GPSBuster: Busting out Hidden GPS Trackers via MSoC Electromagnetic Radiations

Yue Li*
Hunan University
Changsha, China
yuelii@hnu.edu.cn

Zhenxiong Yan*
Hunan University
Changsha, China
yanzhenxiong@hnu.edu.cn

Wenqiang Jin†
Hunan University
Changsha, China
wqjin@hnu.edu.cn

Zhengyu Ning
Hunan University
Changsha, China
zning@hnu.edu.cn

Daibo Liu
Hunan University
Changsha, China
dbliu.sky@gmail.com

Zheng Qin
Hunan University
Changsha, China
zqin@hnu.edu.cn

Yu Liu
Hunan University
Changsha, China
liuyuly@hnu.edu.cn

Huadi Zhu
Boise State University
Idaho, USA
huadizhu@boisestate.edu

Ming Li
The University of Texas at Arlington
Arlington, USA
ming.li@uta.edu

ABSTRACT

The escalating threat of hidden GPS tracking devices poses significant risks to personal privacy and security. Featured by their miniaturization and misleading appearances, GPS devices can be easily disguised in their surroundings making their detection extremely challenging. In this paper, we propose a novel side-channel-driven detection system, *GPSBuster*, leveraging electromagnetic radiation (EMR) emitted by GPS trackers. Our feasibility studies and hardware analysis reveal that unique EMR patterns associated with the tracker's operation, stemming from the quartz oscillator, local oscillator, and mixer in the Mixed-Signal on Chip (MSoC) system. Nevertheless, as a side-channel leakage, EMRs can be extremely weak and suffer from the ambient noise inference, rendering the detections impractical. To address these challenges, we develop the signal processing techniques with noise removals and a dual-dimensional folding mechanism to accumulate the spectrum energy and protrude the EMR patterns with high Signal-to-Noise Ratios (SNR). Our detection prototype, built with a portable HackRF One device, allows users to perform a scan-to-detect manner and achieves an overall success rate of 98.4% on top-10 selling GPS trackers under various testing cases. The maximum detection range is 0.61m.

CCS CONCEPTS

• **Security and privacy → Side-channel analysis and countermeasures**.

*Equal contribution.
†**Corresponding author**.

CCS '24, October 14–18, 2024, Salt Lake City, UT, USA

ACM ISBN 979-8-4007-0636-3/24/10
https://doi.org/10.1145/3658644.3690362

KEYWORDS

Electromagnetic Radiation (EMR); Side-channel; Privacy Protections

ACM Reference Format:
Yue Li, Zhenxiong Yan, Wenqiang Jin, Zhengyu Ning, Daibo Liu, Zheng Qin, Yu Liu, Huadi Zhu, and Ming Li. 2024. GPSBuster: Busting out Hidden GPS Trackers via MSoC Electromagnetic Radiations. In *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS '24), October 14–18, 2024, Salt Lake City, UT, USA.* ACM, Salt Lake City, USA, 16 pages. https://doi.org/10.1145/3658644.3690362

1 INTRODUCTION

Hidden GPS tracking devices pose a significant threat to personal privacy, exposing individuals to potential cyberstalking and various criminal activities. The monitored geo-location patterns captured by these trackers can lead to unauthorized surveillance, break-ins, vehicle theft, and the theft of commercial secrets. The Department of Defense (DoD) [28] has issued warnings highlighting the risks associated with GPS trackers, emphasizing their potential to make users easy targets. By leaking individuals' daily routines, these devices can provide insights into their residences and family situations, posing a serious threat to personal security. Further compounding these concerns, recent studies [3] reveal that GPS trackers, typically marketed for legitimate purposes such as vehicle security or child safety, are easily used for *intimate partner surveillance*(IPS) and even *advertised* for use in IPS and other covert surveillance. These devices effectively enable IPS without the abuser having any specialized technical skill. However, commercially available device detection tools are unusable and often fail to detect anything [3] Moreover, the information collected by GPS trackers could be exploited by divorce lawyers and insurance companies, impacting individuals both financially and legally. The pervasiveness of GPS tracking technology underscores the importance of developing effective countermeasures to protect personal privacy.

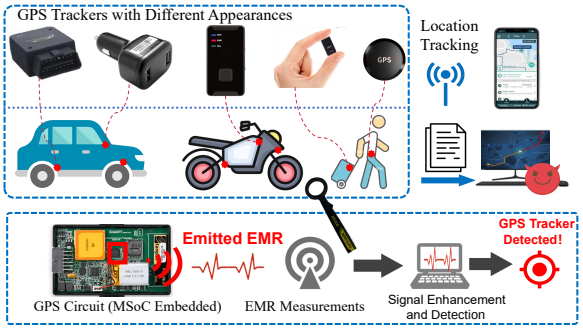


Figure 1: Malicious GPS trackers have misleading appearances and could be super miniaturized. An attacker may secretly hide them in the victims' vehicles or daily carry-ons, and both online and offline tracking methods could be adopted to acquire and analyze the travel trajectories. *GPSBuster* exploits the EMR of GPS trackers to perform the detection.

