

You Can Drive But You Cannot Hide: Detection of Hidden Cellular GPS Vehicle Trackers

Moshe Chaim Satt
New York University

Donghan Hu
New York University

Patrick Zielinski
New York University

Danny Yuxing Huang
New York University

Abstract

Cyberstalking poses a significant international threat due to the large number of individuals affected worldwide and the severe nature of many incidents, which can be violent. Perpetrators often employ cellular GPS tracking devices to follow drivers or passengers in transit, exploiting the fact that these vehicles aren't linked to Wi-Fi or Bluetooth networks. Adding to the issue are factors such as the low initial cost of these devices, their easy availability online, and their small size which allows them to be concealed in a target's vehicle. To our knowledge, no previous research addresses the detection of clandestine cellular devices, making this study the first to introduce an affordable and practical solution for would-be victims. Our research is specifically dedicated to identifying hidden 4G LTE IoT cellular GPS tracking devices on or in a vehicle. We present an innovative algorithm designed for effective uplink frequency analysis, enabling dependable detection within a three-foot range when utilizing standard commercial hardware. This study aims to improve the privacy and security within the vehicular community.

1 Introduction

Each year in the United States, approximately 13.5 million individuals experience stalking [16], and on a global scale, in 2011, the number of victims was more than 18.75 million [50]. In 2019, of all stalking victims in the U.S., 80 percent, equating to 2,738,470 people, experienced stalking by technological means [33]. In the same year, electronic devices or applications were used to monitor 14 percent of victims, which is equivalent to 394,000 people [33]. A significant number of victims were stealthily tracked using concealed cellular GPS devices placed on or within their vehicles. Unfortunately, some victims faced violent attacks and were murdered after being monitored in their vehicles [24, 31, 51, 52]. In other unfortunate instances, thieves broke into homes after tracking homeowners who drove away from their homes [21]. The proliferation of low-cost, off-the-shelf Global Positioning System (GPS) tracking devices has introduced significant privacy

and security concerns for individuals targeted by cyberstalking, intimate partner surveillance (IPS), and burglary crimes. Cellular GPS vehicle trackers utilize 4G Long Term Evolution (LTE) Internet of Things (IoT) networks to transmit real-time location data, often without the knowledge or consent of the vehicle's owner. 4G LTE GPS cellular vehicle tracking devices function in the dedicated narrowband IoT spectrum. These trackers typically utilize one of the two sections of the 4G LTE spectrum, as shown in Table 1, NB-IoT (Narrow Band IoT) (also known as LTE Cat NB1 / NB2) or LTE-M (also known as eMTC and LTE Cat M1/M2 protocols) [38, 53]. These devices can be discreetly attached to vehicles, allowing malicious actors to remotely monitor the movement of individuals. Despite increasing risks, existing techniques for detecting hidden GPS tracking devices have been shown to be woefully inadequate [14].

By providing a cost-effective and accessible means for detecting covert GPS tracking, our research aims to mitigate the risks associated with illicit surveillance and strengthen the security of individuals, businesses, and communities.

This paper contributes 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. We detail our experimental validation, including real-world testing with commercially available tracking devices, to assess detection accuracy and feasibility. We also discuss broader implications for privacy protection, limitations of our current approach, and future directions for adapting this methodology to next-generation cellular networks, including 5G and beyond.

2 Related Work

With the exception of work [22, 28] shown in Table 2, current studies targeting 4G LTE network vulnerabilities require the capture of downlink cellular radio signals from the cell tower to mobile device [12, 20, 23, 27, 39]. This presents a challenge because it requires filtering out the background

Table 1: Comparison of LTE Cat-M (also known as LTE-M) and NB-IoT capabilities [35]

	LTE-M	NB-IoT
Also known as	eMTC, LTE Cat-M1	LTE Cat-NB1
Specification	Based on LTE	Based on a subset of LTE
Bandwidth	1.08Mhz (equivalent to an LTE channel)	180KHz (fits into a GSM channel)
Max throughput	360 kbps	30/60 kbps
Network deployment	Relatively easy for operators to add to existing LTE networks	Easier for operators with GSM networks to incorporate
Frequency deployment	LTE in-band	LTE in-band, LTE guard band, and GSM repurposing
Voice/data support	Voice and data	Data only
Range	Up to 4x	Up to 7x
Mobility/cell reselection	Yes	Limited
Module size	Suitable for wearables	Suitable for wearables
Power consumption	Up to 10 years of battery lifetime	Up to 10 years of battery lifetime

noise of all cellular signals that the tower is continuously transmitting to numerous mobile devices. GPS vehicle tracker devices connected to cellular networks transmit a signal at very low power to preserve their limited battery life. Traditional detection methods focus on electromagnetic radiation (EMR) analysis [29,41], which requires expensive specialized equipment and manual vehicle sweeps with short-range effectiveness. There is previous work [40] on detecting hidden *Wi-Fi* IoT devices and other work [43] on *active* attacks on LTE IoT cellular networks. To our knowledge, there is no *open source* practical solution that allows everyday users to *passively* detect *uplink* transmissions from hidden 4G LTE cellular GPS vehicle tracking devices, which specifically operate on LTE *IoT* cellular networks, in real-world scenarios, without requiring any prior knowledge about the hidden device.

4G LTE localization attacks: Previous research by Kotuliak et al. [28] has examined LTE vulnerabilities and passive localization attacks, using uplink transmissions, from *smartphone* cellular devices operating on *standard* LTE radio spectrum, but it does not discuss devices that use LTE *IoT* radio spectrum, which GPS trackers use. Related research by Hoang et al. [22] does not address the identification of nearby devices or the discovery of hidden devices. Specifically, their solution "LTESniffer", the first open source 4G LTE uplink transmission sniffer, was verified by testing and consulting with the authors to not detect the uplink of 4G LTE IoT devices when they are operating in the dedicated cellular IoT spectrum, such as the GPS vehicle tracking devices that we focus on here. We discovered the capability to uncover hidden 4G LTE IoT cellular GPS vehicle tracking devices without prior knowledge of the device. We also perform this passively without using a radio transmitter, unlike other active

attacks, such as setting up fake cellular radio base stations. In the United States, the Federal Communication Commission (FCC), under the Communications Act of 1934, as amended, prohibits unauthorized and unlicensed operation of a radio frequency station, including cellular transmission. It also prohibits the operation of equipment designed to interfere with cell phone communications [19].

Cyberstalking attacks: As far as we are aware, our study is a pioneer in its emphasis on a vehicle-centric cellular cyberstalking threat model. An attacker seeking to track a vehicle without sharing access or ownership with the victim would affix a budget-friendly GPS tracker on the vehicle's exterior or underneath, often utilizing a magnetic attachment. This tracker acquires location data from GPS satellites and periodically communicates this data to the cellular network upon motion detection [48]. A mobile cellular device will usually connect to the nearest cell tower that offers the strongest signal. In addition, the device records the next strongest signal from the next closest tower. As the device progresses away from a particular tower, it changes from one tower to another to ensure consistent cellular network connectivity [44]. Our proposed solution must consider the mobility inherent in a vehicle-based cyberstalking threat model and attacker and must quickly and accurately identify the cellular carrier and the LTE IoT uplink frequency band used by the tracker, even if there is a change in the frequency bands due to cell tower transitions.

GPS device localization: In Table 3, we draw a clear comparison between our research and the study by Li et al. [29] that addresses the detection of covert GPS vehicle tracking devices. While their methodology does not identify cellular signals, it successfully detects GPS tracking devices

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	✓	✓	✓	✓

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)

through the analysis of electromagnetic radiation from the side channel (EMR). Their detection capability extends to a range of 0.61 meters and is exclusively designed for GPS tracker devices. Due to this limited range, a meticulous inspection of the vehicle is necessary. It is ineffective in identifying other cellular devices, such as GPS tracking applications on smartphones or concealed cellular cameras. In addition, their approach involves relatively expensive hardware, priced at more than \$400. Also, their approach lacks portability and user-friendliness, since it requires a connection to a laptop. In contrast, our approach has shown a reliable detection range of at least 3 feet, enhancing its ability to detect beyond just GPS trackers. Our approach employs inexpensive off-the-shelf hardware priced around \$150 and functions as a fully portable stand-alone unit that does not need to be connected to a computer during scanning. We recognize that their approach might be more suited for GPS

trackers that are non-cellular and store position data locally.

