# Stars Can Tell:

## A Robust Method to Defend against GPS Spoofing Attacks using Off-the-shelf Chipset

**Shinan Liu***, Xiang Cheng*, Hanchao Yang, Yuanchao Shu, Xiaoran Weng, Ping Guo, Kexiong (Curtis) Zeng, Gang Wang, Yaling Yang

University of Chicago

Virginia Tech

CityU Hong Kong

UESTC

UIUC

facebook

Microsoft Research

# GPS spoofing is a concerning threat.

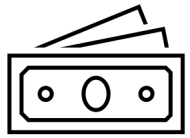
- If spoofed, GPS receivers get **arbitrary location and time**


In 2017, ships were fooled by GPS spoofing in Black Sea


In 2018/2020, self-driving cars diverted to dangerous roads

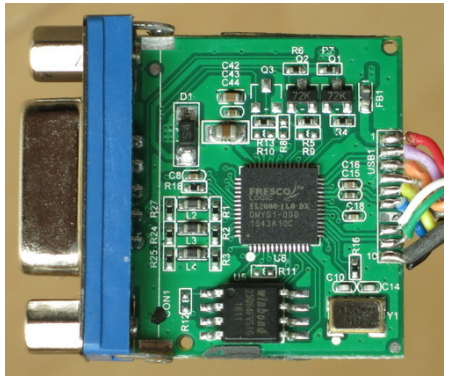

In 2011, researchers pointed out stock servers vulnerable to time asynchrony

# Spoofers are still evolving.



Cheaper

- $5000+ => ~$35
- Close-source => open access



Stronger

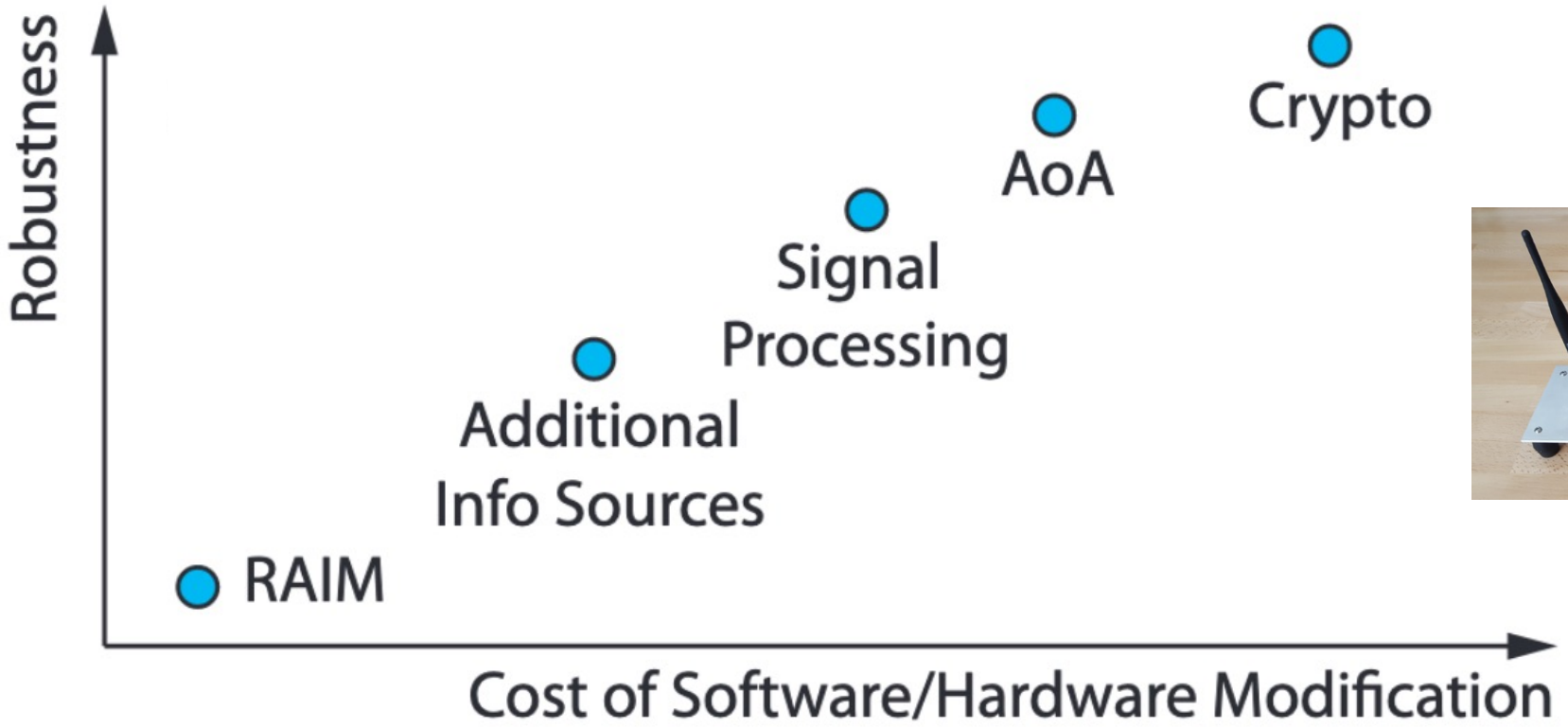
- Brutal overpower => Smooth takeover

⇒ Threat we are facing

- Single state-of-the-art spoofer
- No physical access

# Anti-spoofing methods face trade-off.

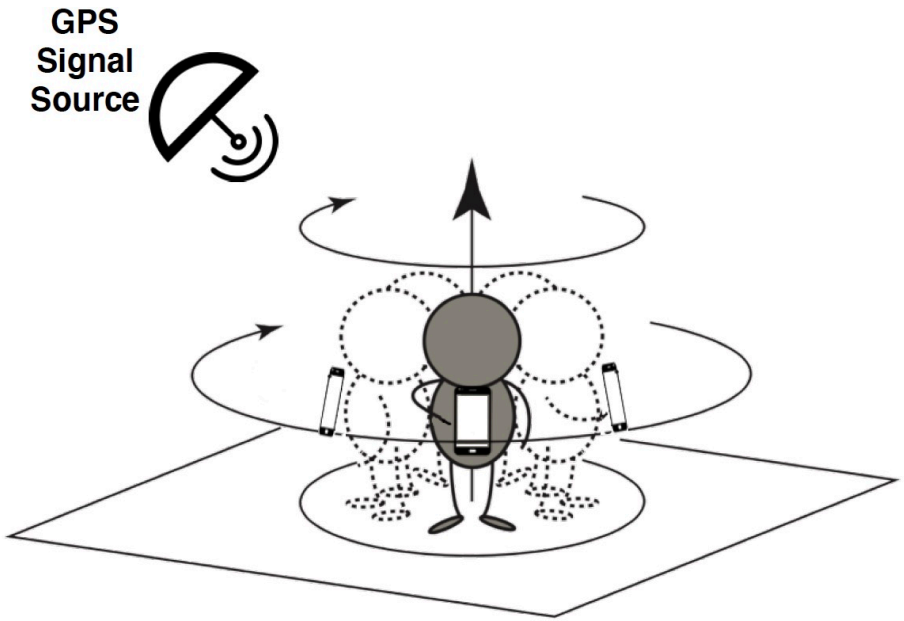
Previous methods: trade-off between **Robustness** and **Cost**

