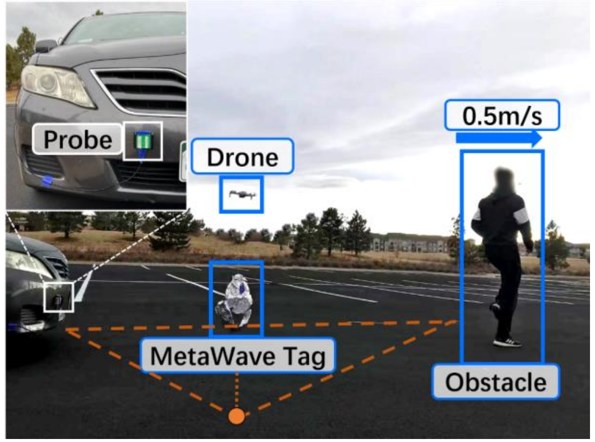


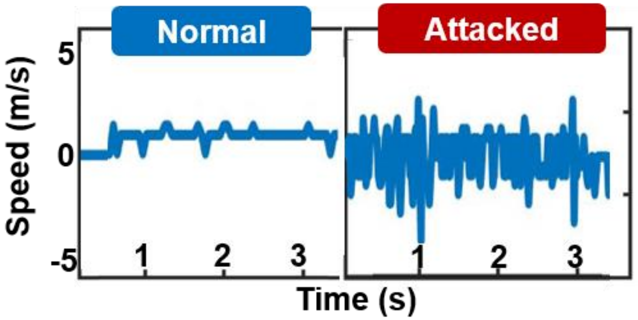






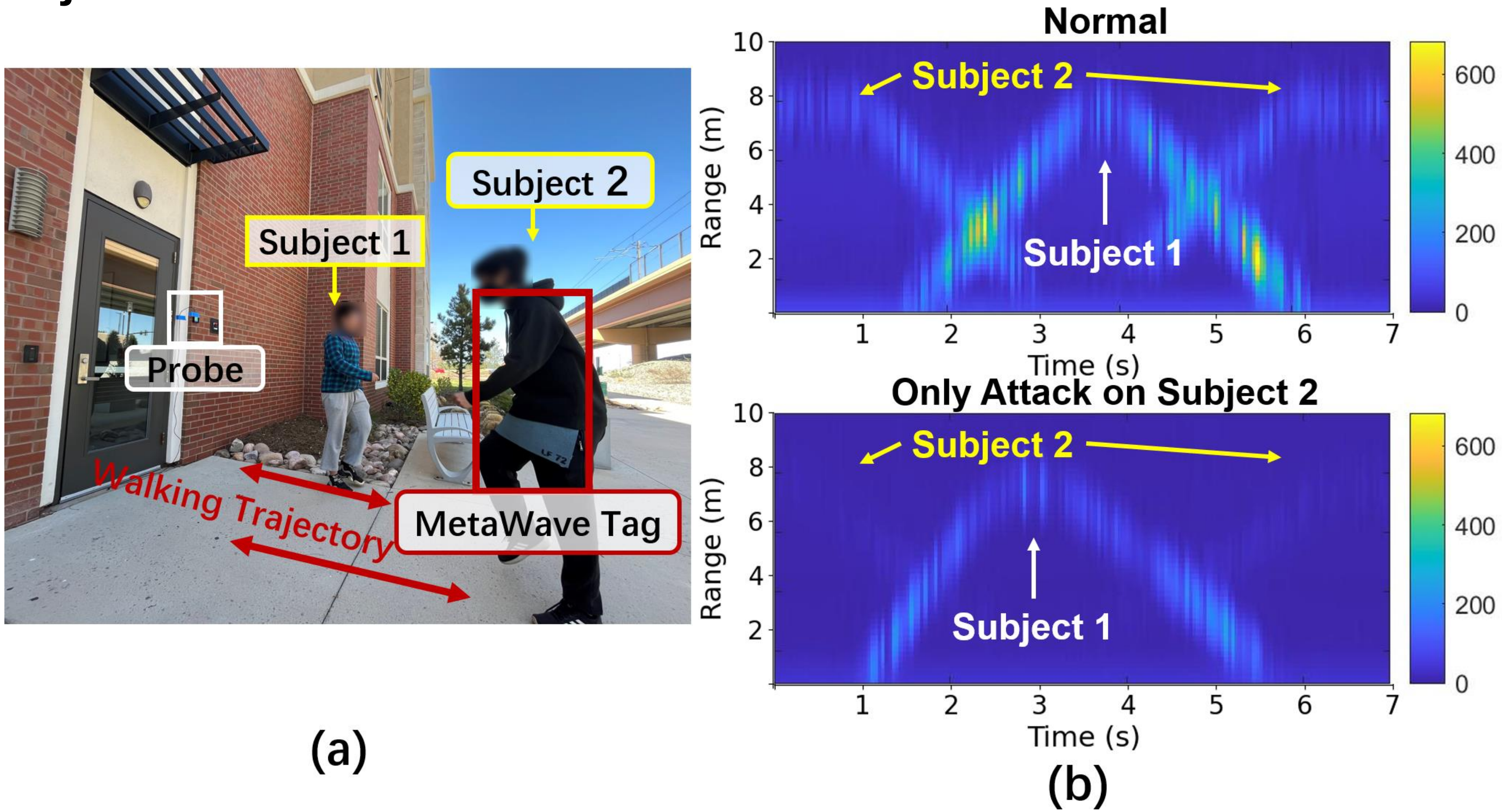






Real-World Attack Evaluation

- Multi-Object Attack

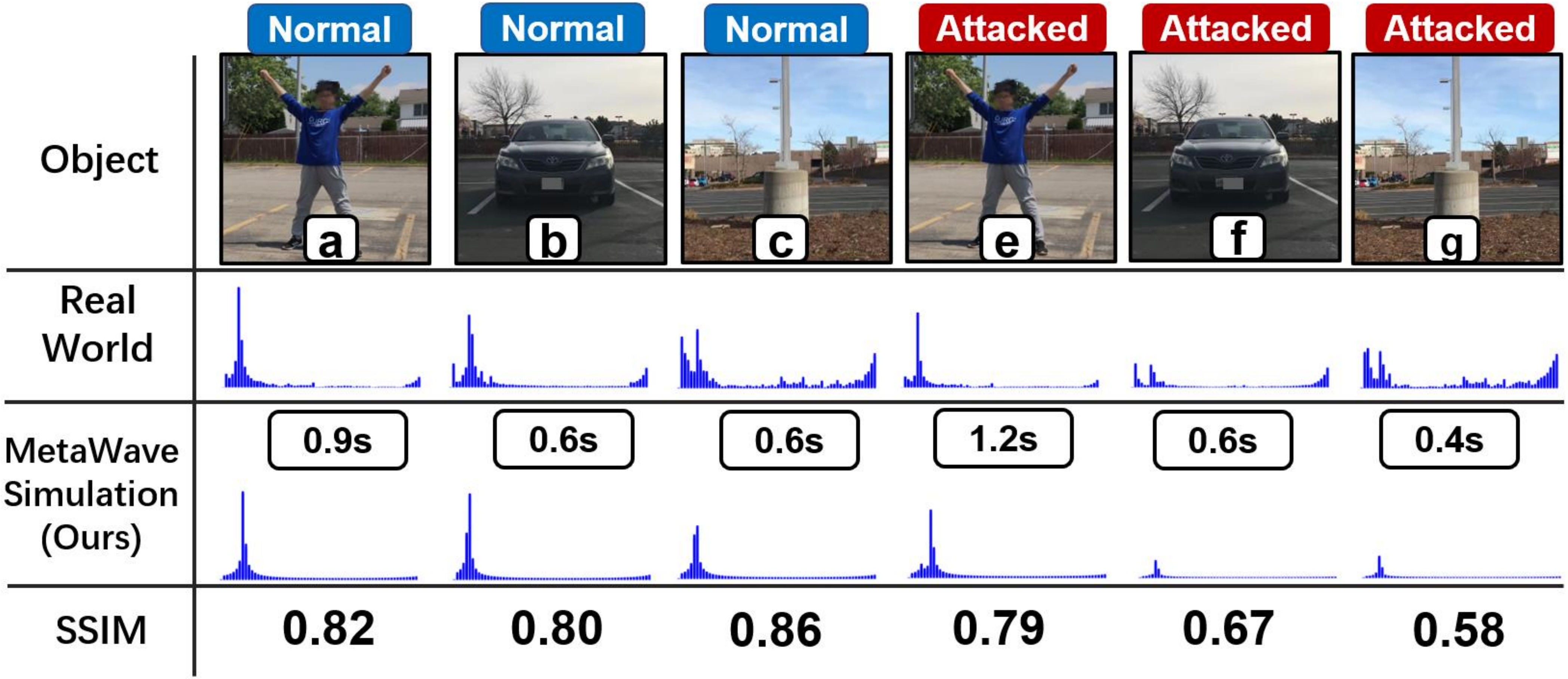


(a)

(b)

Simulator-Based Attack System Evaluation