In this paper, we present our novel methodology for passively detecting nearby 4G LTE IoT cellular GPS tracking devices, a topic previously unexplored. This research is a pioneering work that combines all of these aspects to identify hidden cellular devices. We introduce an algorithm and technique that allow for the quick detection of these devices and potentially any other hidden IoT devices that operate over the same networks.

3 Research Questions

In this paper, we seek to answer several research questions on the detection of hidden 4G LTE IoT cellular devices in general, which we can then apply to our specific study on the detection of hidden 4G LTE IoT GPS tracking devices.

- **RQ1:** What is the speed and precision with which one can identify the uplink frequency ranges for each carrier’s local cellular towers? Is it feasible to promptly and straightforwardly 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?
- **RQ2:** 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? See Table 4 for a comparison of the transmission power and noise figures of the uplink and downlink.
- **RQ3:** Could utilizing a portable and inexpensive standard radio frequency spectrum analyzer called tinySA (the tiny spectrum analyzer shown in Figure 1) be capable of identifying 4G LTE IoT cellular signals?
- **RQ4:** What is the maximum distance from which the tinySA can detect signals? Considering that the uplink

Table 4: NB-IoT and LTE Cat-M transmit power and noise figure assumptions [32].

	NB-IoT Downlink	NB-IoT Uplink	LTE Cat-M Downlink	LTE Cat-M Uplink
Transmit Power	46 dBm	23 dBm	43 dBm	23 dBm
Noise Figure	9 dB	5 dB	5 dB	3 dB

transmission from an LTE IoT device is significantly weaker compared to the downlink [32], to what extent is the detection of such low-power signals restricted?

4 Challenges

Detecting concealed cellular devices presents notable challenges, and we will examine each of these:

Challenge 1: Identifying the cellular network provider to which the device is connected, which differs depending on the country and region in which it is used.

NB-IoT caters to low-bandwidth IoT devices, offering a maximum data transmission rate of 100 kbps. In contrast, LTE Cat-M supports a higher maximum data rate of 1 Mbps [35]. In the United States, cellular carriers have assigned specific parts of their spectrum for both protocols. However, AT&T has announced plans to discontinue its NB-IoT service in early 2025 [25]. 4G LTE IoT spectrum shares parts of existing LTE frequency bands allocated to cellular carriers around the world.

Challenge 2: Identifying the cellular frequency bands linked to the carrier, which differ depending on the country and region in which they operate.

Challenge 3: Identifying which frequency bands are used at local cell sites that support the carrier network. In the United States, Table 5 illustrates that AT&T utilizes 4G LTE bands 2, 4, and 12 [10]. As shown in Table 6, T-Mobile utilizes 4G LTE bands 2, 4, 5, 12, 66, and 71 [42]. Table 7 indicates that Verizon uses 4G LTE bands 2, 4, 5, 13, and 66 [38]. These LTE bands include both the NB-IoT and LTE Cat-M protocols. Although our study focused specifically on 4G LTE IoT cellular networks in the United States, the principles should be applicable to any cellular network provider around the world.

Challenge 4: Determining the cellular uplink frequencies that correspond to the active frequency bands used by each carrier in the local cell tower.

Challenge 5: Performing a rapid scan of the cellular uplink frequency band in the carrier’s local cell tower to detect the uplink signal from a cellular device. For reference, 4G LTE scanning poses more challenges compared to Wi-Fi channel scanning. Wi-Fi comprises 88 individual channels in the 2.4 GHz, 5 GHz, and 6 GHz bands [17]. Each Wi-Fi channel functions on a different radio frequency within the designated Wi-Fi band. In contrast, 4G LTE bands encompass broad swaths of numerous radio frequency bands with thousands of radio frequencies and do not use single

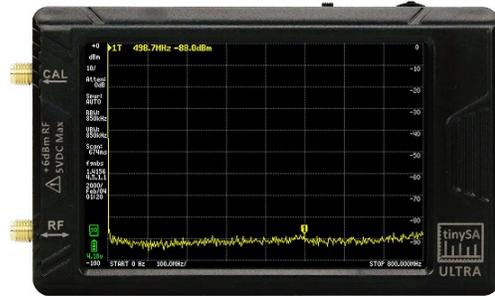


Figure 1: The tinySA Ultra portable mini spectrum analyzer covers a frequency range of 100 kHz to 5.3 GHz and costs approximately \$150 on Amazon [7].

Table 5: AT&T LTE Bands (US) [10].

Band	Uplink (in MHz)	Downlink (in MHz)
2	1850 – 1910	1930 – 1990
4	1710 – 1755	2110 – 2155
12	699 – 716	729 – 746

frequency channels. [37].

5 Methods

In this study, we propose a novel and low-cost method to detect hidden 4G LTE IoT cellular GPS vehicle tracking devices using widely available spectrum analysis tools. Our approach focuses on monitoring the LTE IoT uplink frequency bands, allowing us to isolate signals transmitted from concealed tracking devices to nearby cell towers. Unlike downlink monitoring, which requires complex filtering to distinguish target signals from broader cellular traffic, our method provides a

Table 6: T-Mobile LTE Bands (US) [42].

Band	Uplink (in MHz)	Downlink (in MHz)
2	1850 – 1910	1930 – 1990
4	1710 – 1755	2110 – 2155
5	824 – 849	869 – 894
12	699 – 716	729 – 746
66	1710 – 1780	2110 – 2200
71	663 – 698	617 – 652

Table 7: Verizon LTE Bands (US) [38].

Band	Uplink (in MHz)	Downlink (in MHz)
2	1850 – 1910	1930 – 1990
4	1710 – 1755	2110 – 2155
5	824 – 849	869 – 894
13	777 – 787	746 – 756
66	1710 – 1780	2110 – 2200

more precise and efficient mechanism to identify unauthorized tracking devices. The objective of this research is to develop a technical method to quickly and reliably identify hidden 4G LTE IoT cellular GPS tracking devices that are mounted within or attached externally to a vehicle, using affordable and easily accessible tools. In addition, the study seeks to create an algorithm that can enhance awareness of the local cellular network environment, facilitating directed scanning of the frequency spectrum. In the subsequent discussion, we discuss strategies to enhance the dependability of the results while also reducing the time required to yield these results by employing a portable and cost-effective device. We present an algorithm and detection framework that leverages a portable, standalone spectrum analyzer to scan for cellular GPS tracker transmissions.

For the first and second challenges, we reference tables of known cellular LTE IoT frequency bands assigned to each carrier that operates in the local region where we conduct our detection, such as those in Tables 5, 6, and 7 for the United States. We verify the appropriate 4G LTE IoT frequency bands aligning them with established authentic data, utilizing publicly available APIs alongside databases of existing cellular towers.

For the third and fourth challenges, we created a novel technique to determine the uplink frequencies of local 4G LTE IoT cell towers, querying a public API to determine their cellular identifier, filtered by those only operating on the LTE and NB IoT radio spectrum. We then query a public website using the cellular identifier we retrieved to obtain the specific uplink frequency and its corresponding LTE band to scan. The given frequency represents the center of the uplink band, but uplink signals can be detected anywhere in that radio passband. By concentrating on the uplink, we can avoid the need to track the noisy and congested downlink. Monitoring the downlink complicates the differentiation of devices and increases the potential for false positives.

For the fifth challenge, we performed a novel approach using the tinySA and evaluated the practicality of detecting 4G LTE IoT cellular radio signals transmitted by a concealed GPS tracker within a vehicular environment. We set the tinySA to scan the uplink bands determined in the previous steps. We wanted to pay attention to the lower power uplink segment of the IoT device to lessen interference from alternative cell towers and substantially diminish the need to filter out unre-

lated signals.