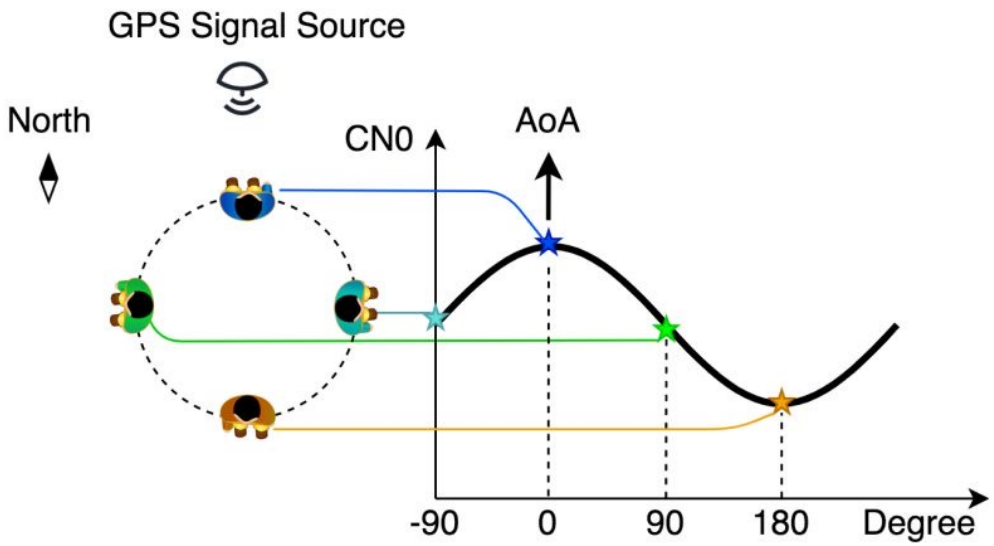



Can a spoofing detector be both **robust and low-cost**?

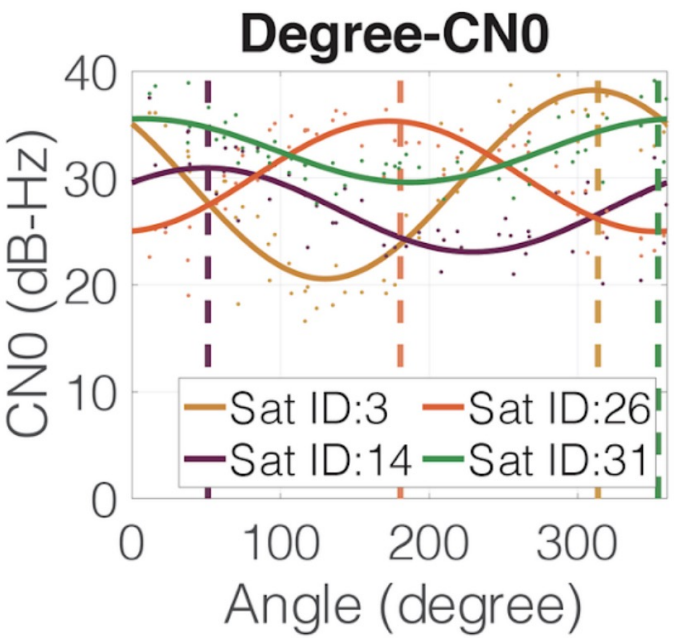
# Receiver + Blockage + Rotation = GPS Spoofing Detector !

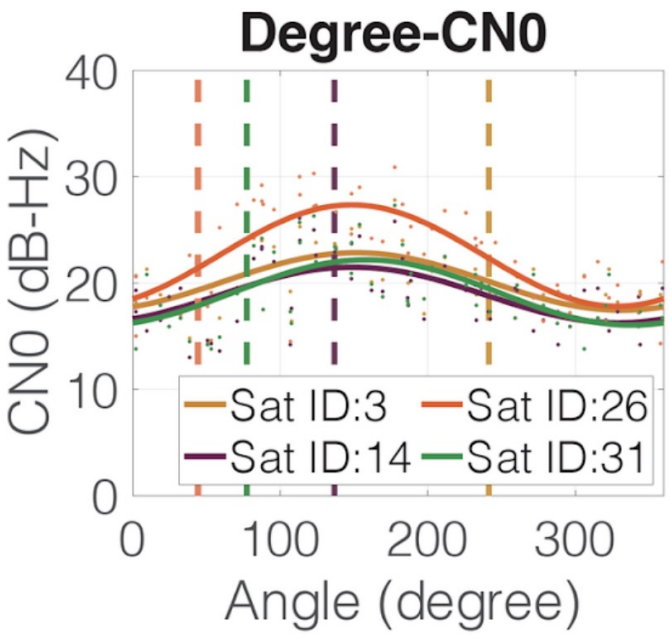
- Our idea is to get **AoAs** by **synthesizing a directional antenna-array using omnidirectional antennas** on commercial devices like smartphones.



# Spoofing is detected by information from multiple satellites.




NonSpoofing VS Spoofing

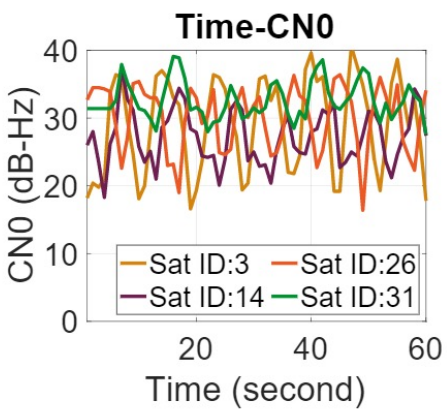
(Signals spread, angles different VS Signals align, angles same)

# THREE detection algorithms are proposed.

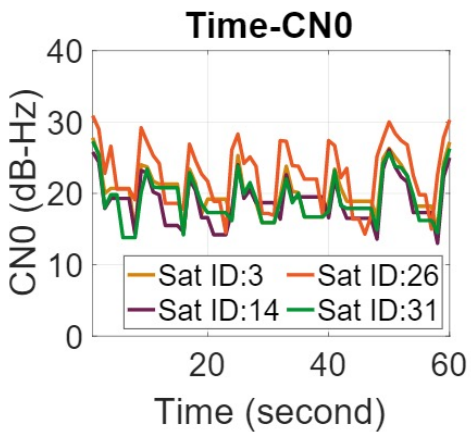
- Method 1: AoA-Diff = $\overline{|\mathrm{AoA} - \mathrm{AoE}|}$