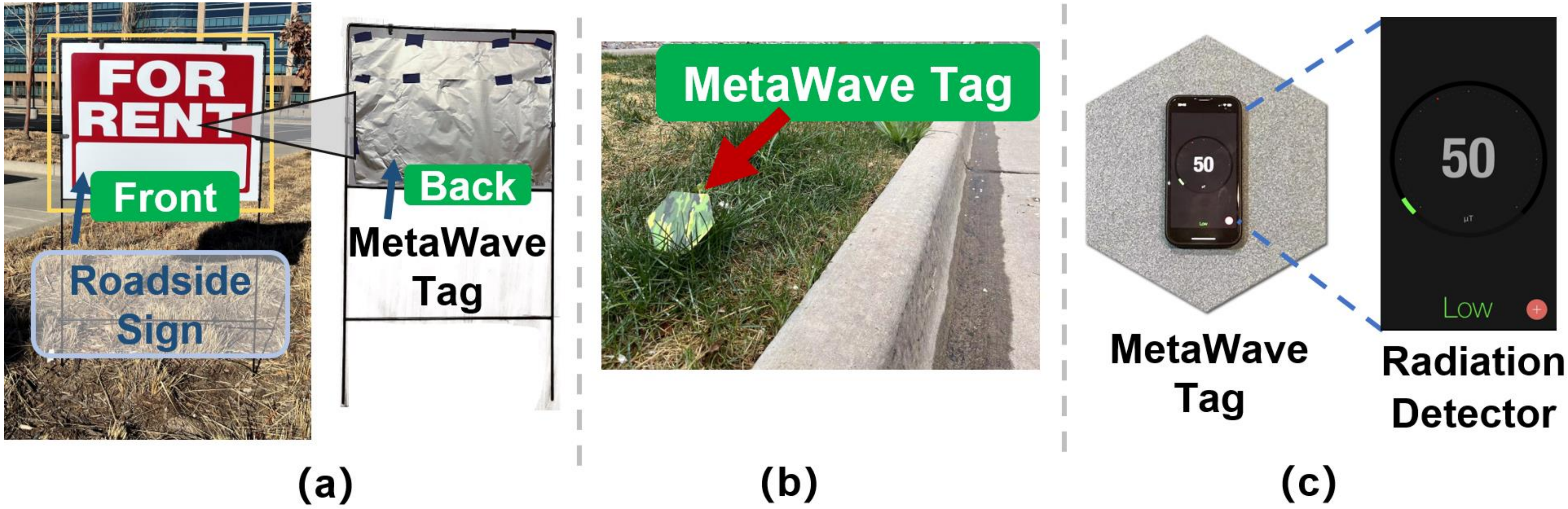
- System Simulation Performance



	Normal	Normal	Normal	Attacked	Attacked	Attacked
Object	a	b	c	e	f	g
Real World						
MetaWave Simulation (Ours)	0.9s	0.6s	0.6s	1.2s	0.6s	0.4s
SSIM	0.82	0.80	0.86	0.79	0.67	0.58