Detecting hidden GPS trackers has become a challenging task due to advancements in mixed-signal on-chip (MSoC) technologies, allowing for the integration of various circuit modules into compact chips. These miniature GPS trackers can be easily concealed, for example, underneath vehicles or inside carry-on bags. The passive nature of GPS positioning devices, which rely on receiving broadcasted signals from satellites to compute real-time geo-coordinates, further complicates detection efforts as no active measurement signals are transmitted. Nevertheless, in real-world attacks, adversaries may use offline GPS trackers to continuously record a victim's geo-coordinates on a local storage card, retrieving the information at a later, more convenient time. Additionally, with wireless connectivity (such as cellular networks or Wi-Fi), GPS trackers can stealthily transmit geo-coordinates to an adversary's server. However, attempting to detect hidden GPS trackers by monitoring their wireless transmissions is impractical. Adversaries can request data transmissions at any time, while detection systems cannot mandate that suspected victims (e.g., vehicles) remain stationary for extended periods (hours or days) to check for GPS-data-related transmissions. Moreover, the prevalence of commercial off-the-shelf (COTS) devices with multiple connectivity options (cellular, Wi-Fi, Bluetooth) contributes to a polluted wireless spectrum, making meaningful detection challenging. These unique challenges render existing designs for detecting secret-stealing devices, such as cameras or microphones based on wireless traffic analysis [6, 12, 18, 22, 35, 39, 44], light emissions [14, 20, 21, 36], and RF transmissions [23, 34, 40, 50], inapplicable to hidden GPS trackers.

In this paper, we propose a novel side-channel-driven design to tackle the challenge of detecting hidden GPS trackers, as shown in Figure 1. Specifically, we find that electromagnetic radiation (EMR) emitted by electronic devices was considered as an effective side-channel reflecting the devices' system information. Recent studies have demonstrated the potential of using EMR to recover secret AES-128 keys [51, 52], capture screen contents [2, 11, 24], and intercept users' keystrokes [15, 31]. Motivated by this body of evidence, we ask *"Can GPS trackers exhibit distinguishable EMR leakages linked to their inherent circuit modules, facilitating effective detection?"* To answer this question, we outline three research goals (RG).

- **RG1:** Characterize GPS trackers' EMRs at different working statuses to investigate how well they are correlated.
- **RG2:** Locate the EMR sources of GPS trackers, identifying unique radiation mechanisms and spectra distinguishable from other devices.
- **RG3:** Develop a robust detection system to correctly identify and confirm the presence of an arbitrary hidden GPS tracker, especially considering GPS trackers' EMRs typically have low signal-to-noise ratios (SNR).

To achieve **RG1** and **RG2**, we conducted a feasibility study to analyze the correlations between GPS trackers' working status and their EMR spectrum leakages. The results revealed that when GPS trackers were actively receiving positioning signals from satellites and decoding geo-coordinates, they emitted measurable EMR leakages scattered at two unique spectrum ranges: $\mathbf{Band_L}$: 25MHz-105MHz and $\mathbf{Band_H}$: 1545MHz-1625MHz. In both ranges, there was one most prominent frequency peak aligned with several smaller peaks separated by an equal interval. By de-shelling the GPS tracker and isolating each circuit module with metal copper covers, we localized the origin of the EMR radiations to the MSoC unit. Further analysis indicated that these radiation patterns could result from EMR couplings between multiple circuit components inside the MSoC. A deep investigation into the GPS tracker's MSoC compositions and its signal processing pipelines led us to infer that the EMR leakages are generated by the *frequency mixing* procedure involving three primary components: a quartz oscillator (QO), a local oscillator (LO), and a mixer. Specifically, the EMR coupling between the quartz oscillator and mixer generates the $\mathbf{Band_L}$ radiation spectrum, while the EMR coupling between the local oscillator and mixer generates the $\mathbf{Band_H}$ radiation spectrum. These assumptions were made based on key observations that the distribution patterns of frequency peaks within the EMR spectrums matched with intercorrelations of output frequencies corresponding to the QO, LO, and mixer. To further verify these assumptions, we conducted an additional experiment by shielding the GPS tracker's antenna with copper metal to reduce the GPS signal strength processed by these circuit components. If the EMRs originate from these assumed circuit modules, their signal should also be reduced. The results of our signal-shielding experiment confirmed a decrease in EMRs, thus validating our assumptions. Overall, our feasibility study yields comprehensive evidence supporting the viability of detecting concealed GPS trackers through analysis of their emitted EMRs. Within this context, we have successfully identified the crucial sources and distinctive patterns of EMRs, forming the foundational elements for our proposed detection process.