- Method 2: AoA-Dev = $\sqrt{\frac{\sum(AoA_i - \overline{AoA})^2}{N(AoA)}}$

- Method 3: CN0-Corr

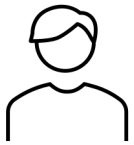
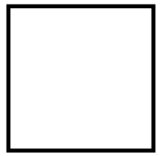


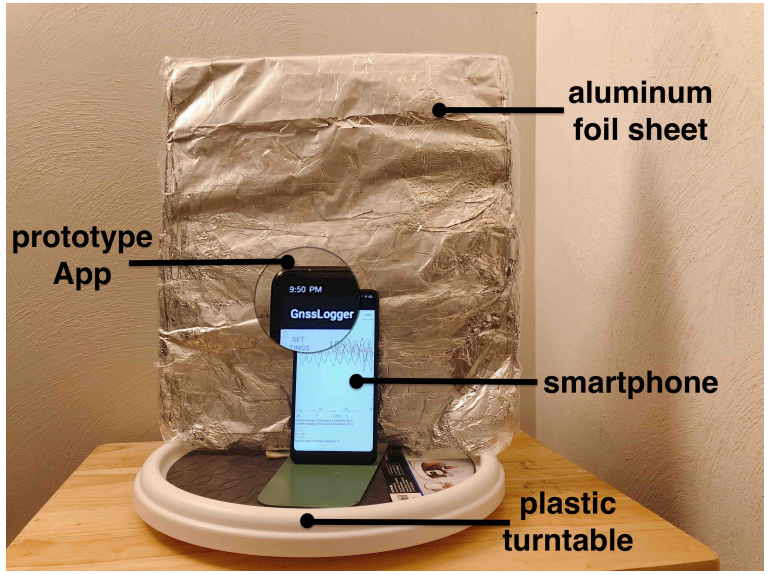

Legitimate signals




Spoofing signals

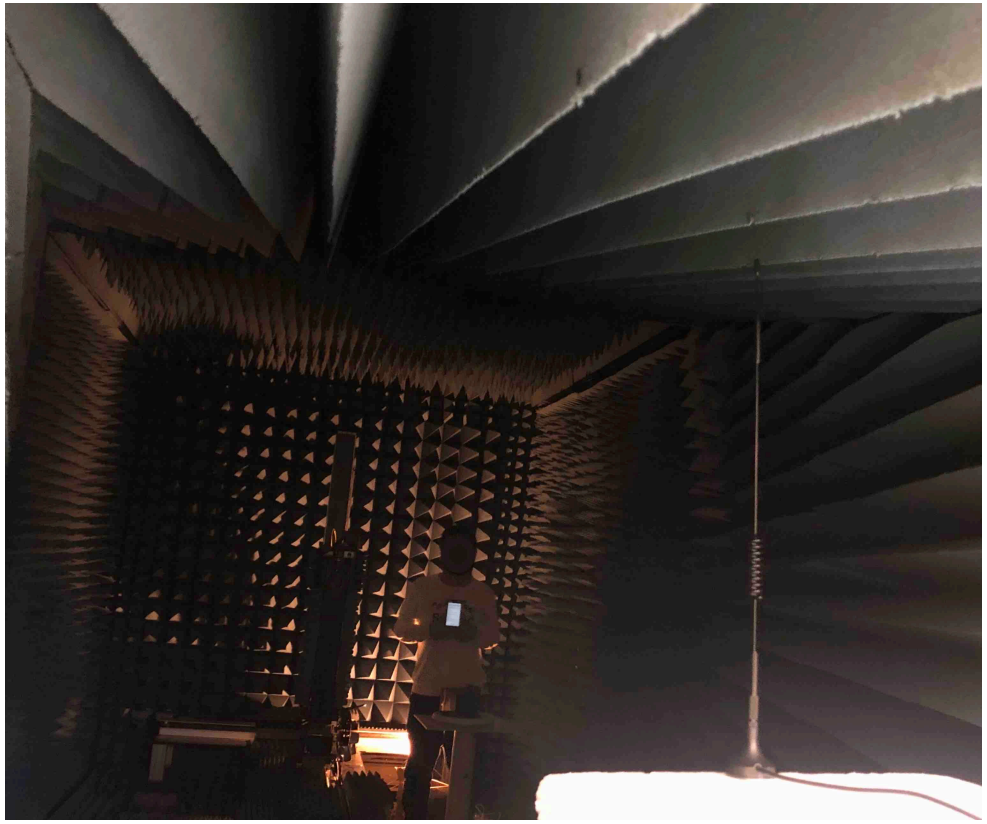
# Multiple settings were tested for evaluation.

- Environment: open air  , urban canyon 
- Blockage: human body  , metal sheet 
- Experiment device
  - Spoofer: HackRF One
  - Receiver: Mi Mix 2
    - OS: Android 8
    - GPS report rate: 1 Hz




Metal Blockage

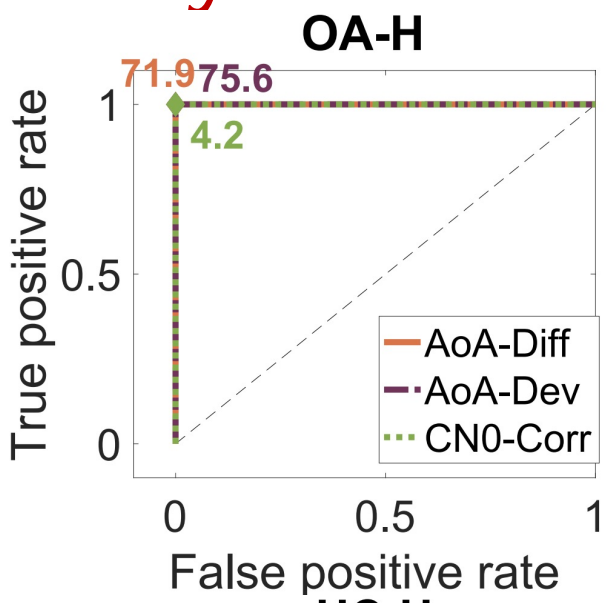
# We take Ethics and Legality seriously.