Countermeasures

- Security Check / Radiation Detection



Countermeasures

- **RF Fingerprinting**
  - Use the physical characteristics to judge if the echo signal comes from the same hardware
  - It can be used to detect malicious signal, but not passive tags.
- False Alarm Detection
  - Constant False-Alarm Rate (CFAR) technology
  - Meta-material tags to change the echo signal along with the environment
- Multi-sensor
  - Employ different mmWave sensors operating under different sensing frequency
  - MetaWave attacks are effective over a wide band of sensing frequencies

Countermeasures

- RF Fingerprinting
  - Use the physical characteristics to judge if the echo signal comes from the same hardware
  - It can be used to detect malicious signal, but not passive tags.
- **False Alarm Detection**
  - Constant False-Alarm Rate (CFAR) technology
  - Meta-material tags to change the echo signal along with the environment
- Multi-sensor
  - Employ different mmWave sensors operating under different sensing frequency
  - MetaWave attacks are effective over a wide band of sensing frequencies

Countermeasures

- RF Fingerprinting
  - Use the physical characteristics to judge if the echo signal comes from the same hardware
  - It can be used to detect malicious signal, but not passive tags.
- False Alarm Detection
  - Constant False-Alarm Rate (CFAR) technology
  - Meta-material tags to change the echo signal along with the environment
- **Multi-sensor**
  - Employ different mmWave sensors operating under different sensing frequency
  - MetaWave attacks are effective over a wide band of sensing frequencies

Conclusion

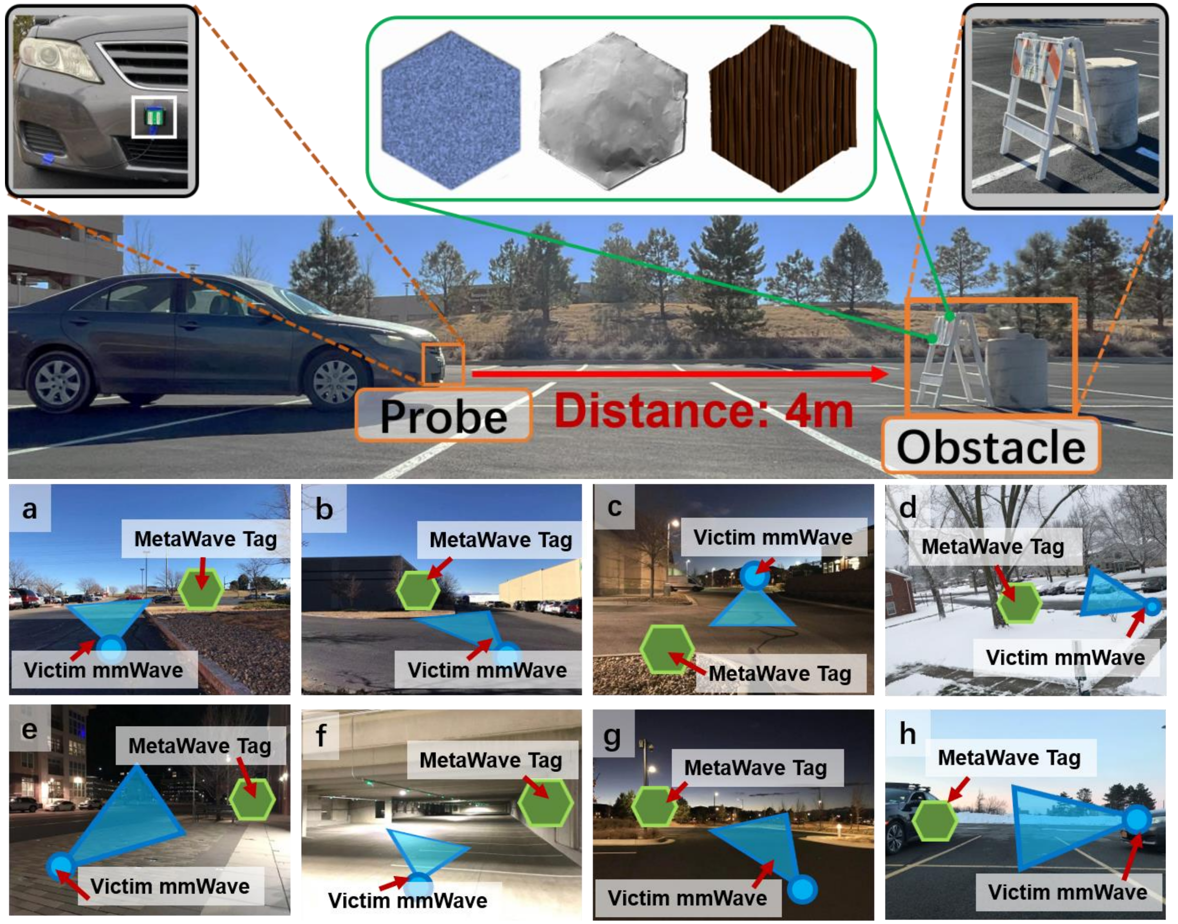
- New passive attack type with meta-material enhanced tags on mmWave sensing

- The first low-cost and easily obtainable meta-material-enhanced tags with specific designs for mmWave ghost and vanish attacks.

- Simulator-based mmWave attack framework to optimize the attack.

