

You Can Drive But You Cannot Hide

Detection of Hidden Cellular GPS Vehicle Trackers

PRESENTED BY MOSHE C. SATT

08/11/25

PROBLEM STATEMENT

NYU

13.5 MILLION EXPERIENCE STALKING IN THE US

Of which technology stalking contributes a whopping **80%**

394,000 people are monitored by low cost devices

NYU

Emerging Threat: Low-Cost GPS Trackers

- **Proliferation of inexpensive, off-the-shelf GPS trackers**
  - Widely accessible and easy to deploy
- **Use of 4G LTE IoT technologies**
  - Leverage NB-IoT (LTE Cat NB1/NB2) or LTE-M (LTE Cat M1/M2)
- **Devices can be discreetly attached to vehicles**
  - Enables **remote tracking** of individuals without consent
- **Major privacy and security implications**
  - Used by malicious actors for stalking or surveillance
- **Current detection methods are largely ineffective**
  - **Inadequate tools** to identify and locate hidden trackers

NYU

OUR SOLUTION

The first usable and scalable solution for detecting 4G LTE IoT cellular GPS vehicle trackers without requiring prior knowledge of their network configuration, using inexpensive commodity hardware and a novel detection method

Related work and Relevance

NYU

HOW IS THIS SOLUTION DIFFERENT?

Table 2: Comparison with existing work on localization and spying attacks on hidden 4G LTE cellular devices.

Work	No Prior Knowledge Required	Passive Attack	Uplink Monitoring	Hidden Cellular IoT Device Detection
Kohls et al. [27]	✗	✓	✗	✗
Bae et al. [12]	✗	✗	✗	✗
Rupprecht et al. [39]	✗	✓	✗	✗
Fraunholz et al. [20]	✗	✓	✗	✗
Hoang et al. [22]	✗	✓	✓	✗
Hong et al. [23]	✗	✗	✗	✗
Kotuliak et al. [28]	✗	✓	✓	✗
This Paper	✓	✓	✓	✓

HOW IS THIS SOLUTION DIFFERENT?

Table 3: Comparison with existing work on detecting hidden GPS vehicle tracking devices.

Li et al. [29]	This Paper
Requires a connected laptop for detection	No laptop needed for detection
Maximum detection range 0.61m	Maximum reliable detection range 0.91m, usable beyond 0.91m with less accuracy
Relatively expensive (>$400)	Relatively inexpensive (<$150)
Can only detect GPS tracker device via side channel EMR	Can detect any cellular device including GPS vehicle trackers and cameras
Not a standalone solution	Portable and standalone solution
Can detect passive GPS trackers (non-cellular)	Cannot detect passive GPS trackers (non-cellular)

NYU

Research Questions and Associated Challenges

NYU

What do we seek to answer?

- What is the speed and precision with which one can identify the uplink frequency ranges for each carrier's local cellular towers? Is it possible to identify the cellular carriers operating in the nearby cell towers, subsequently determine the LTE IoT frequency bands in operation, and then identify the LTE IoT uplink frequencies for each band for scanning purposes?

- By concentrating on the uplink signal to detect hidden devices, despite its significant weakness relative to the downlink signal from the cell tower by a factor of 2, could detection be more efficient due to the reduced need to filter downlink interference and lower noise figure?

- Could utilizing a portable and inexpensive standard radio frequency spectrum analyzer called tinySA be capable of identifying 4G LTE IoT cellular signals?

- What is the maximum distance from which the tinySA can detect signals? Considering that the uplink transmission from an LTE IoT device is significantly weaker compared to the downlink, to what extent is the detection of such low-power signals restricted?

What are the challenges we need to overcome to answer those questions?

- Identifying the cellular network provider to which the device is connected, which differs depending on the country and region in which it is used.
- Identifying the cellular frequency bands linked to the carrier, which differ depending on the country and region in which they operate.
- Identifying which frequency bands are used at local cell sites that support the carrier network
- Determining the cellular uplink frequencies that correspond to the active frequency bands used by each carrier in the local cell tower.
- Performing a rapid scan of the cellular uplink frequency band in the carrier's local cell tower to detect he uplink signal from a cellular device

Methods

NYU

Monitoring LTE IoT frequency uplink frequency bands

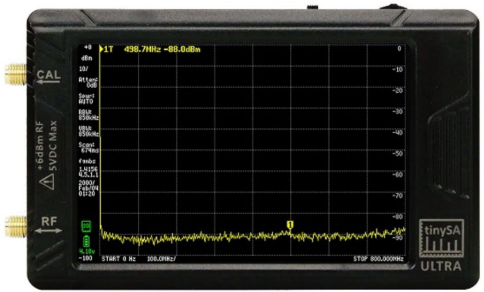


Figure 1: The tinySA Ultra portable mini spectrum analyzer covers a frequency range of 100 kHz to 5.3 GHz and costs approximately $150 on Amazon [7].