Nevertheless, building an effective GPS tracker detection system is a non-trivial task. The emitted EMRs are inherently weak and rapidly diminish with increasing measurement distances, easily susceptible to contamination by electromagnetic interference from nearby electronic devices. This makes it challenging to accurately characterize the EMR patterns of GPS trackers and identify them with a high level of confidence (**RG3**). We propose a two-step process to enhance the signal-to-noise ratio (SNR) of EMRs. Initially, we employed a Minimum Mean Square Error (MMSE) method to

model the spectrum distributions of environmental noises, attenuating them to a low level. Subsequently, a dual-dimensional folding algorithm was devised to accumulate the energy of EMR spectrum peaks in both the time and frequency domains, effectively boosting the SNR. These methodologies extended the detection distance from a few centimeters to a maximum of 0.61 meters in real-world tests. With the enhanced GPS trackers' EMRs, we further built a comprehensive detection algorithm based on the EMR distribution patterns, while considering both scenarios where the victim has established an MSoC database for GPS trackers or lacks such prior information.

To evaluate the effectiveness of the detection system, we build a prototype using Hack RF devices which are portable in size, facilitating the users to hold its antenna and move around to receive the potential EMRs for the detection purpose. We conduct evaluations on 10 top-selling tracker devices with different appearances and sizes under the interference of other 5 types of electronics. Our results indicate that the proposed *GPSBuster* system is robust against electronic inferences, transparent to physical blocking obstacles, and remains effective even when the tracker device has a low battery level or experiences low SNR of received GPS signals. The system can effectively detect all the hidden tracker devices with an overall success rate of 98.4%. As the initial exploration into detecting hidden GPS trackers, we believe the proof-of-concept detection system, *GPSBuster*, can be a useful tool for safeguarding users' privacy and the company's business secrets. The contributions of this paper are summarized as follows:

- We find that GPS trackers share unique EMR patterns originating from their MSoCs, and demonstrate such side-channel signal can be exploited to perform the detection.
- We characterize the MSoC circuits under the GPS positioning tasks, and perform feasibility studies to reveal its inherent radiation sources and the corresponding EMR patterns. Based on the analysis, we develop the detection methods to enhance the weak EMR signals.
- We build a prototype and demonstrate the effectiveness of the detection system on 10 GPS trackers across various settings.

2 RELATED WORK

2.1 Secret-stealing Device Detection

Due to their miniaturized sizes and misleading appearances, secret-stealing devices are hard to detect with the naked eye. Recent researches have proposed hardware and software-based approaches to detect hidden voice recorders [27, 50], cameras [6, 12, 18, 23, 35, 53], IoT sensing devices [39, 44], superheterodyne receivers[45] and wireless radio frequency eavesdroppers [3, 4, 30, 40]. Note that Stagner et al.[45], Shen et al.[40] and Chaman et al.[4] leverage the local oscillator (LO) emissions to detect superheterodyne receivers and Wi-Fi terminals, which are far less common in GPS trackers. Furthermore, such detection designs focused on analyzing the information related to the device's wireless module, i.e., traffic data and transmitted (or leaked) RF signals. For example, spy vs. spy [50] detects hidden voice recorders by characterizing their RF signals when transmitting recorded audio files via wireless connectives. CSI:DeSpy [35] collects the traffic fluctuations and correlates them with channel states information (CSI) variations to detect the hidden Wi-Fi cameras. Earfisher [40] detects wireless channel eavesdroppers by transmitting bait traffics and capturing the EMR leakages originating from eavesdroppers' DDR memory. However, the above designs are only applicable when the device has wireless connectivity modules. In the case of GPS trackers, the attacker may adopt an offline tracking strategy that records the GPS traces locally and picks up the tracker at a time window that is convenient for him. For example, the attacker may show up and pick up a GPS tracker attached to the victim's vehicle, when he went for grocery shopping and left the vehicle at the parking lot. We aim to develop a comprehensive detection method that works for both online and offline trackers.

To detect the devices with offline secret-stealing alternatives, researchers start to investigate the inherent correlations between the information processed by the device and its side-channel responses. In particular, CamRadar [23] and DeHiREC [58] show that hidden cameras and microphones leak measurable EMRs from their analog-to-digital (ADC) module when converting the analog sensory data to videos and voice files. Similar observations are also validated by TickTock [34], which are leveraged to detect the working status (on/off) of laptops' microphones. In comparison, unlike cameras and microphones, the geo-coordinates recorded by GPS trackers are typically around a few Kbits, which is considerably smaller than videos and voices. Therefore, it can barely induce strong EMR leakages from the ADC-related modules. In addition, almost every electronic has ADC modules, it could be hard to distinguish them by analyzing the ADC's EMR leakages.