Evaluation Setup

- System Setup

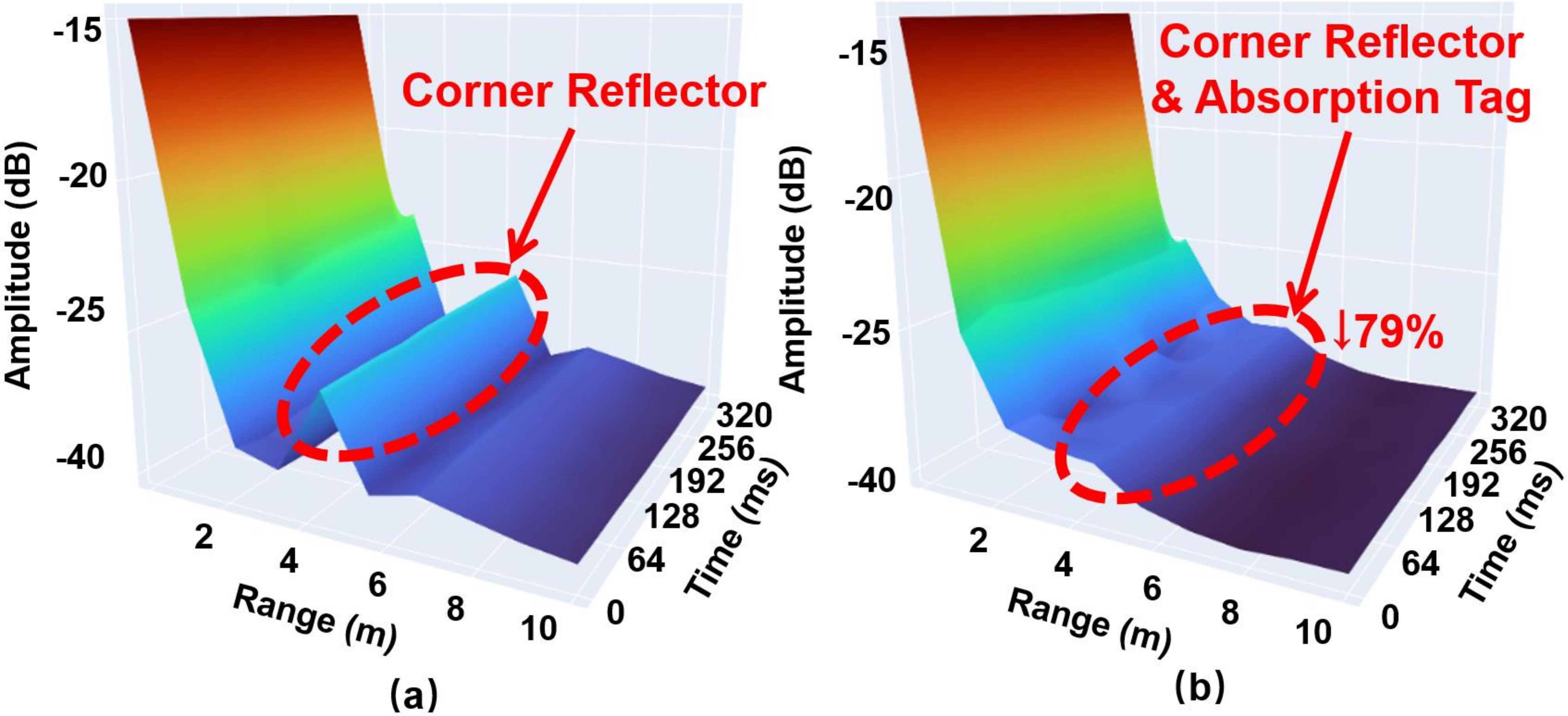


Introduction

- Features
  - Stealthy -- Passive Tag
  - Viable -- easily obtainable COTS material tag, low bar to launch attacks
  - Versatile -- multi-function attacks through a united design framework