We sought to identify the ability of the tinySA to effectively identify cellular transmissions from the 4G LTE IoT GPS tracker and determine whether unwanted foreign cell signals can be ignored or filtered efficiently. We captured signals in real time by enabling the maximum hold / maximum decay function on the tinySA. This function holds the displayed signal peaks on the screen in maximum hold mode, and additionally diminishes them slowly over the course of 20 seconds in maximum decay mode, so that we can easily observe and capture signal peaks that are significantly stronger than the baseline noise signal levels. Each tinySA capture generates a CSV (comma separated value) file of the entire radio band we are scanning and contains signal strength values in dBm (decibel milliwatts) for every frequency. We drive the vehicle to generate cellular transmissions from the hidden cellular vehicle tracker and watch for large signal peaks at fixed regular timing intervals, such as every minute, as was the case for most of our devices. We simplified the frequency ranges necessary for scanning by focusing only on the pertinent frequency bands that correspond to nearby cell towers, facilitated by an understanding of the uplink frequency bands utilized by regional cell tower carriers. We ensured the trustworthiness of the identified 4G LTE IoT cellular network traffic data by corroborating them with verified ground truth data.

5.1 Determining Cellular Carrier Uplink Frequency In Use

In Table 8, we summarize our evaluation of the five top highly rated 4G LTE and "5G" cellular GPS vehicle trackers available for purchase on Amazon, shown in Figure 2. When searching for "4G LTE GPS" and sorting by "Best Sellers", Tracki was ranked third [8] and offered the most affordable price at \$9.88. Under the "Featured" sort option, Amcrest was ranked first [3]. For the query "GPS Tracker" sorted by "Featured," Tracki held the first position [8]. Searching for "5G Tracker," LoneStar ranked first in "Featured" and third among "Best Sellers" [5]. Meanwhile, iTrail secured the third spot in the category "Featured" for "5G GPS Tracker" [6]. The Brickhouse and Amcrest trackers were the second and third least expensive, priced at \$19.95 and \$29.99, respectively [3,4].

By analyzing the radio frequency spectrum, our tests showed that the devices operate in the 4G LTE band 2 or the 4G LTE band 12, on the AT&T and T-Mobile networks, respectively, as shown in Table 9. The term "5G" used by some of the trackers was determined to be a marketing term as the devices actually use 4G LTE spectrum, not 5G spectrum. We did not test any devices on the Verizon network.

Our GPS devices are equipped with an internal accelerometer that initiates cellular data transmissions after any movement or handling. Our evaluation aimed to include a range of devices, specifically those that operate in LTE bands 2 and 12, and operate on AT&T and T-Mobile networks. In

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]



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]

particular, one of our test devices incorporates a distinctive Wi-Fi receiver, enabling it to determine its location by scanning nearby Wi-Fi networks when GPS signals are lacking. In addition, it features a Bluetooth radio for tracking the device by the owner through a smartphone application. Our research is concentrated exclusively on the cellular radios present in these devices.

To locate hidden 4G LTE GPS vehicle trackers, we must identify the 4G LTE IoT cellular service provider network that is used by the hidden device. Then we need to determine

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

the specific 4G LTE IoT frequency bands and associated uplink frequencies employed by that carrier at cell towers in the immediate vicinity. The typical coverage radius of a cell tower is 1 to 3 miles, and in dense urban environments, the coverage of a cell tower usually reaches 0.25 to 1 mile before handing off a connection to another nearby cell site [1].

Every 4G LTE cell site consists of a base station that is identified by a 20-bit or 28-bit eNodeB (evolved NodeB) identifier. This serves as its unique identifier within the carrier cellular network. The ECI (Evolved Universal Terrestrial Radio Access Network Cell Identifier), also known as a cellular identifier or cellid, is used to distinctly identify a cell within a carrier's Public Land Mobile Network (PLMN). The cell identifier is calculated by multiplying 256 by the eNodeB identifier and then adding the result to the local tower's cell number (0-255 per eNodeB). The ECI can address up to 256 cells per eNodeB, depending on the length of the eNodeB identifier [11] [45]. By analyzing this information in real time based on our current location, we can perform reliable and rapid scans of the radio spectrum that the hidden device is



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.

likely to be transmitting in.

- We determine the geographic coordinates (latitude and longitude) of our current location.
- A public API (application programming interface) is called at opencellid.org (see Table 10) to request information on all NB-IoT and LTE towers within the specified minimum and maximum latitude and longitude limits.
- From this API, we receive the cell identifier along with the MNC (mobile network code) and MCC (mobile country code) that represents the carrier in use at each cell tower, known as an eNodeB, in the specified coverage area of any country.
- For each network provider, we lookup the cellular identifier on the public "cellmapper" website (see Figure 4) and obtain the uplink frequency and LTE band for each specific cell site. Cellmapper.net did not appear to have an option to filter on NB-IoT networks. Although we can query cellmapper.net for nearby 4G LTE cell towers, considering future work where we would like to automate as much as possible, it is quicker and easier to use opencellid.org to obtain the cell identifier. This requires the use of a free API key and is limited to 1000 requests per day [34]. Both opencellid.org and [cellmapper](http://cellmapper.net) utilize crowd-sourced data.

5.2 Experimental Setup

Laboratory analysis focused on exploring the correlation between distance and signal intensity. While we evaluated and tested capturing uplink signals using the tinySA from all 5 tracking devices, the detailed controlled experiments were confined to the Amcrest device in order to control for that variable. We performed 10 experiments for each of the 12 specified distances, starting from one inch, increasing by increments of one foot to 11 feet, and including a control

with the tracker turned off. During each experiment, we documented the signal levels across each frequency within the uplink band, comprising 450 frequencies from 700 to 715 MHz. For every trial, we calculated the average signal strength for all frequencies, as well as for the top 10 and the top 5 strongest frequencies. Subsequently, we computed the average of the strongest signals over 10 trials by averaging the results from the top 10 and top 5 strongest frequencies. In addition, the standard deviation was determined for each average of the strongest signals.

We also carried out experiments to locate the tracker both inside the glove compartment of the vehicle and outside the vehicle underneath the front and rear bumpers of a 2011 Honda Pilot SUV. This should be representative of the average length of any passenger vehicle. We did not test in other vehicle types or in other vehicle makes / models. For detecting the tracker inside the vehicle, we used the small portable retractable whip antenna that comes in the tinySA box. To detect the tracker when it was affixed externally, we used a magnetic mount cellular antenna, shown in Figure 5, placing it at the front of the vehicle's roof to find trackers attached to the front. Similarly, placing the antenna at the rear of the roof was used to detect hidden trackers attached to the rear of the vehicle. We drove the vehicle to initiate data transmissions of periodic position updates every minute by the device via the cellular data network. The devices were housed in a magnetic and waterproof case, and driving the vehicle activated data transmission of the vehicle's location by the devices via their built-in accelerometer and GPS receiver. Figure 6 summarizes the indoor experimental protocol, while Figure 7 summarizes the outdoor protocol. Figure 3 demonstrates the locations of the tinySA and the tracker during various outdoor experiments.

We wanted to first establish a baseline for detection capabilities and distance in a closed indoor laboratory environment to eliminate any potential false positives, such as spurious signals generated from other vehicles and pedestrians. We also did not know whether the metal body of a vehicle could cause signals to be attenuated or refracted, which could potentially skew our results.

5.2.1 Detailed Indoor Experimental Protocol:

1. To establish a control for signal capture and measure ambient noise levels, we turned off the tracker and used the tinySA in the maximum hold mode [47] to capture the highest signal intensities of the ambient environment during the scan. This setting continuously leaves the highest peaks and strongest signal values on the screen so that they can be easily viewed and captured.
2. We conducted each trial for 2 minutes, then saved the maximum hold data onto a micro SD card, and later exported it into Excel.