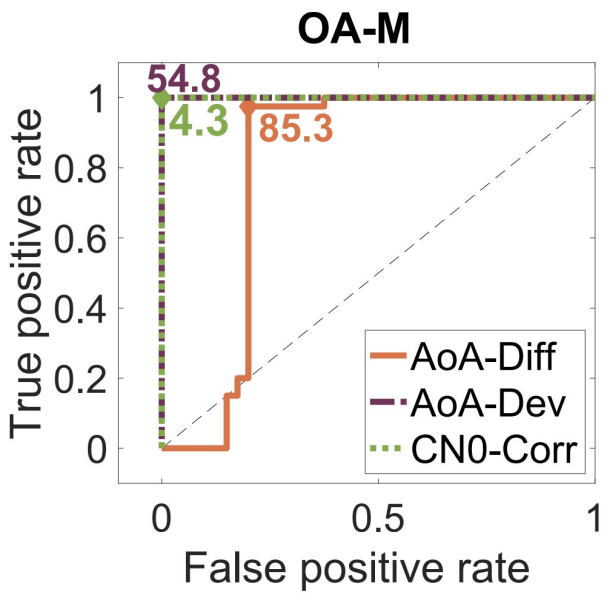


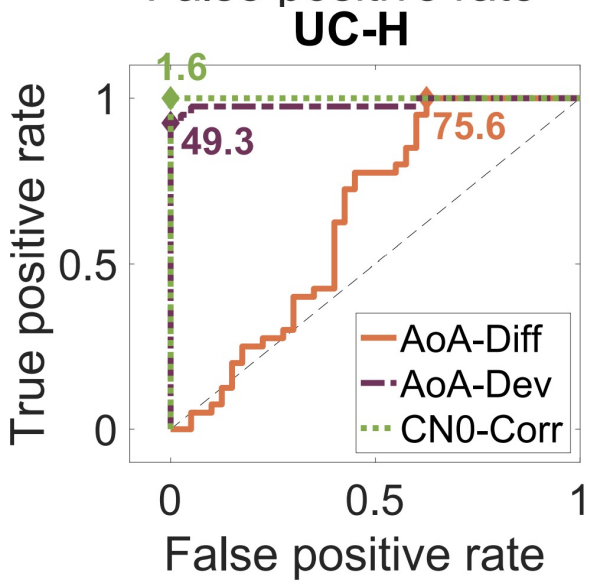
Anechoic chamber used for testing

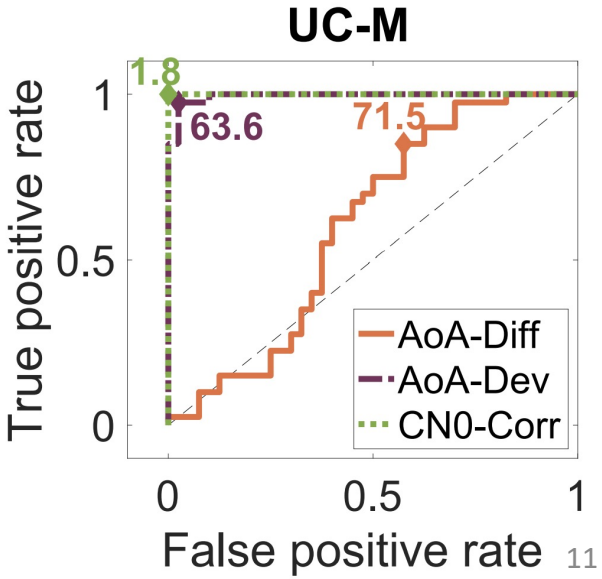
# Evaluation: Accuracy

- Each figure has 40 spoofing cases and 40 non-spoofing cases
- Each case records 30 seconds of data