Preliminaries

- Feasibility Study



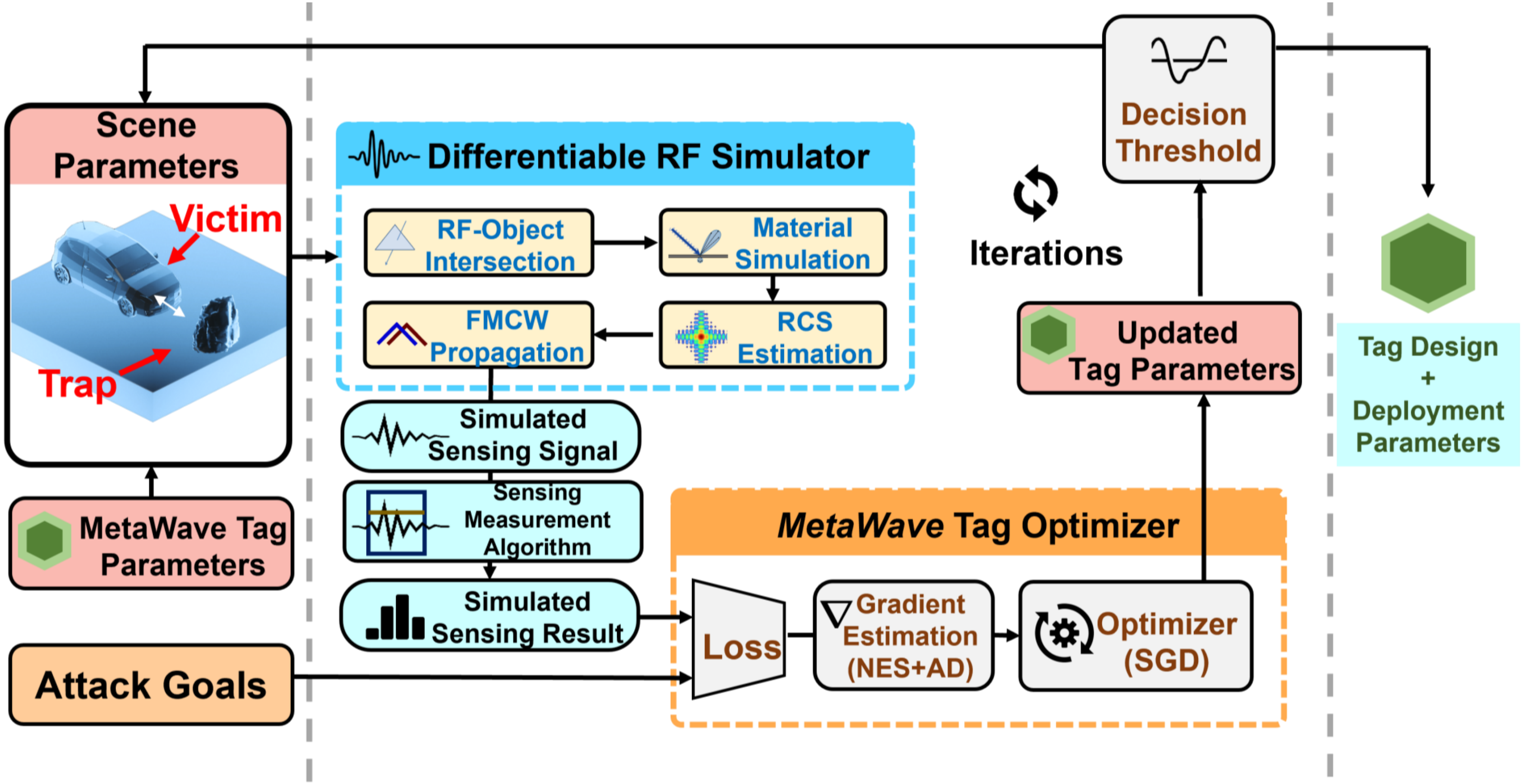
Corner Reflector

Corner Reflector & Absorption Tag

↓79%

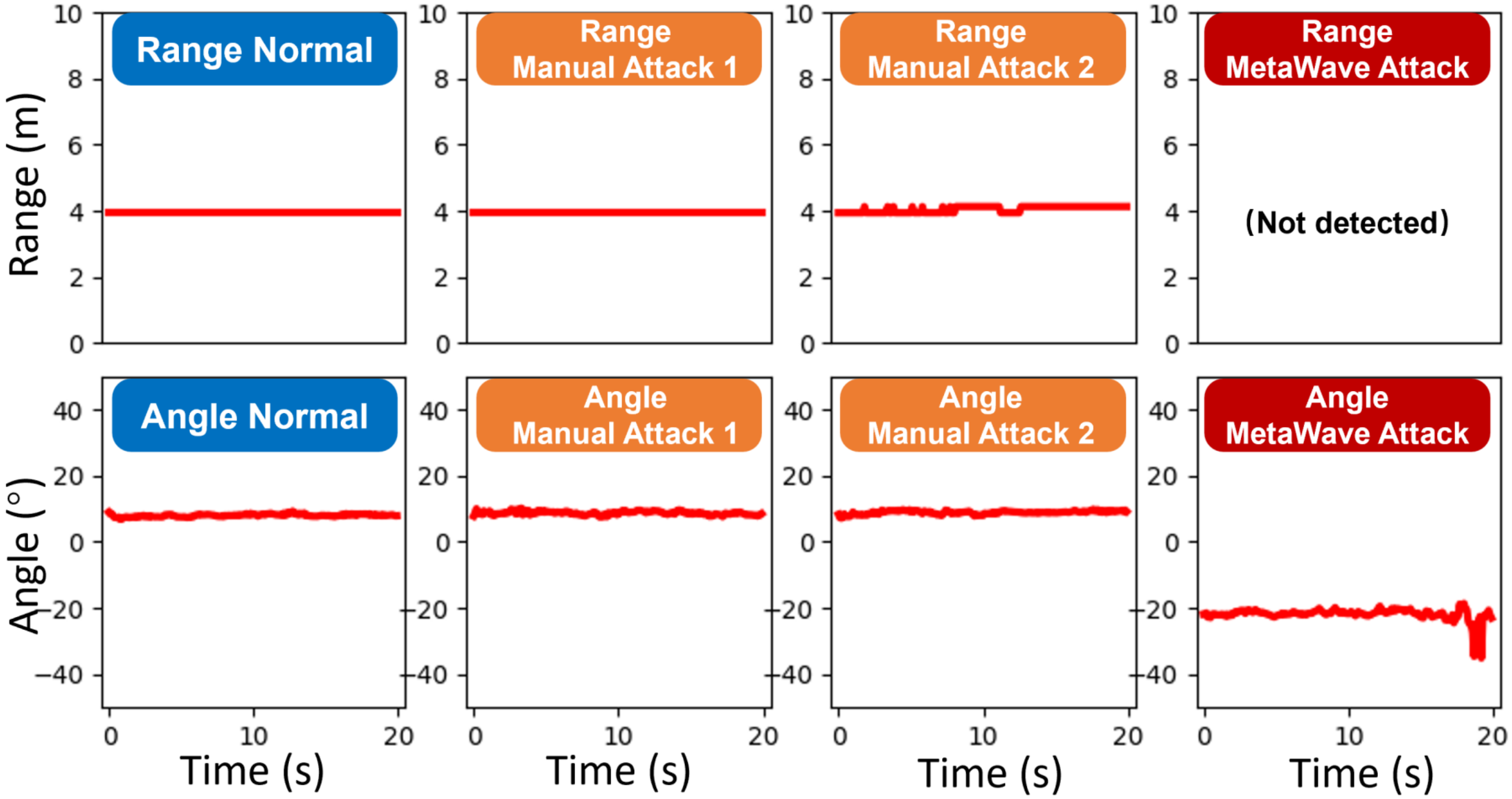
System Design

- ***MetaWave*** Attack Framework Design



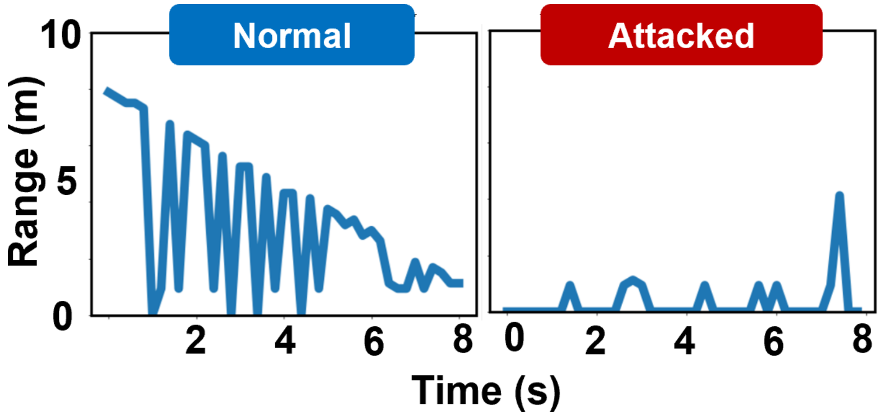
Practicality and Generalization Evaluation