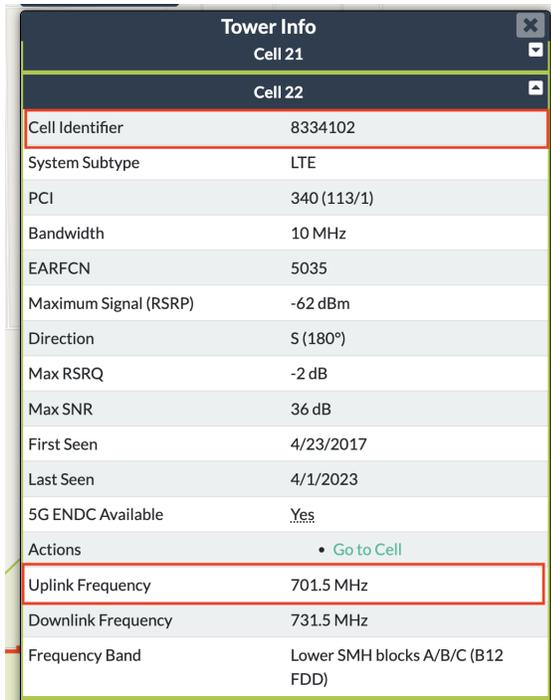


Figure 4: cellmapper.net showing a T-Mobile cell tower on LTE Band 12, for a given cell identifier and with its uplink frequency [15].

3. This process was carried out for a total of 10 trials.
4. We carried out 10 trials at each of 12 distinct distances: 0 feet (almost one inch), 1 foot, 2 feet, 3 feet, 4 feet, up to 11 feet, resulting in 10 ambient noise trials, plus 120 trials with the tracker active at varying distances.
5. We turned on the tracker after starting the tinySA's and enabled the maximum hold setting.
6. At 1 minute, we refreshed the Amcrest GPS app to verify the generation of an additional signal. This step is not necessary to find the device and is only used to confirm the ground truth. This validation step can be removed for real-world usage.
7. At the 2-minute mark, we captured the maximum hold trace, uploaded it, and turned off the GPS tracker.
8. There was a 5-minute break between the tests to ensure that the tracker was completely powered down and no longer transmitting signals.

After establishing a control and a detection range by conducting a series of indoor experiments, we then moved to the real world environment of the vehicle to see how our results might vary due to the attenuation and shielding of the metal vehicle body and due to the dynamic outdoor nature and proximity to other vehicles and pedestrians.

Table 10: OpenCellID.org API showing how the parameters to use for a query for LTE towers bound to a specific area [34].

Parameter	Data type	Description	Optional
<latmin>	double	Minimal bounding latitude	no
<lonmin>	double	Minimal bounding longitude	no
<latmax>	double	Maximal bounding latitude	no
<lonmax>	double	Maximal bounding longitude	no
<mnc>	integer	Mobile network code or system identifier; If you want to restrict the result	yes
<radio>	string	You can specify GSM, UMTS, LTE, NR, NB-IOT, or CDMA as the radio of returned cells. Otherwise cells with any radios will be returned.	yes

5.2.2 Detailed Outdoor Experimental Protocol:

1. To establish a noise baseline and for initial scanning, we began with the tracker powered off and used the tinySA's maximum decay function [47]. This feature captures the signal's peak intensities during a scan and gradually decreases over 20 seconds, allowing us to record signals before they fade, thus enabling detection of subsequent signals over time.
2. We allowed the first trial to run for 10 minutes and, for each minute, we saved the data onto the micro SD card to be later imported into Excel.
3. This procedure was executed 10 times in total.
4. Following this, we conducted 10 tests with the GPS tracker placed in the glove compartment of the vehicle.
5. The tracker was powered on, and the tinySA's maximum decay setting was enabled.
6. We allowed the next trial to run for 10 minutes and, for each minute, we saved the data onto the micro SD card to be later imported into Excel.
7. This procedure was executed 10 times in total.
8. We drove the vehicle for 10 minutes for each test to initiate data transmissions of periodic position updates every minute by the device via the cellular network.



Figure 5: The magnetic mount cellular antenna on the front part of the roof of the vehicle is connected to the tinySA. The GPS tracker is magnetically attached underneath the front bumper of the vehicle.

9. This procedure was executed 10 times in total.
10. Signal traces showing significant spikes were saved every minute over a 10-minute period, with validation in seconds performed in real time through the smartphone application of the corresponding GPS tracker, as shown in Figure 8. This step is not necessary to find the device and is only used to confirm the ground truth. This validation step can be removed for real-world usage.
11. Between each trial, there was a minimum of a 3-minute pause to ensure that the tracker stopped transmitting signals.
12. Subsequently, 10 trials were conducted with the GPS tracker magnetically affixed to the vehicle's exterior under both the front and rear bumpers.
13. Similarly to previous runs, the tracker was activated and the tinySA's maximum decay setting was enabled.
14. The vehicle was driven again for 10 minutes to cause periodic transmissions of cellular data traffic from the device at every minute.
15. For 10 minutes, signal traces that show major spikes at roughly 1-minute intervals were saved, with validation within seconds carried out in real time via the smartphone app of the corresponding GPS tracker as shown in Figure 8.
16. A minimum of a 3-minute break followed each test to confirm that the tracker signals had stopped.

5.3 Determining Signal Source

We concluded that the observed spike in visible amplitude originates from our tracker and tinySA within a Faraday bag, which prevents any signals from outside the shielded bag from being detected. This was achieved by establishing a baseline for random radio frequency (RF) noise levels with no interference signals except for the tinySA inside the Faraday bag (see Figure 11). By placing both the tracker and the tinySA within an RF-shielded Faraday bag, we determined that the peaks in signal strength were coming from the GPS tracker and not from any other transmitting cellular device.

In practical tests beyond a Faraday bag, if the source of a signal originated from another mobile device, we would not observe a consistently strong signal level at identical fixed time periods. If a nearby vehicle has its own cellular GPS tracker, the signal would intensify as we approach the source and diminish as we move away. A radio frequency signal can only maintain a constant amplitude while in motion if the distance between the source and the receiver does not change [2]. The intensity of radio waves over distance obeys the inverse-square law, which states that intensity is inversely proportional to the square of the distance from a source. In addition, radio waves exhibit free space path loss, which is proportional to the square of the frequency of the radio signal [36]. If we double the distance or the frequency, we get four times less power. If we halve the distance or frequency, the received power is increased four times. Also, if our vehicle is equipped with a cell GPS tracker and we detect a signal surge without having driven the vehicle recently (in the last 10 minutes), it can be classified as a false positive. In contrast, if no signal surge is observed while in motion or after the vehicle has been relocated, it can be considered a false negative.

6 Results and Discussion

6.1 Cellular Tower Ground Truth Data

We were able to answer **RQ1** by quickly, in under a minute, and precisely, by identifying the frequency ranges for each carrier's local cellular towers and uplink frequency and LTE bands, using the method and algorithm we described earlier. 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.

6.2 Cellular Traffic Detection

As shown in Figure 11, 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.

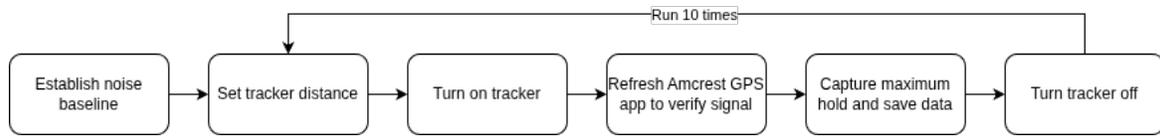


Figure 6: The timeline of the indoor experimental protocol.

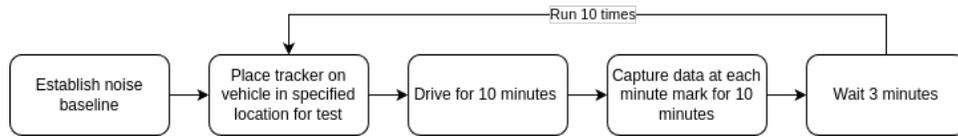


Figure 7: The timeline of the outdoor experimental protocol.