Figure 2: The 4G LTE IoT cellular GPS vehicle tracking devices that we tested (clockwise, from upper left): Tracki TRKM010B [49], iTrail GPS903-4G [26], Brickhouse Spark Nano 7 [13], Amcrest AM-GL300W4G [9], and LoneStar Oyster3-4G [30]

Table 9: The 4G LTE IoT cellular GPS vehicle trackers that we tested and the uplink frequencies that we captured, by carrier and LTE band.

Carrier	LTE Band	Uplink	Tracker
AT&T	2	1855 MHz	none
AT&T	12	709 MHz	Amcrest, Brickhouse, LoneStar
T-Mobile	2	1877.5 MHz	Tracki
T-Mobile	12	701.5 MHz	iTrail

NYU

Monitoring LTE IoT frequency uplink frequency bands

Table 8: The 4G LTE IoT cellular GPS vehicle tracking devices we evaluated in this study.

Make	Model	Reporting Interval	Cellular Carrier	Purchase Price on Amazon (2024)	Monthly Service Charge	LTE Bands
LoneStar	Oyster3-4G	5 minutes	AT&T	$149.92	$14.95	1 / 2 / 3 / 4 / 5 / 8 / 12 / 13 / 18 / 19 / 20 / 26 / 28 [30]
iTrail	GPS903-4G	1 minute	T-Mobile	$189	$12.99	2 / 4 / 12 [26]
Brickhouse	Spark Nano 7	1 minute	AT&T	$19.95	$29.99	1 / 2 / 3 / 4 / 5 / 8 / 12 / 13 / 18 / 19 / 20 / 25 / 26 / 27 / 28 / 66 / 71 / 85 [13]
Tracki	TRKM010B	1 minute	T-Mobile	$9.88	$19.95	1 / 2 / 3 / 4 / 5 / 7 / 8 / 12 / 13 / 17 / 18 / 19 / 20 / 25 / 26 / 41 [49]
Amcrest	AM-GL300W-4G	1 minute	AT&T	$29.99	$42.99	2 / 4 / 12 / 13 [9]

Monitoring LTE IoT frequency uplink frequency bands



Figure 3: The tracker and tinySA locations for the experiments. The dotted shapes represent the locations for the test in the glovebox, while the solid line shapes represent the locations for the exterior tests. Circle 2 demonstrates the front bumper location, while Circle 3 demonstrates the rear bumper location.

NYU

Indoor and Outdoor Experiment Protocols

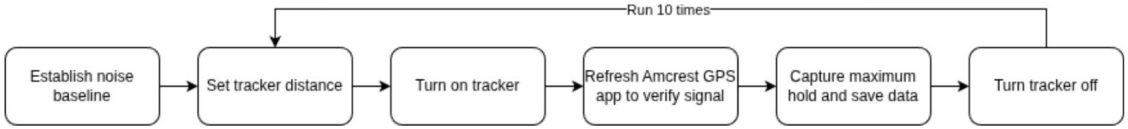


Figure 6: The timeline of the indoor experimental protocol.

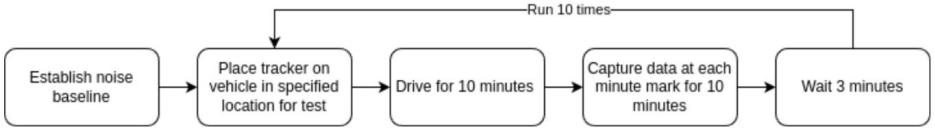


Figure 7: The timeline of the outdoor experimental protocol.

Results

NYU

Results of RQ1

- We were able to answer RQ1 by identifying the frequency ranges for each carrier's local cellular towers and uplink frequency and LTE bands
- We bound these data in latitude and longitude of a radius of our choosing, depending on whether we are in an urban or suburban environment

Results of RQ2

- We were able to answer RQ2 by establishing a control in a Faraday bag, creating a baseline in an RF-quiet environment with no other interfering cellular signals, and then comparing it to real-world experimental data in an RF-noisy environment.