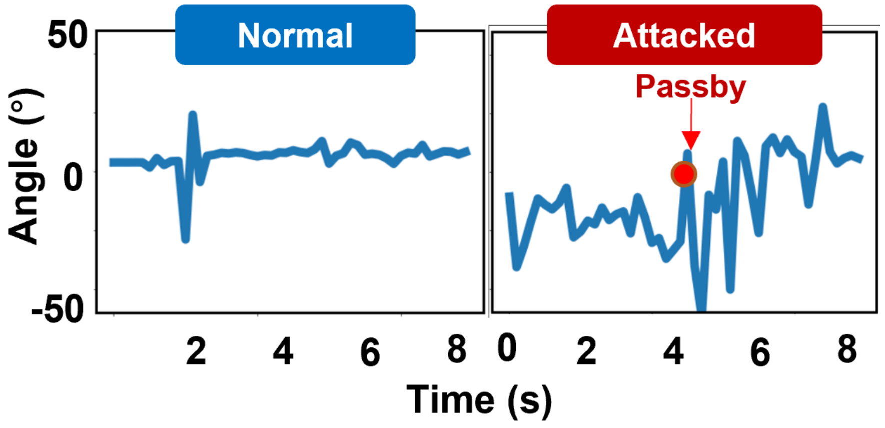
- ***MetaWave*** Tag Optimizer Analysis



Real-World Attack Evaluation

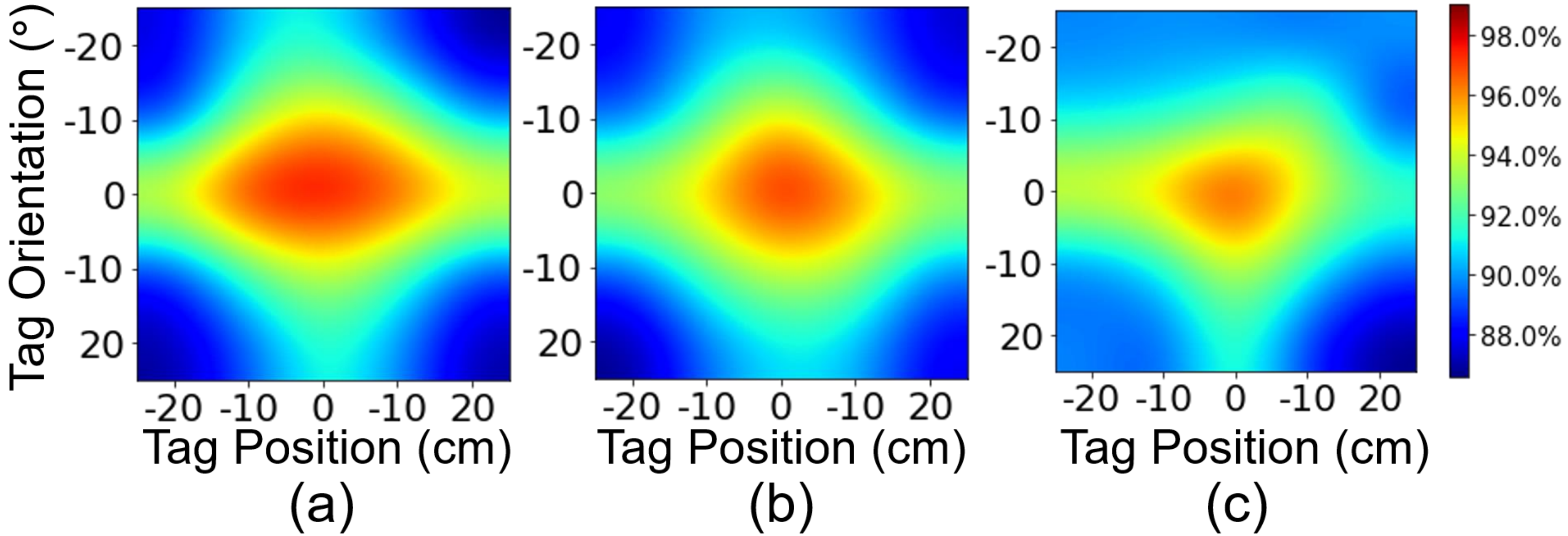
- Dynamic Attack of the Moving mmWave Sensor