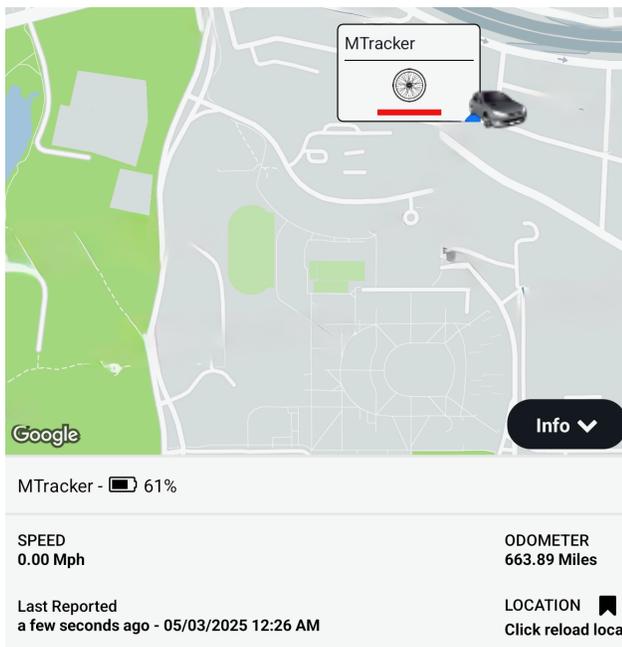


Figure 8: A screenshot from the Amcrest GPS Pro App showing how we verify correlation of signal peaks to GPS cellular reporting intervals. Note the "Last Reported a few seconds ago" at 12:26 AM correlates with 00:26:07 timestamp in Figure 16.

We were able to answer **RQ3** and **RQ4** using the tinySA to detect cellular signals. Verification of signal peak timestamps with those from GPS smartphone applications (see Figure 8) was used as a ground truth to confirm precision. Figures 9 and 10 illustrate the findings of the indoor experiment, which indicate that the tinySA can successfully detect the GPS tracker signal in a range of up to three feet. Beyond this range, the signal strength drops significantly, reducing the reliability of detection. The R^2 value of 0.9784 in the 0-3 ft distance graph confirms that almost all the variability in signal strength can be attributed to changes in distance, demonstrating a strong

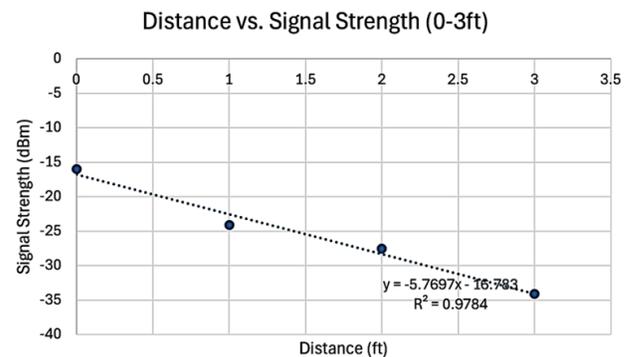


Figure 9: The indoor lab test when the tracker is 3 feet away from tinySA. The tracker was turned on when the timer was started and the location was requested from the app at the one minute mark. Each trial runs for a total of two minutes. The maximum hold setting on the tinySA was used to help store the strongest signal at each frequency. The tracker was operating on LTE band 12 and the tinySA was set to scan the range of 700-715 MHz.

linear relationship. The cutoff distance for reliable detection was set at 3 feet because, at 4 feet, the signal cutoff point (-54 dBm as established in the control trials) is reached within one standard deviation of the mean.

We conducted tests to position the GPS tracker both inside the glove compartment of the vehicle and magnetically affixed to the exterior of the vehicle on the front and rear bumpers. Figure 12 illustrates that the strongest detected signal, when the tracker was turned off inside the vehicle, was measured at -95.6 dBm. As shown in Figure 13, when the tracker was turned on and placed in the glove compartment of the vehicle, we captured recurring transmissions at fixed 1-minute intervals, with a peak of -59.7 dBm using the portable whip antenna attached to the tinySA. As depicted in Figure 14, when the tracker was located under the rear bumper of the vehicle, consistent transmissions occurred every minute with a peak signal strength of -72.5 dBm using the magnetic mount

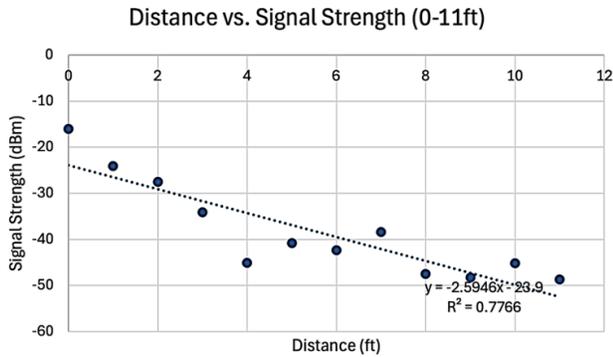


Figure 10: Lab tests for all distances from tinySA to tracker, ranging from one inch, one foot, two feet, . . . , and 11 feet apart. The captured signal strength from the GPS tracker diminishes as we increasingly move the tinySA farther away from the fixed transmitter of the device [2].

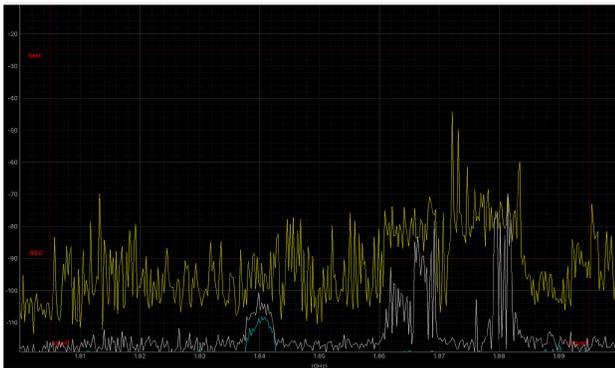


Figure 11: Determining that the visible amplitude spike is generated by our tracker by using a Faraday bag.

cellular antenna on the rear of the roof.

As shown in Figure 15, positioning the tracker below the vehicle's front bumper led to consistent 1-minute interval transmissions, detected with a peak of -62.6 dBm using the magnetic mount cellular antenna on the front of the roof.

An increase of 20 dBm or more in RSSI (relative signal strength indication) equals a power disparity of at least 100 times. Our extensive testing focused on the 700 MHz LTE Band 12, for the 1800 MHz LTE Band 2 we can expect to see an additional 9 db reduction in signal strength at a 1 meter distance between receiver and transmitter [18]. After accounting for the additional loss of signal strength due to free-space path loss, there is still a 20 db or greater increase in amplitude of the uplink signal compared to the ambient noise floor. As depicted in Figure 16, with the tracker mounted underneath the front bumper of the vehicle, we see regular strong signal peaks (blue dots) significantly above the ambient noise level (red dots) at approximately 1 minute intervals. The time interval is 00:03:30 to 00:26:07, which is in correlation

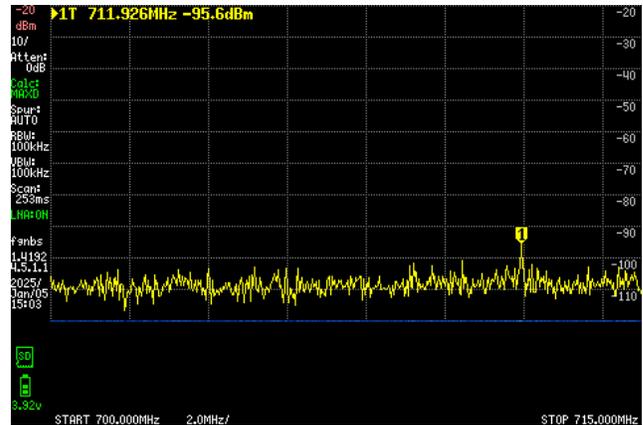


Figure 12: The strongest signal present when the tracker is powered off in the glove compartment was -95.6 dBm using the maximum decay setting and the portable whip antenna attached to the tinySA.

with the ground truth of 12:26 AM of the Amcrest GPS Pro smartphone app shown in Figure 8.