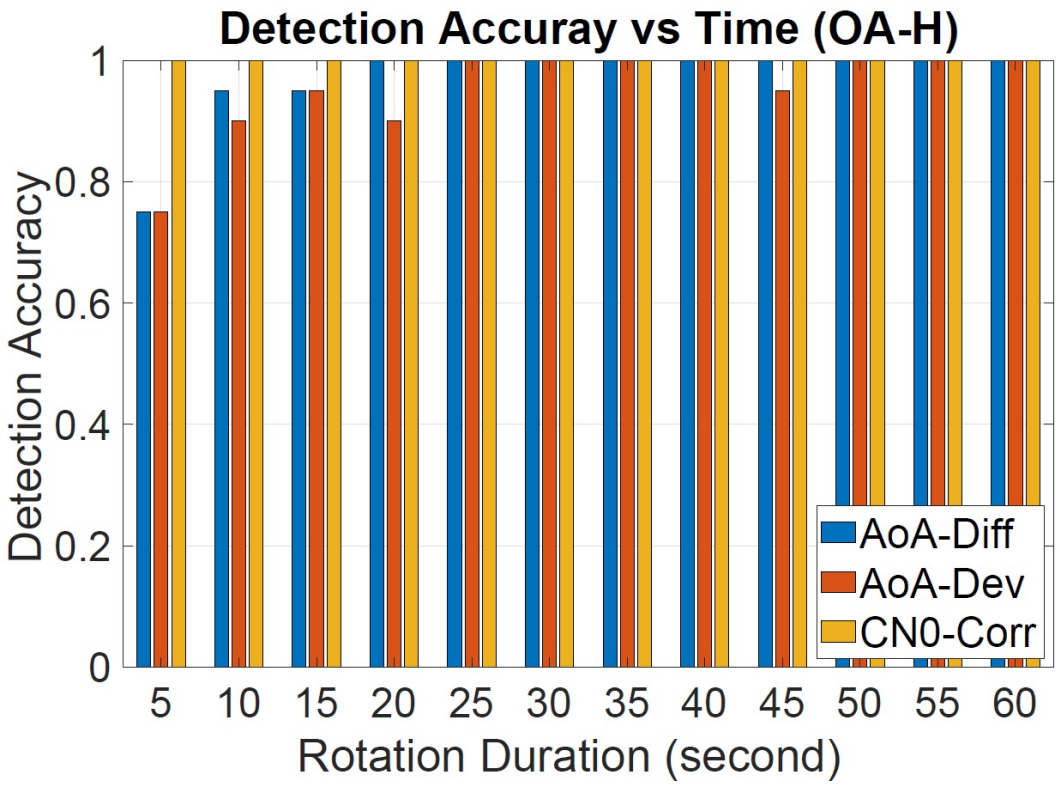



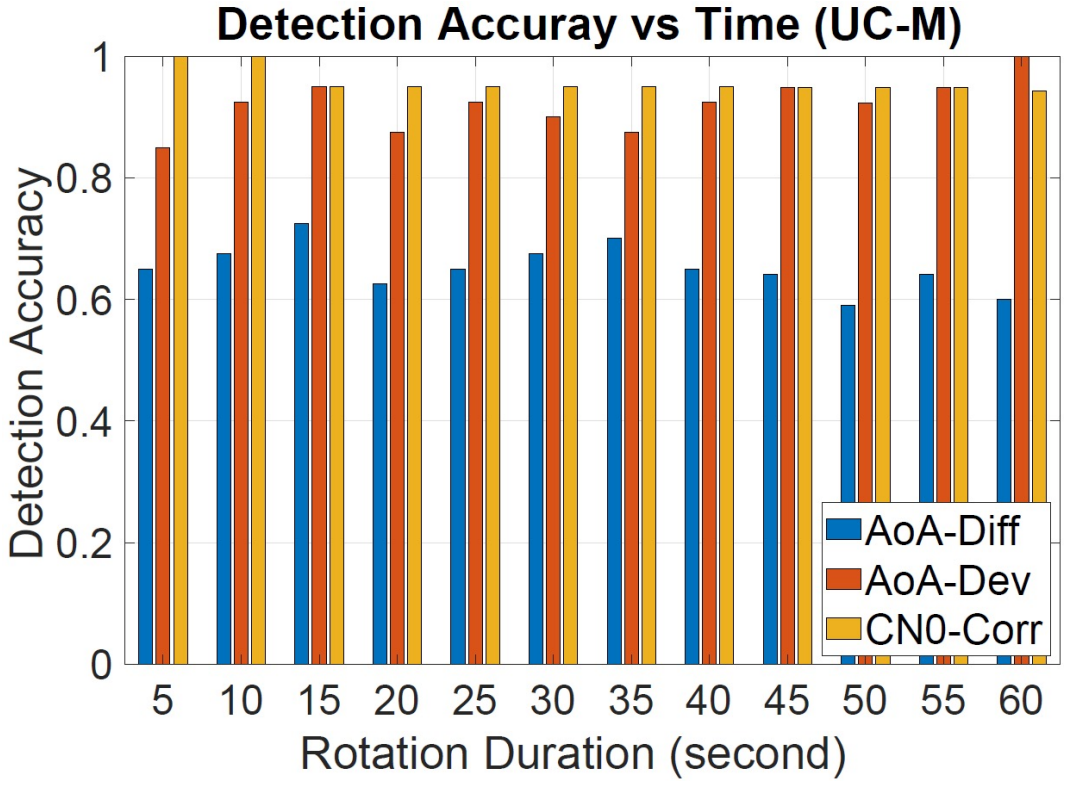




OA-H: Open air human blockage
OA-M: Open air metal blockage
UC-H: Urban canyon human blockage
UC-M: Urban canyon metal blockage

# Evaluation: Time

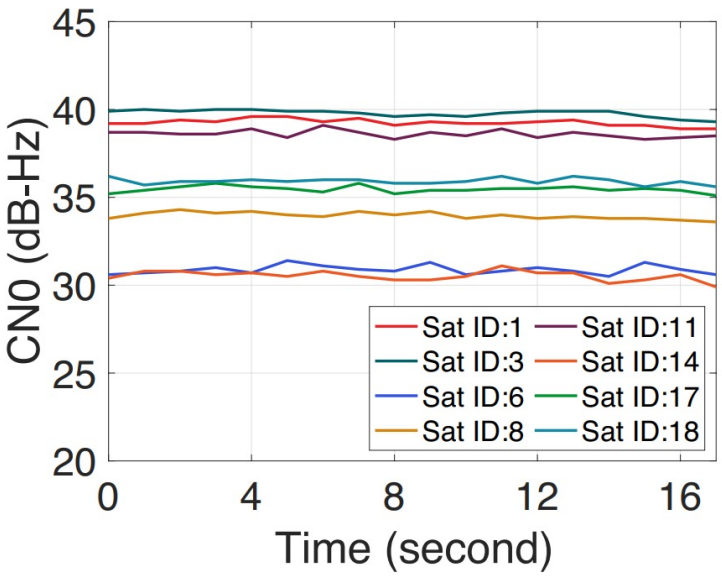


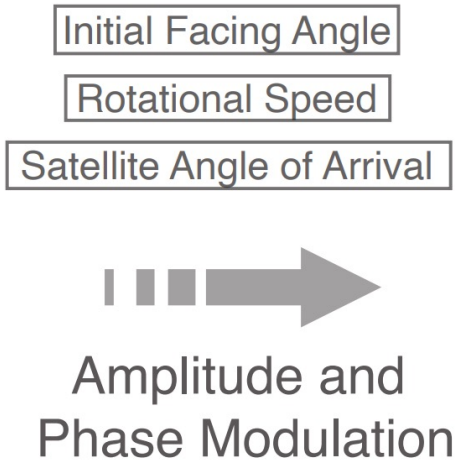
What if the spoofer is **aware** of these defenses?

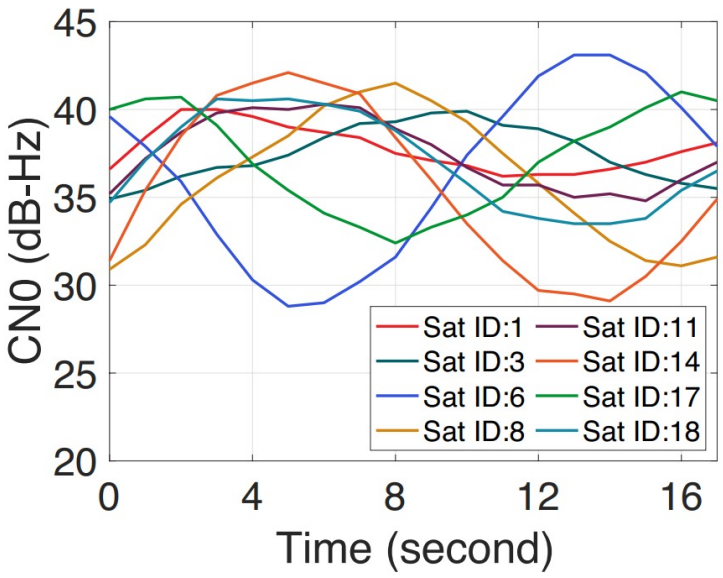
# Adaptive attack mimics different satellites during rotations.