Practicality and Generalization Evaluation

- Attack Measurement



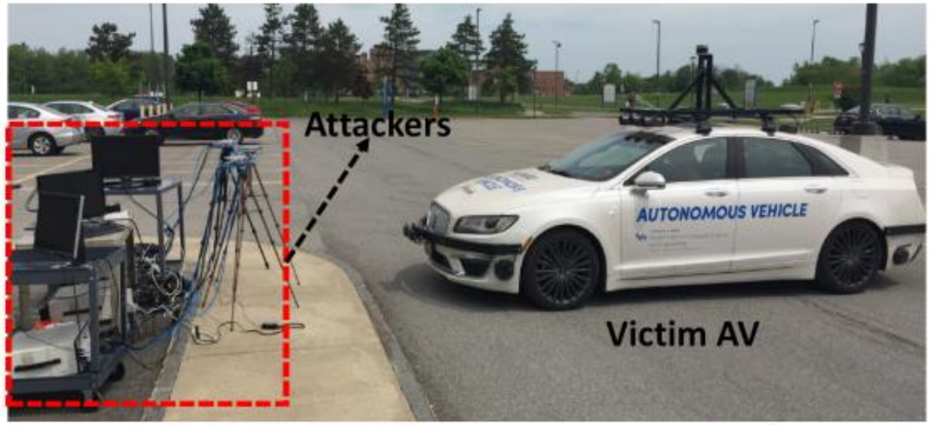
Attack Range Measurement

Attack Angle Measurement

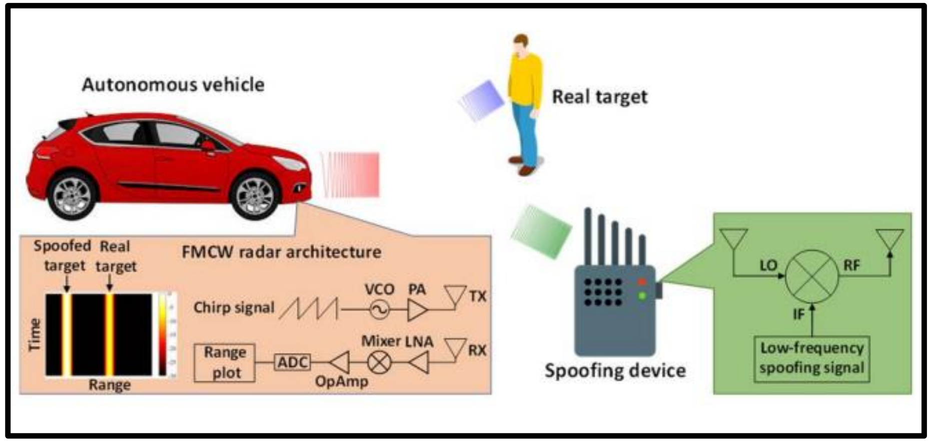
Attack Speed Measurement

Related Work

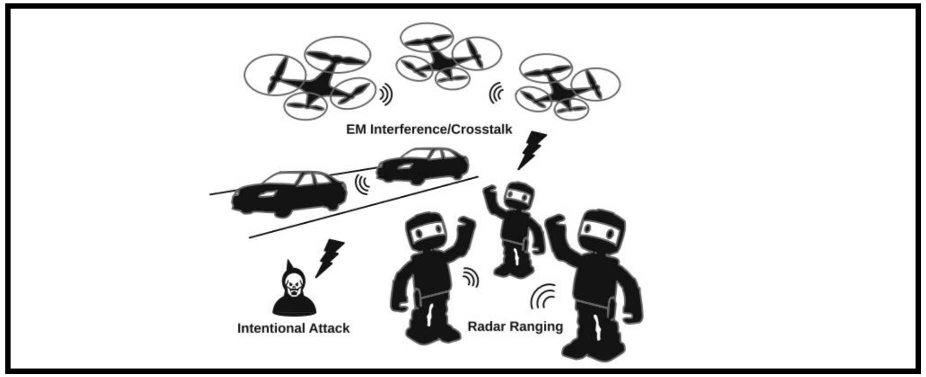
- Attack on mmWave Sensing



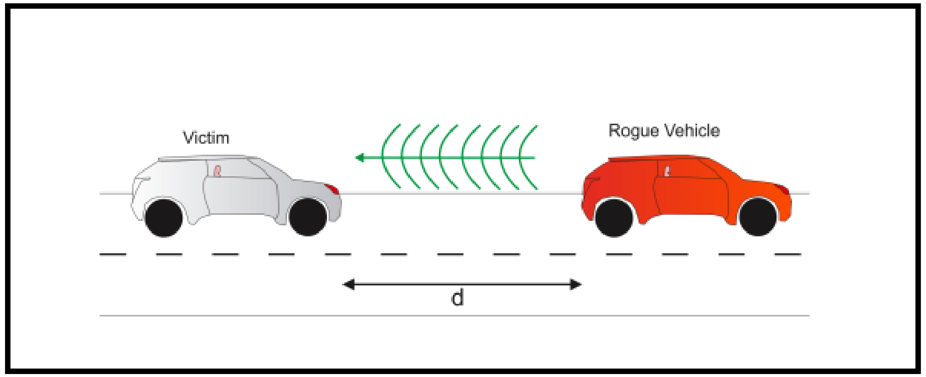
Sun et al.



Nallabolu et al.



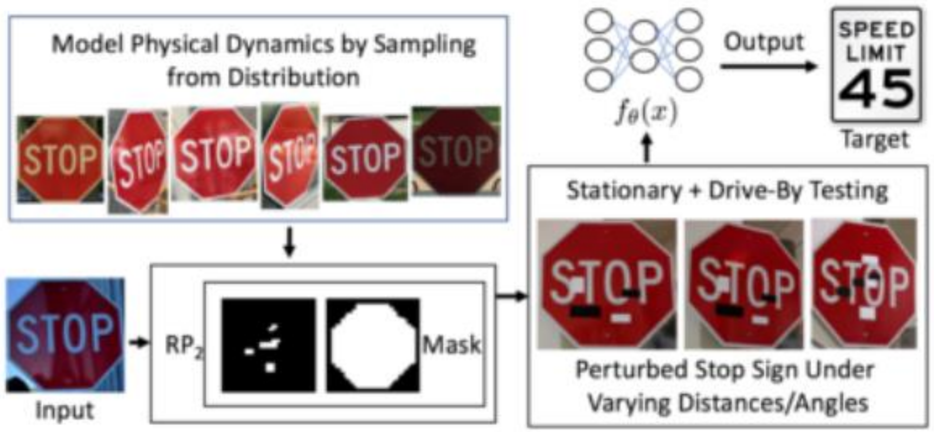
Nashimoto et al.



Komissarov et al.