Results of RQ3 and RQ4

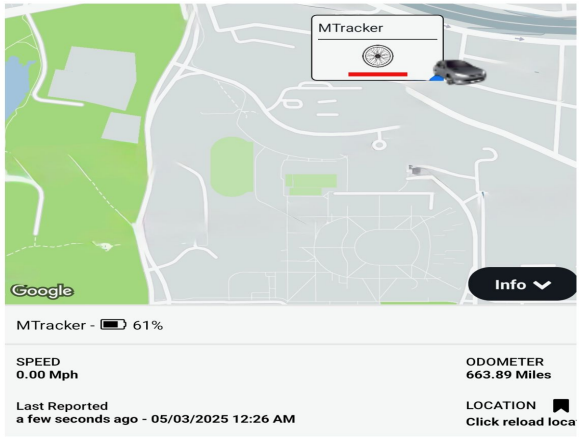


Figure 8: A screenshot from the Amcrest GPS Pro App showing how we verify correlation of signal peaks to GPS cellular reporting intervals. Note the "Last Reported a few seconds ago" at 12:26 AM correlates with 00:26:07 timestamp in Figure 16.

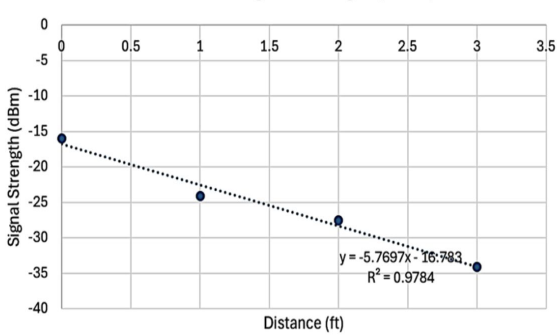


Figure 9: The indoor lab test when the tracker is 3 feet away from tinySA. The tracker was turned on when the timer was started and the location was requested from the app at the one minute mark. Each trial runs for a total of two minutes. The maximum hold setting on the tinySA was used to help store the strongest signal at each frequency. The tracker was

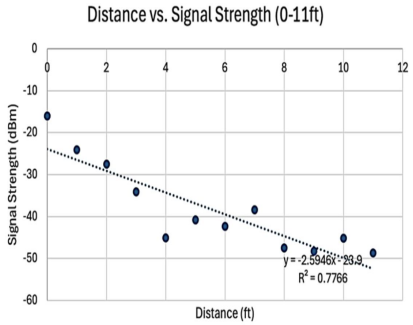


Figure 10: Lab tests for all distances from tinySA to tracker, ranging from one inch, one foot, two feet, …, and 11 feet apart. The captured signal strength from the GPS tracker diminishes as we increasingly move the tinySA farther away from the fixed transmitter of the device [2].

Results of RQ3 and RQ4

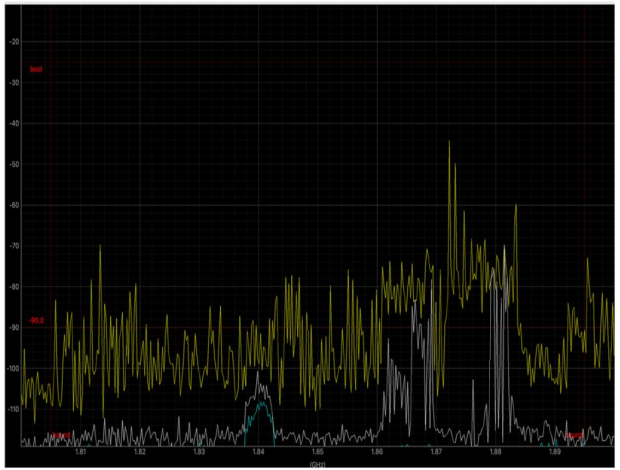


Figure 11: Determining that the visible amplitude spike is generated by our tracker by using a Faraday bag.