- The attacker has to "observe" the rotation speed and the initial facing angle of the GPS receiver




Basic Attack

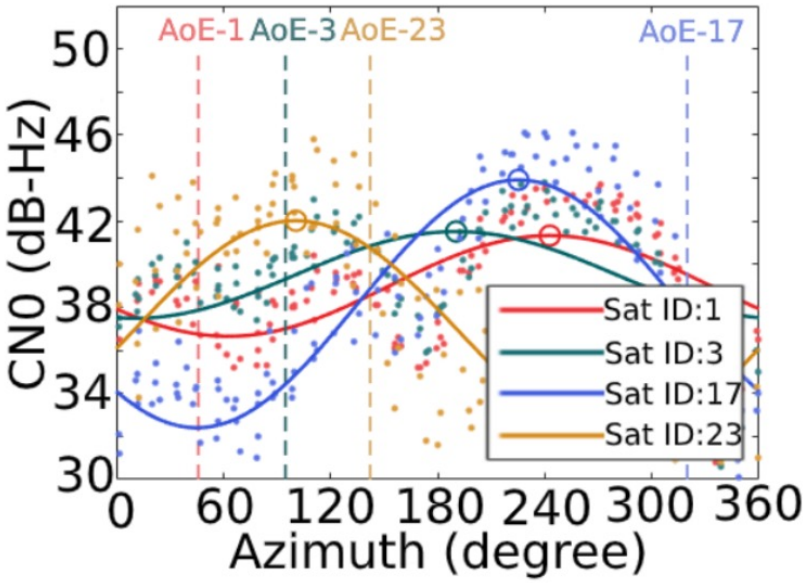


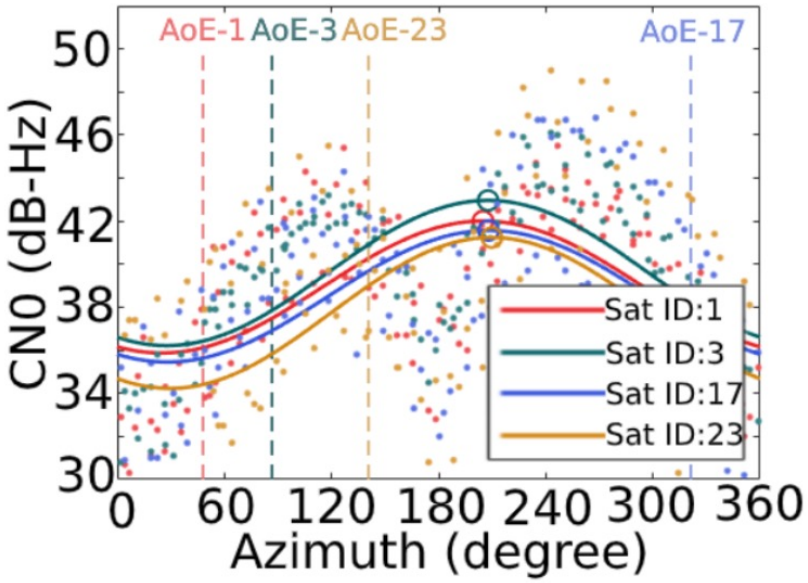

Adaptive Attack

# Advanced defense leverages rotation as a "secrete key"

- Rotation speed of a GPS receiver is inherently a secret that can be dynamically changed by the defender.




(a) Correct guess of rotation speed and initial phase.




(b) Incorrect guess of rotation speed and initial phase.

# Advanced Detection: Average over the cycle (AROC)

- Intuition: rotating multiple cycles can average out incorrect guess on phase domain.
- Steps:
  - Rotate many cycles
  - Slice into many degree slots
  - Averaging CN0 measurement in each slot

$A_i$: Received single strength
$\theta_i$: Signal i elevation angle
$\varphi_i$: Signal i azimuth angle
$G_i$: Periodical function:
$G_i(\theta_i, \varphi_i) = G_i(\theta_i, \varphi_i + 2\pi k)\ \forall k \in \mathbb{Z}$
$\Delta$: Change in rotation angle
$S_i(t)$: Spoofing signal strength at time t
$t_\Delta$: Time when receiver rotate $\Delta$ angle
$A_i', \omega_i, \gamma_i, D_i$: Amplitude, frequency, phase, mean value of advanced spoofing signals
$L_i$: Basic spoofing signal strength
$\upsilon$: Rotation speed

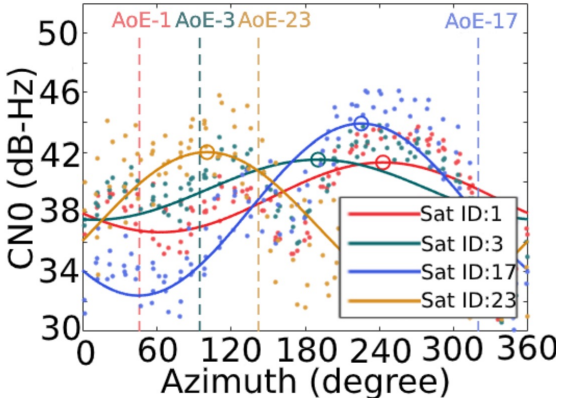
$$\overline{A_i(t_\Delta)} = \frac{\sum_{k=0}^{n} A_i(\Delta + 2\pi k)}{n}$$

$$= \frac{G_i(\theta, \varphi + \Delta) A_i' L_i}{n} \sum_{k=0}^{n} \cos(\omega \cdot t_{\Delta+2\pi k} + \gamma_i) + G_i(\theta, \varphi + \Delta) D_i L_i$$

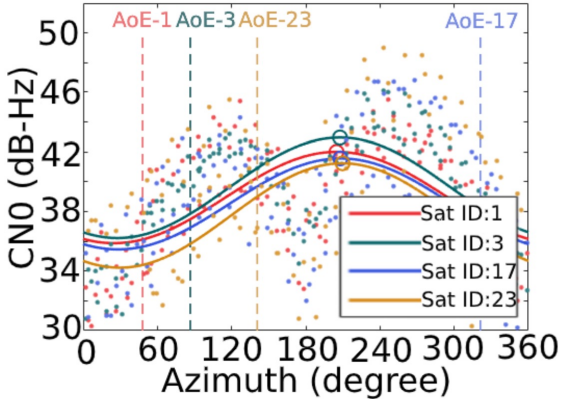
- Then $t_{\Delta+2\pi k} = \Delta/\upsilon + 2\pi k/\upsilon$, when $\omega/\upsilon \notin \mathbb{Z}$, we have:

$$\frac{\sum_{k=0}^{n} \cos(\omega \cdot t_{\Delta+2\pi k} + \gamma_i)}{n} \approx 0, n \to \infty$$

- So $\overline{A_i(t_\Delta)} \approx G_i(\theta, \varphi + \Delta) D_i L_i, n \to \infty$