In our controlled experiments, we observed a clear correlation between signal spikes detected on the tinySA and the transmission activities of the GPS trackers. In the lab environment, these spikes/peaks were detected precisely at 1-minute intervals, and the ground truth was verified in the corresponding smartphone app. In vehicle-based tests, regular peaks appeared every minute, corresponding to the expected transmission intervals of the GPS trackers. This exclusive correlation between the detected peaks on the tinySA and the apparent transmission activities of the GPS trackers strongly suggests causation. We confirmed the ground truth by seeing the exact timestamp detected on the tinySA (in seconds) on the corresponding GPS smartphone tracking app, shown in Figure 8.

As a result of our methodology and testing, utilizing our detection algorithm and commodity hardware, we can empower vehicle occupants with a tool to determine if they are being tracked by a hidden cellular tracker. We were able to detect the presence of a 4G LTE IoT cellular GPS vehicle tracking device in the laboratory environment and vehicle environment using the tinySA Ultra spectrum analyzer. By analyzing the signal peaks observed during the experiment, we established a maximum reliable detection range for the tinySA. The data revealed that the tinySA could detect the GPS tracker signal within a range of up to three feet. Beyond this distance, the signal strength decreased significantly, making detection less reliable. From zero to three feet, there is a linear correlation between distance and signal strength, as shown in. These findings were used to establish a three-foot detection threshold, which can serve as a guide for users about the proximity required for effective detection.

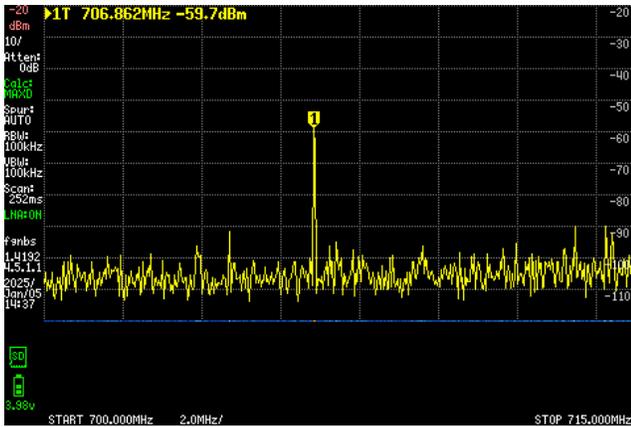


Figure 13: The tracker was in the glove compartment of the vehicle. Regular transmissions at 1-minute intervals were detected peaking at -59.7 dBm using the maximum decay setting with the portable whip antenna attached to the tinySA.

For an actual victim, our setup could be used as a mobile detection system while driving outdoors. If the user observes similar regular peaks on the tinySA while driving or immediately following a drive, they can confidently suspect the presence of a cellular GPS tracker on their vehicle. This practical application provides a viable method for individuals to verify if they are being tracked without requiring advanced technical expertise.

7 Limitations and Future Work

7.1 Limitations

Other Vehicle Types: Although we tested only on a single vehicle type, considering that we tested hidden trackers inside the vehicle and underneath both ends (front and rear bumpers), we feel it should be representative of the average length of any passenger vehicle. We did not test in other vehicle types / models.

Other Signal Peaks: We must determine a method to effectively filter out other strong signals that could be present in the area. A key distinction between other cellular signals and those emitted from the tracker lies in the tracker's transmission, which occurs as beacons at consistent, predetermined time intervals, such as every minute. In addition, when we are moving, the signal strength between the tracker and the receiver remains constant. Consequently, we can disregard any signal that does not transmit at a regular, recurring time interval or fluctuates in amplitude while the vehicle is in motion. This would require ensuring that there are no other devices in or on the vehicle, such as an insurance dongle, that could also transmit at regular fixed intervals.

tinySA Ultra Mode: In order to capture band 2 uplink spectrum, we enabled the "ultra" mode on the tinySA, which

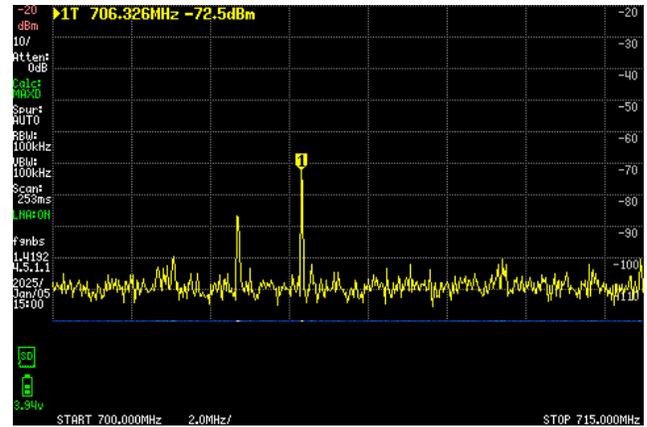


Figure 14: The tracker was placed underneath the rear bumper of the vehicle. Regular transmissions at 1-minute intervals were detected peaking at -72.5 dBm, using the maximum decay setting, with the magnetic cellular antenna on the rear roof of the vehicle.

raises the upper frequency limit of the device from 800 MHz to 5.4 GHz. Enabling ultra mode to scan above 800 MHz introduces a number of disadvantages, including increased scan time and the failure to capture signals of very short duration [46]. We did not experience any of these disadvantages when we scanned above 800 MHz in ultra mode.

Device Roaming: When a cellular device roams, it switches from one cell tower to another. It is imperative for us to maintain a consistent view of the device's signal throughout these transitions. The embedded accelerometers in the GPS tracking devices should eliminate the need to do actual drive tests, provided that we are not in the unlikely situation of a fringe area ping-ponging between cellular sites. If we were, we would need to conduct our testing in an area where we could lock onto a specific cell tower after moving the vehicle slightly to generate cellular data transmissions.

Limited to Active GPS Devices: The scope of our study focuses exclusively on GPS devices that actively transmit data over cellular networks. These are real-time tracking devices that send location information via mobile phone networks. In contrast, the study does not consider passive GPS devices that do not transmit data live but instead store information locally, typically requiring manual data retrieval and download at a later time.

Limited to Unmodified Third-Party Consumer GPS Vehicle Trackers: Our paper is limited to the detection of standard third-party consumer GPS vehicle trackers widely available and inexpensive to purchase on websites such as Amazon.com. We did not evaluate embedded vehicle locating devices or devices that have been modified to limit their transmission rates to avoid detection.

Our five GPS test devices were limited to 2 of the 3 US cellular carriers: Due to the unavailability of GPS devices

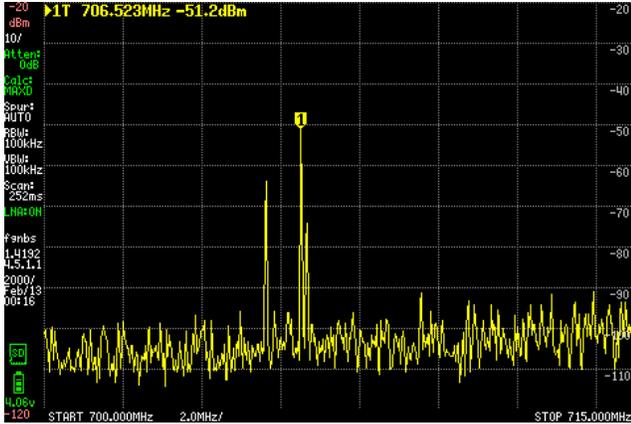


Figure 15: Tracker is magnetically attached underneath the front bumper of the vehicle. Regular transmissions at 1-minute intervals were detected peaking at -51.2 dBm using the maximum decay setting of the tinySA with the magnetic cellular antenna on the front roof of the vehicle.

compatible with the Verizon network on Amazon.com, we were unable to perform any testing on the Verizon network. Consequently, our scope of testing was restricted to the networks operated by AT&T and T-Mobile within the United States.