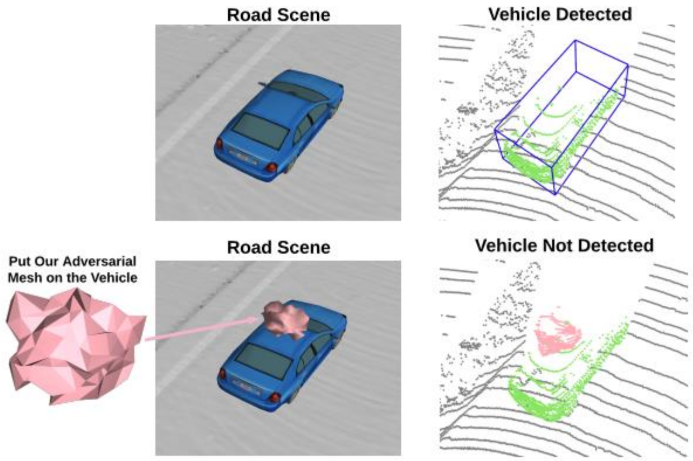
Related Work

- Physical Attack on Sensing


Model Physical Dynamics by Sampling from Distribution
STOP
Output
SPEED LIMIT 45
Target
$f_\theta(x)$
Stationary + Drive-By Testing
Perturbed Stop Sign Under Varying Distances/Angles
Input
RP$_2$
Mask

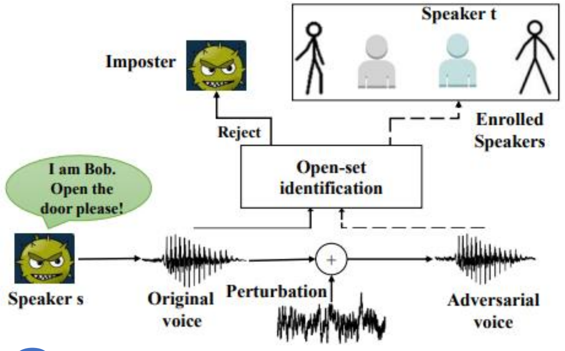
Camera

Wei et al.



Lidar

Tu et al.

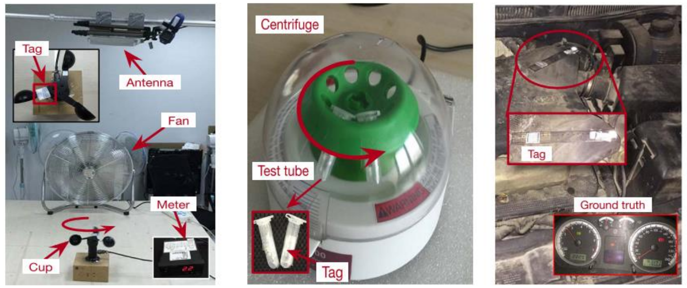


Voice

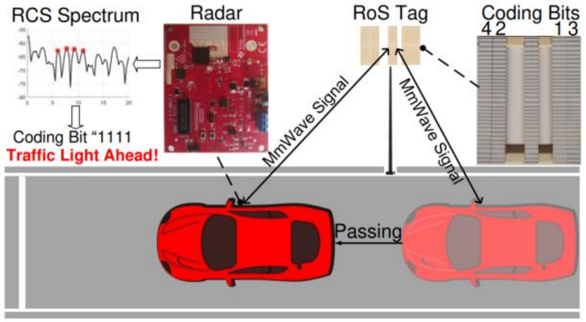
Chen et al.

Related Work

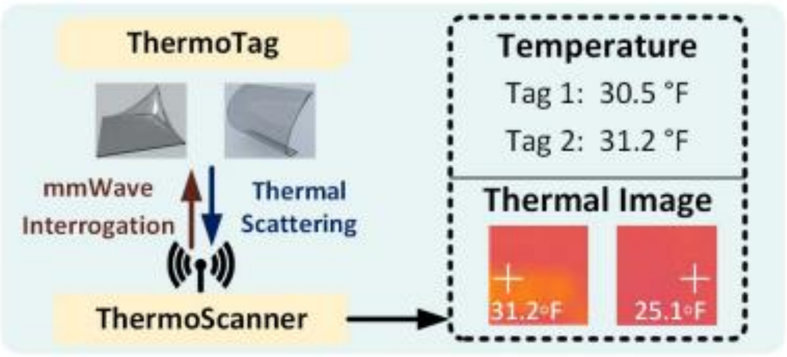
- mmWave Sensing with Meta-material Tags



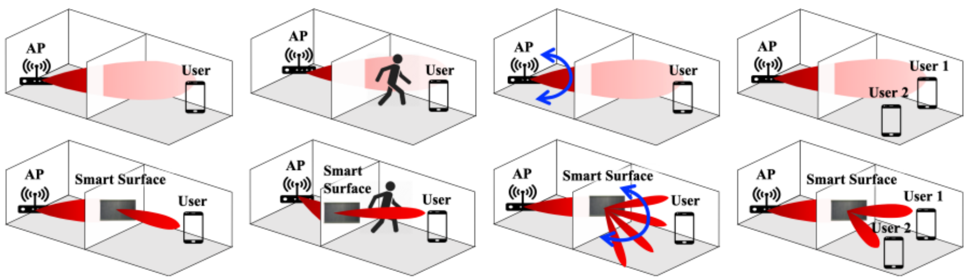
Lin et al.



Nolan et al.

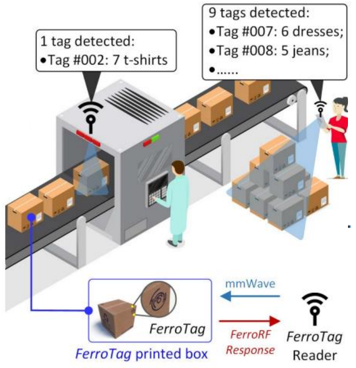


Chen et al.

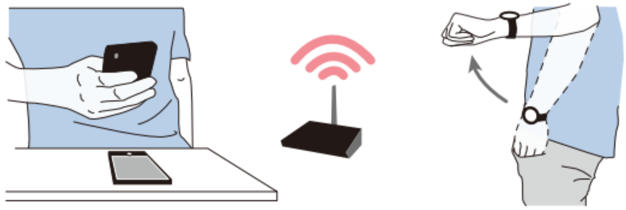


(a) Beam relay and focusing. (b) Path diversity. (c) Beam searching. (d) Multicast.

Cho et al.



Li et al.



Chen et al.

Countermeasures

- Victim awareness
  - RF Fingerprint
  - False Alarm Detection
  - Multiply mmWave Sensors