Correct guess




Incorrect guess

# Advanced Detection: Spectrum Analysis (SA)

- Intuition: rotation and modulation have different frequency component
- Step 1: Express the received signal strength as:

$$A_i(\Delta) = G_i(\theta, \varphi + \Delta) S_i(t_\Delta)$$

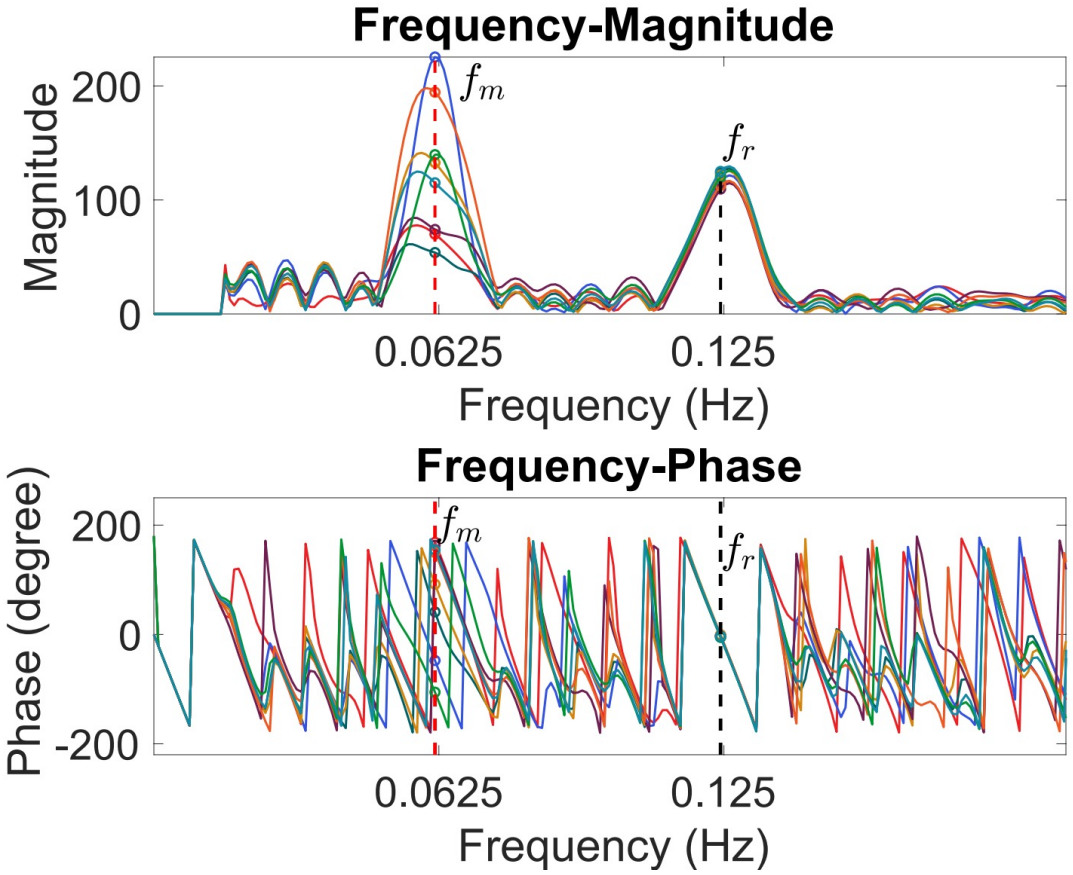
- Step 2: Approximate expression of $G$

$$G \approx M \cdot \cos(vt + \varphi_i) + C$$

- Step 3: Combine with $S_i$ expression in the previous slide

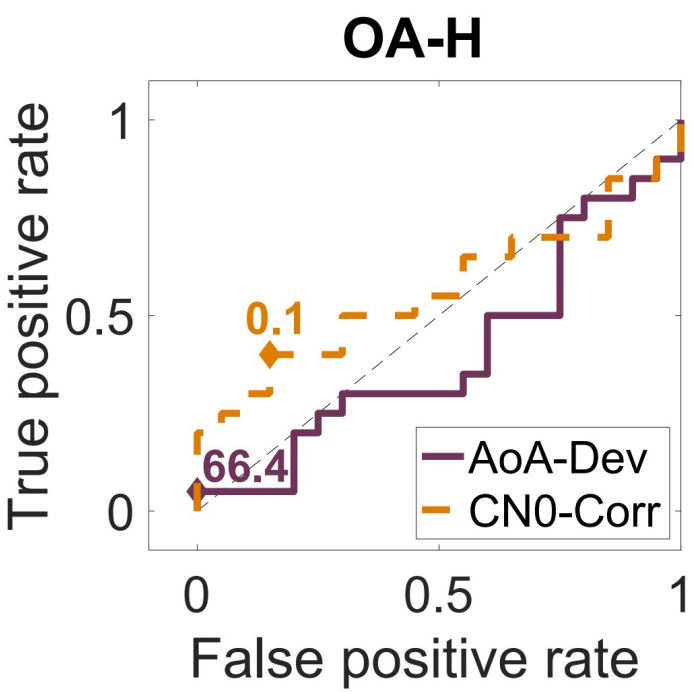
$$A_i(\Delta) = (M\cos(vt + \varphi_i) + C)[A_i' \cos(\omega \cdot t + \gamma) + D_i]L_i$$

$$= L_i \left[ \frac{MA_i'}{2} \cos\big((v + \omega)t + \varphi_i + \gamma\big) + \frac{MA_i'}{2} \cos\big((v - \omega)t + \varphi_i + \gamma\big) + MD_i \cos(vt + \varphi_i) + CA_i' \cos(\omega t + \gamma) + CD_i \right]$$

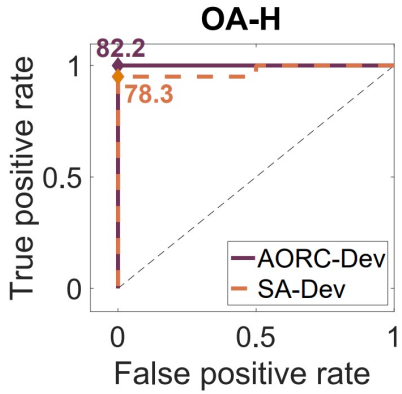



M:Rotation amplitude
$f_m$: Modulation Frequency
$f_r$: Rotation Frequency

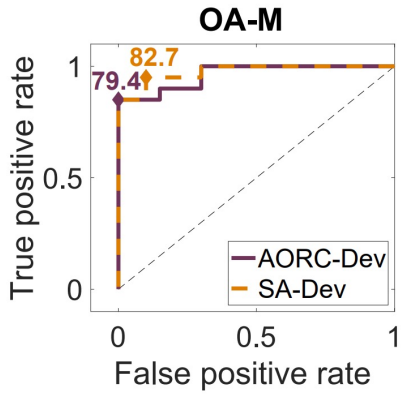
# Advanced Detection Evaluation: Accuracy



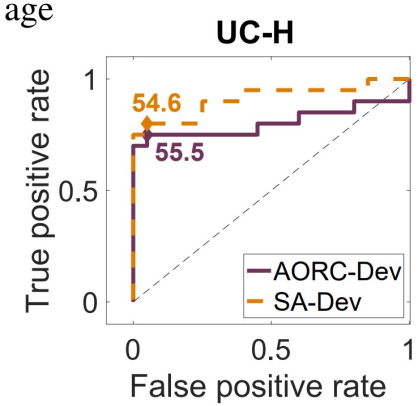

Adaptive Spoofing vs Basic Detection (8s)