7.2 Future Work

At present, GPS vehicle trackers in the United States that rely on cellular technology function exclusively on 4G LTE IoT narrowband cellular networks. Looking ahead, it is predicted that these systems will transition to newer generations such as 5G, 6G, and potentially further advancements. This shift will likely occur as cellular providers phase out older network technologies, much like the discontinuation of 2G and 3G networks in previous years. Consequently, this will require a comprehensive update of our research. We must reexamine and explore anew to uncover solutions that align with these technological advances.

We aim to engage with affected individuals and focus groups to evaluate real-world usability through Human-Computer Interaction (HCI) techniques. Our aim is to explore the development of a system similar to an AirTag, which uses a smartphone to alert users about the possibility of a tracking device following them. Additionally, we plan to create a smartphone application that not only informs users if they are being observed but also has the capability to locate the tracker's position. This feature is designed to mirror the functionality provided by Apple's and Android's Find My services. We can work with groups such as the Clinic to End Tech Abuse (CETA) to help survivors of intimate partner violence (IPV) who are experiencing technology-facilitated abuse and may not have access or funding for the equipment. We can also ex-

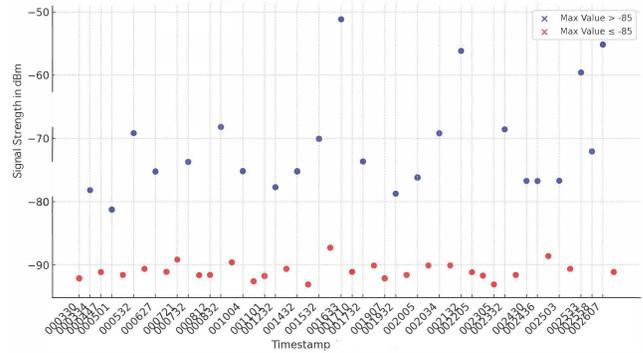


Figure 16: With the tracker mounted underneath the front bumper of vehicle we see regular strong signal peaks (blue dots) significantly above the ambient noise level (red dots) at 1 minute intervals. Y-axis is signal strength in dBm. X-axis is the time interval we drove the vehicle from 00:03:30 to 00:26:07. Note that this correlates to the "Last Reported a few seconds ago" 12:26 AM ground truth in the Amcrest GPS Pro app shown in Figure 8.

plore using any future lower-cost portable spectrum analyzers that may arrive on the market.

In the future, we can also build a "black box" that contains the tinySA and interfaces to a smartphone via a Bluetooth or a serial over USB interface, utilizing the tinySA console mode. This could allow us to further automate the spectrum capture and analysis process without requiring end-user interaction with the device. We can explore potential supplementing with a consumer-oriented service, such as a mobile rig based on a flatbed tow truck along with several tinySA. The tow truck would not need to drive alongside our target vehicle because the trackers transmit as soon as they sense movement with their embedded accelerometers, eliminating the need to do actual drive testing. We can explore extending the range of detection with consideration of trade-offs, such as using passive RF power combining or multiplexing multiple antennas as one source.

8 Conclusion

Identifying hidden 4G LTE IoT cellular GPS vehicle tracking devices is crucial to equip potential cyberstalking victims with a practical tool to detect surveillance devices. This research employs the tinySA, an economical handheld spectrum analyzer, to spot signals from 4G LTE IoT cellular GPS vehicle trackers and establish quantitative detection criteria. Observing the uplink frequency that these trackers use, significant signal peaks greater than 20 dBm were detected upon tracker activation. Controlled experiments, conducted in both the laboratory and vehicles, examined how the distance between the tracker and the tinySA affects signal strength, establishing a

reliable detection threshold both indoors and in vehicles.

9 Acknowledgments

The authors thank the reviewers and the shepherd for their valuable feedback on the paper. The authors also thank Professors Ali Abedi, Rosanna Bellini, Rahul Chatterjee, Rachel Greenstadt, Ramesh Karri, Yongdae Kim, Nasir Memon, and Torsten Suel. We also thank Chrystanyaa Brown, Joel Caminer, Sivan Elisha, Odette Kuehn, Susmitha Kusuma, Marlett Lewis, Yabsra Maelaf, Danielle Park, Joe Prakash, Kari Schwartz, Madeline Slaughter, and Hoang Dinh Tuan. We also thank ARDC, ARRL, Cornell Tech CETA, KAIST System Security lab, NYU Center for Cybersecurity, NYU mLab, NYU OSIRIS, NYU Tandon CSE, and NYU Tandon UGSRP.

References

- [1] Adam Simmons. Cell tower range: How far do they reach? <https://dgtlinfra.com/cell-tower-range-how-far-reach/>.
- [2] Alex Milne. When it comes to rf, distance plays tricks with the mind. <https://www.rfvenue.com/blog/2014/12/15/when-it-comes-to-rf-distance-plays-tricks-with-the-mind>.
- [3] Amazon. Amcrest gps gl300 gps tracker for vehicles (4g lte) - portable mini hidden real-time gps tracking device for vehicles, cars, kids, pets, assets, text/email/push alerts, twin magnet weatherproof case. <https://www.amazon.com/Amcrest-LTE-GPS-Tracker-Geo-Fencing/dp/B07P87SZMJ>.
- [4] Amazon. Brickhouse car trackers for your vehicle - spark nano 7 gps tracker with magnetic waterproof case - hidden real-time 4g lte vehicle finder - gps tracking device for cars & more - subscription required. <https://www.amazon.com/Brickhouse-GPS-Tracker-Vehicle-Subscription/dp/B01MYVBUJZ>.
- [5] Amazon. Lonestar tracking gps tracker: Oyster3 4g/5g - long battery life hidden car gps tracker device, anti-theft car security for vehicles,cars,trucks, assets, real-time gps tracking (subscription required). <https://www.amazon.com/LoneStar-Tracking-Oyster3-Tracker-Assets/dp/B07X8B5627>.
- [6] Amazon. Magnetic gps tracker - 5g, secure & hidden, long battery life, seamless global tracking, weatherproof design, no hidden fees, real-time alerts, itrail app integration, sms notifications, auto 3g, 4g. <https://www.amazon.com/Magnetic-GPS-Tracker-Weatherproof-Notifications/dp/B0CJXJ9NYN>.
- [7] Amazon. Seesii tinysa ultra spectrum analyzer, 4.0 inch 100khz to 5.3ghz handheld tiny frequency analyzer with 32gb card, 2-in-1 signal generator 100khz to 800mhz mf/hf/vhf uhf input,v0.4.5.1,2024 upgraded. <https://www.amazon.com/Upgraded-TinySA-Spectrum-Frequency-Generator/dp/B0BBGK9QJB>.
- [8] Amazon. Tracki gps tracker for vehicles, car, kids, assets. subscription needed 4g lte gps tracking device. unlimited distance, us & worldwide. small portable real time mini magnetic. <https://www.amazon.com/Tracki-Magnetic-Required-Worldwide-Motorcycles/dp/B07N4DHFZM>.
- [9] Amcrest. Am-gl300w-4g technical specifications. https://drive.google.com/file/d/1bhztzZ70Pg8wAVu0V0nQ8ltjNdchneKV_/view.
- [10] AT&T. At&t iot devices. <https://iotdevices.att.com/networkready.aspx>.
- [11] Azar. Common identifiers used in lte. <https://www.techtrained.com/the-ultimate-cheat-sheet-for-lte-identifiers/>.
- [12] Sangwook Bae, Mincheol Son, Dongkwan Kim, CheolJun Park, Jiho Lee, Sooel Son, and Yongdae Kim. Watching the watchers: Practical video identification attack in LTE networks. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 1307–1324, Boston, MA, August 2022. USENIX Association.
- [13] BrickHouse Security. Spark nano 7 gps tracker specifications. <https://www.brickhousesecurity.com/gps-trackers/spark-nano>.
- [14] Rose Ceccio, Sophie Stephenson, Varun Chadha, Danny Yuxing Huang, and Rahul Chatterjee. Sneaky spy devices and defective detectors: the ecosystem of intimate partner surveillance with covert devices. In *Proceedings of the 32nd USENIX Conference on Security Symposium, SEC '23, USA, 2023*. USENIX Association.
- [15] cellmapper.net. Cellular tower and signal map. <https://bit.ly/4hZXVQv>.
- [16] Inc. Domestic Violence Services Network. January 2024: Stalking – stats, tactics, & impacts. <https://www.dvsn.org/january-2024-stalking-stats-tactics-impacts/>.
- [17] electronicsnotes. Wi-fi channels, frequencies, bands & bandwidths. <https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/channels-frequencies-bands-bandwidth.php>.

