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
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+ \Rightarrow \sim \$35
- Close-source $\Rightarrow$ open access

Stronger
- Brutal overpower $\Rightarrow$ Smooth takeover

$\Rightarrow$ 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 = \( |\text{AoA} - \text{AoE}| \)

• Method 2: AoA-Dev = \( \sqrt{\frac{\sum (\text{AoA}_i - \text{AoA})^2}{N(\text{AoA})}} \)

• Method 3: CN0-Corr

![Graph 1: Time-CN0](image1)

![Graph 2: Time-CN0](image2)

Legitimate signals

Spoofing signals
Multiple settings were tested for evaluation.

- Environment: open air, urban canyon
- Blockage: human body, metal sheet

- Experiment device
  - Spoofing: HackRF One
  - Receiver: Mi Mix 2
    - OS: Android 8
    - GPS report rate: 1 Hz
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
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.
Advanced defense leverages rotation as a “secrecte 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

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

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

• Then \( t_{\Delta+2\pi k} = \frac{\Delta}{\upsilon} + 2\pi k/\upsilon \), when \( \omega/\upsilon \notin \mathbb{Z} \), we have:
  \[ \sum_{k=0}^{n} \cos(\omega \cdot t_{\Delta+2\pi k} + \gamma_i) \approx 0, n \to \infty \]

So \( A_i(t_\Delta) \approx G_i(\theta, \varphi + \Delta)D_iL_i, n \to \infty \)
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 \( G \)
  \[ G \approx M \cdot \cos(\nu t + \varphi_i) + C \]
- Step 3: Combine with \( S_i \) expression in the previous slide
  \[ A_i(\Delta) = (M\cos(\nu t + \varphi_i) + C)[A'_i \cos(\omega \cdot t + \gamma) + D_i]L_i \]
  \[ = L_i \left[ \frac{MA'_i}{2} \cos((\nu + \omega)t + \varphi_i + \gamma) \right. \]
  \[ + \frac{MA'_i}{2} \cos((\nu - \omega)t + \varphi_i + \gamma) + MD_i \cos(\nu t + \varphi_i) \]
  \[ + CA'_i \cos(\omega t + \gamma) + CD_i \]

M: Rotation amplitude
\( f_m \): Modulation Frequency
\( f_r \): Rotation Frequency
Advanced Detection Evaluation: Accuracy

- 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

Adaptive Spoofing vs Basic Detection (8s)

Adaptive Spoofing vs Advanced Detection (120s)
Advanced Detection Evaluation: Time

![Detection Accuracy vs Time (OA-H)](image)

- Detection Accuracy
- Rotation Duration (second)

- AORC-Dev
- SA-Dev
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