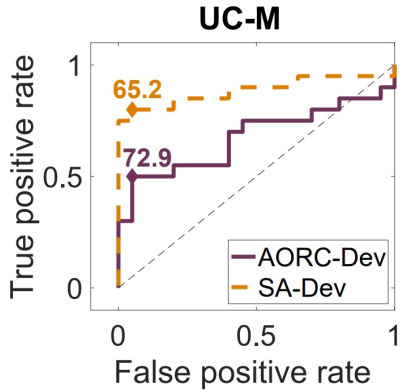

(a) Open air with Human blockage




(b) Open air with Metal blockage




(c) Urban Canyon with Human blockage




(d) Urban Canyon with Metal blockage

Adaptive Spoofing vs Advanced Detection (120s)

Rotation Speed: 6 – 16 seconds per cycle

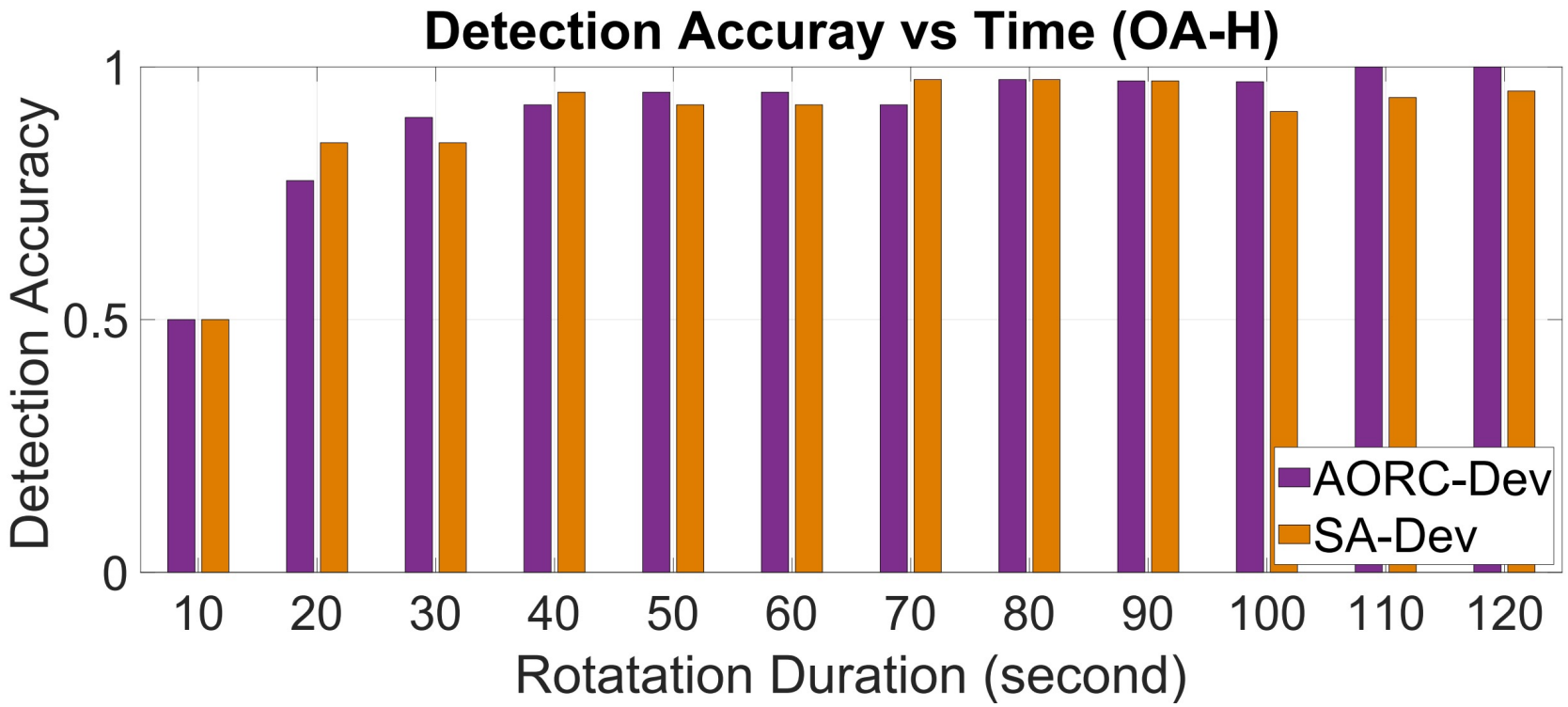
Modulation Speed: 12 seconds per cycle

20 cases of non-spoofing

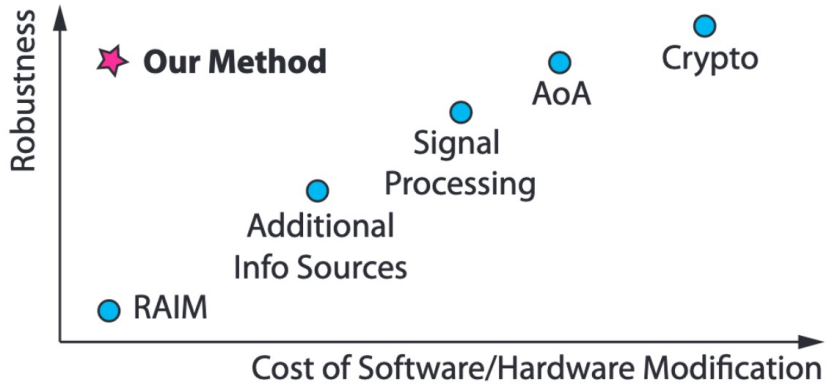
20 cases of spoofing

120 seconds of measurement

# Advanced Detection Evaluation: Time



# Takeaways




- We proposed a new method for GPS spoofing detection that works on off-the-shelf GPS chipsets.
- We explored both basic attacks and adaptive attack and introduced additional measures to fortify the defense.
- We implemented proposed methods and the adaptive attacks. Our method achieves a high accuracy (95%–100%) in 5 seconds.

# Thanks!

Scan this QR code to access contacts, paper, OPEN-SOURCE code, dataset, and Android app!

**Shinan Liu***, Xiang Cheng*, Hanchao Yang, Yuanchao Shu, Xiaoran Weng, Ping Guo, Kexiong (Curtis) Zeng, Gang Wang, Yaling Yang

# Questions?

**Shinan Liu***, Xiang Cheng*, Hanchao Yang, Yuanchao Shu, Xiaoran Weng, Ping Guo, Kexiong (Curtis) Zeng, Gang Wang, Yaling Yang