- [18] everythingrf.com. Free space path loss calculator. <http://www.everythingrf.com/rf-calculators/free-space-path-loss-calculator>.
- [19] FCC. General enforcement areas. <https://www.fcc.gov/enforcement/areas>.
- [20] Daniel Fraunholz, Richard Schörghofer-Vrinssen, Hartmut König, and Richard Zahoransky. Show me your attach request and i'll tell you who you are: Practical fingerprinting attacks in 4g and 5g mobile networks. In *2022 IEEE Conference on Dependable and Secure Computing (DSC)*, pages 1–8, 2022.
- [21] Michael Gauthier. Thieves allegedly using trackers on cars to help them rob multi-million dollar homes. <http://www.carscoops.com/2023/12/thieves-allegedly-using-trackers-on-cars-to-help-them-rob-multi-million-dollar-homes/>.
- [22] Tuan Dinh Hoang, CheolJun Park, Mincheol Son, Taekkyung Oh, Sangwook Bae, Junho Ahn, BeomSeok Oh, and Yongdae Kim. Ltesniffer: An open-source lte downlink/uplink eavesdropper. In *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '23, page 43–48, New York, NY, USA, 2023. Association for Computing Machinery.
- [23] Byeongdo Hong, Sangwook Bae, and Yongdae Kim. GUTI reallocation demystified: Cellular location tracking with changing temporary identifier. In *Network and Distributed System Security Symposium*, 2018.
- [24] U.S. Attorney's Office in the Western District of Missouri. Kc man pleads guilty to cyberstalking that resulted in murder. <https://www.justice.gov/usao-wdmo/pr/kc-man-pleads-guilty-cyberstalking-resulted-murder>.
- [25] James Blackman. At&t quits nb-iot – sales stopped ahead of q1 network shut-down. <https://www.rcwireless.com/20241120/internet-of-things-4/att-quits-nb-iot>.
- [26] KJB Security. itrail endurance gps tracker specifications. <https://www.kjbsecurity.com/shop/endurance-gps-tracker>.
- [27] Katharina Kohls, David Rupperecht, Thorsten Holz, and Christina Pöpper. Lost traffic encryption: Fingerprinting lte/4g traffic on layer two. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '19, page 249–260, New York, NY, USA, 2019. Association for Computing Machinery.
- [28] Martin Kotuliak, Simon Erni, Patrick Leu, Marc Röschlin, and Srdjan Capkun. LTrack: Stealthy tracking of mobile phones in LTE. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 1291–1306, Boston, MA, August 2022. USENIX Association.
- [29] Yue Li, Zhenxiong Yan, Wenqiang Jin, Zhenyu Ning, Daibo Liu, Zheng Qin, Yu Liu, Huadi Zhu, and Ming Li. Gpsbuster: Busting out hidden gps trackers via msoc electromagnetic radiations. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security, CCS '24*, page 3302–3316, New York, NY, USA, 2024. Association for Computing Machinery.
- [30] LoneStar Tracking LLC. Oyster2 4g/5g datasheet. <https://support.lonestartracking.com/support/solutions/articles/31000159394-oyster2-4g-5g-datasheet>.
- [31] Samantha May. Ex-boyfriend placed gps tracker on slain girlfriend's vehicle, records show. <https://wmt.com/news/local/jeffrey-kucharski-taylor-dragicevich-kalamazoo-stabbing-galesburg-police-restraining-order-ex-boyfriend>.
- [32] Michael Bosson. Nb-iot vs lte-m: Comparing the two iot technologies. <https://onomondo.com/blog/nb-iot-vs-lte-m-a-comparison-of-the-two-iot-technology-standards/>.
- [33] Rachel E. Morgan and Jennifer L. Truman. Stalking victimization, 2019. <https://bjs.ojp.gov/content/pub/pdf/sv19.pdf>.
- [34] opencellid. Api - opencellid wiki. <https://wiki.opencellid.org/wiki/API>.
- [35] Qorvo. How nb-iot and lte-m fit into the iot ecosystem: The future of cellular iot. <https://www.qorvo.com/design-hub/blog/how-nb-iot-and-lte-m-fit-into-iot-ecosystem-future-of-cellular-iot>.
- [36] radartutorial.eu. Free-space path loss (fsp). <https://www.radartutorial.eu/01.basics/Free-Space%20Path%20Loss.en.html>.
- [37] Radio Frequency Wireless Electronics. 4g lte frequency bands. <https://www.rfwel.com/us/index.php/4g-lte-frequency-bands>.
- [38] Radio Frequency Wireless Electronics. Cellular iot frequency bands. <https://www.rfwel.com/us/index.php/cellular-iot-frequency-bands>.
- [39] David Rupperecht, Katharina Kohls, Thorsten Holz, and Christina Pöpper. Breaking lte on layer two. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 1121–1136, 2019.

- [40] Rahul Anand Sharma, Elahe Soltanaghaei, Anthony Rowe, and Vyas Sekar. Lumos: Identifying and localizing diverse hidden {IoT} devices in an unfamiliar environment. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 1095–1112, 2022.
- [41] Wei Sun, Hadi Givvehchian, and Dinesh Bharadia. Revealing hidden iot devices through passive detection, fingerprinting, and localization. *Proceedings on Privacy Enhancing Technologies*, 2025.
- [42] T-Mobile. T-mobile network. <https://www.t-mobile.com/support/coverage/t-mobile-network>.
- [43] Zhaowei Tan, Boyan Ding, Jinghao Zhao, Yunqi Guo, and Songwu Lu. Breaking cellular iot with forged data-plane signaling: Attacks and countermeasure. *ACM Trans. Sen. Netw.*, 18(4), November 2022.
- [44] Techlteworld. Handover in lte. <https://techlteworld.com/handover-in-lte/>.
- [45] TELCOMA Global. What is the formula for cell id (eci) in lte networks? <https://telcomaglobal.com/p/formula-cell-id-eci-lte-networks/>.
- [46] tinysa.org. tinysa ultra mode. <https://tinysa.org/wiki/pmwiki.php?n=TinySA4.Ultra>.
- [47] tinysa.org/. Welcome to the tinysa® wiki! <https://www.tinysa.org/wiki/>.
- [48] Tracki. How gps tracker works and cell phone tower triangulation accuracy. <https://tracki.com/pages/how-gps-tracker-works-and-cell-phone-tower-triangulation-accuracy>.
- [49] Trackimo. Trackimo™ universal 4g model № trkm010. https://www.trackimo-gps.co.jp/trkm2023/wp-content/uploads/2023/02/DataSheets_TrackimoT-Universal-4G-New-1-2.pdf.
- [50] Suzan Van Der Aa. International (cyber) stalking: Impediments to investigation and prosecution. *The new faces of victimhood: Globalization, transnational crimes and victim rights*, pages 191–213, 2011.
- [51] Lydia Warren. 'she was deathly scared he would kill her': Friends reveal fears of hospital receptionist 'gunned down by prominent surgeon lover now on the run'. <https://www.dailymail.co.uk/news/article-2159247/Timothy-Jorden-Jackie-Wisniewski-deathly-scared-surgeon-lover-kill-her.html>.
- [52] Betsy Webster. Men accused of buying small gps trackers used to target murder victims. <https://www.komu.com/news/state/men-accused-of-buying-small-gps-trackers-used-to-target-murder-vic>
- [tims/article_2f1befc6-4228-5d29-a6e8-43eb7529001c.html](https://www.komu.com/news/state/men-accused-of-buying-small-gps-trackers-used-to-target-murder-vic).
- [53] Wikipedia. Lte-m. <https://en.wikipedia.org/wiki/LTE-M>.