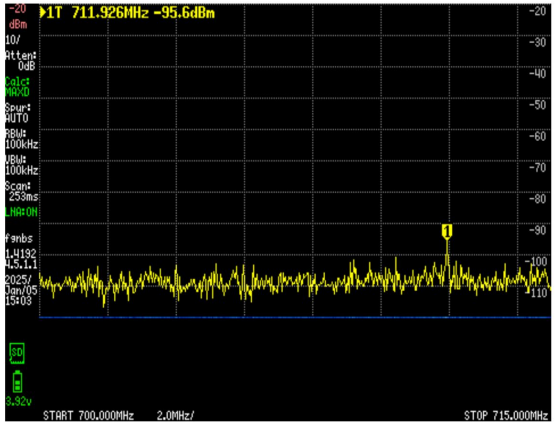


Figure 12: The strongest signal present when the tracker is powered off in the glove compartment was -95.6 dBm using the maximum decay setting and the portable whip antenna attached to the tinySA.

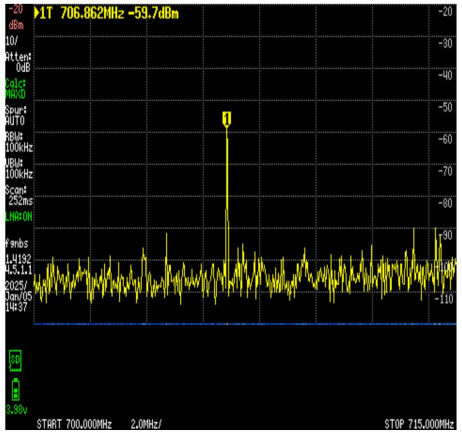


Figure 13: The tracker was in the glove compartment of the vehicle. Regular transmissions at 1-minute intervals were detected peaking at -59.7 dBm using the maximum decay setting with the portable whip antenna attached to the tinySA.

Limitations



Limitations

- Only tested **one vehicle type**, other models were not considered for this study
- Still need to determine an effective way to filter out other **strong signal peaks**
- **Enabling ultra mode in tinySA**; upper frequency limit increased to 5.4 GHz from 800 MHz
- **Accounting for signal strength** when a cellular device transitions between cell towers
- Only focused on **GPS devices** that actively **transmits data over cellular networks**
- Limited to **Unmodified Third-Party Consumer GPS** Vehicle Trackers
- Five GPS test devices were limited to **2 of the 3 US cellular carriers**

Future Work

NYU

Current & Future Landscape of GPS Trackers

- **Current State (U.S.)**:
  - GPS vehicle trackers use 4G LTE IoT narrowband networks.
  - Operate within uplink frequency ranges reserved for LTE IoT.
- **Future Transition:**
  - Gradual shift to 5G, 6G, and beyond expected.
  - Triggered by phase-out of legacy networks (e.g., 2G, 3G).
- **Implication for Research:**
  - Requires a complete reevaluation of detection techniques.
  - Need to adapt to new transmission behaviors and frequency bands.

User-Centric & Scalable Future Approaches

- **Human-Centered Design Focus:**
  - Leverage Human-Computer Interaction (HCI) for real-world testing.
  - Collaborate with focus groups and affected individuals.
- **Proposed Tools:**
  - AirTag-like smartphone alert system to detect trackers.
  - Mobile app to locate suspected trackers, similar to Find My.
- **Social Impact & Accessibility:**
  - Partner with groups like CETA to support IPV survivors.
  - Explore lower-cost portable spectrum analyzers for broader access.

Future Engineering – Automation & Range

- **Hardware Automation Ideas:**
  - Build a "black box" with tinySA + smartphone via Bluetooth/USB.
  - Run tinySA in console mode to enable automated scanning.
- **Mobile Detection Rigs:**
  - Use flatbed tow trucks with multiple tinySAs.
  - No need to trail the target vehicle—trackers emit on motion detection.
- **Advanced Techniques:**
  - Investigate RF power combining and antenna multiplexing.
  - Optimize for range extension vs. cost and complexity trade-offs.

Conclusion

NYU

Conclusion

- **Core Objective:**
  - Provide a practical tool to help detect GPS trackers, especially for cyberstalking victims.
- **Detection Strategy:**
  - Use tinySA handheld spectrum analyzer.
  - Focus on uplink LTE IoT frequency bands.
- **Detection Results:**
  - Identified >20 dBm signal peaks during tracker activation.
  - Controlled tests show consistent threshold for detection.
- **Practical Validation:**
  - Tested in lab and real vehicles.
  - Signal strength varies with distance—used to establish detection limits.