2.2 EMR Side-channel

Electronic devices unavoidably leak EMR while they are functioning, which is considered as an effective side-channel for information reconstruction, device fingerprinting, and anomaly detection. In the early 1980s, Van Eck first published an experimental result showing the screen contents of a cathode ray tube (CRT) display can be reconstructed by analyzing its emitted EMRs. Inspired by these promising results, researchers have made more innovative contributions in investigating the potential of leveraging EMR side-channel for information extractions. Previous studies have shown that EMR leakages can be exploited to crack RSA keys [1] and AES keys [51, 52], reconstruct screen data [2, 11, 24], infer input on touchscreen keystrokes [15] and USB keyboard [31, 46], reconstruct neural network architectures [25, 56], and even eavesdropping audio data [5, 8, 19]. The above studies focused on EMR-based side-channel attacks while our goal is defense-oriented, i.e., detecting and identifying hidden GPS trackers through their leaked EMRs. Sehatbakhshk et al. [37] leverage the device's EM side-channel to verify the integrity of response computations in building the system's trustworthy execution environment. Cheng et al. [7] propose DeMiCPU to distinguish different CPUs based on their EMR patterns. Shen et al. [41] present MemScope, a system that senses electromagnetic fingerprinting of memory heartbeats, i.e., the clock that synchronizes memory and memory controller. Our research is parallel to these studies and utilizes the coupled EMRs originating from hidden GPS trackers' inherent MSoC circuits, i.e., quartz oscillator, local oscillator, and IF Filter to detect unauthorized geo-location tracking.

3 THREAT MODEL

3.1 Attack Model

We consider an attacker with specific goals and capabilities. The attacker's primary objective is to clandestinely track the locations of individuals, vehicles, or personal items using hidden GPS trackers.

Scope. In this work, we refer the GPS trackers as those devices specially made for tracking purposes by leveraging the GPS positioning techniques. The GPS sensors embedded on smartphones are out of our scope, since both Android and IOS pose strict permission controls on accessing the positioning sensors. As a result, the attacker could not obtain such tracking permissions without the victim's agreement.

The hidden GPS trackers are assumed to be small-sized, battery-powered devices, strategically placed in concealed positions for discreet location tracking. The trackers may possess wireless connectivity options, such as Wi-Fi, cellular networks, or Bluetooth, enabling the transmission of real-time location data to a remote monitoring server. Alternatively, the trackers may feature sufficient local storage to record target geo-coordinates over an extended period, allowing the attacker to retrieve the data later. We pose no assumptions about the trackers' types.

It's important to note that there are no restrictions on the appearance or manufacturing of the GPS trackers. For instance, the attacker could employ a GPS tracker disguised as a common item, like a phone charger (as shown in Figure 1).

Hidden Positions. Since GPS trackers rely on receiving radio-frequency (RF) signals from satellites to compute geo-coordinates, we assume the attacker places the trackers in hidden positions that are not fully shielded by metal objects. This is due to the significant energy loss experienced by RF signals when penetrating metal. Consequently, a weak signal might not provide sufficient information for the GPS tracker to decode meaningful data and obtain accurate location coordinates. For example, the attacker could place the GPS tracker in a bag, wallet, jacket, or shoes, but not inside a metal water cup.

Limited manipulation of MSoC hardware. We assume the attackers use consumer-grade GPS trackers. They can change the GPS tracker configurations but are unable to modify the MSoC system.

3.2 Detection Model

Primary Goal. As a detection system, GPSBuster is designed to identify concealed GPS trackers in diverse and complex environments. We refrain from making assumptions about the operational principles of GPS trackers, allowing for variations such as Wi-Fi/cellular-enabled or standalone devices. The detection system also has no prior knowledge about the GPS tracker's type and hardware specifics.

Usage Instructions. For the detection and location of unauthorized GPS trackers, the detection system is implemented in the form of a portable device, providing users with the flexibility to move around while scanning for EMR emanations and searching for hidden GPS trackers (i.e., scan-to-detect manner).

In real-world environments, there are various types of EMR. To achieve detection in general cases, no assumptions should be made about the cleanliness of the electromagnetic (EM) environment (e.g., an EM-shielded room) surrounding the detection system. For instance, hidden GPS trackers could be placed in private vehicles or personal carry-on bags, where various electronic devices are present, potentially causing strong EMR interference. The detection system should maintain the capability to extract and analyze the EMR characteristics of hidden GPS trackers under such noisy environments.

4 BACKGROUNDS

We first introduce the basic architecture and operational processes inherent to GPS trackers. Then, we explain how and why EMRs are produced by GPS tracker's MSoC circuits.

4.1 GPS Tracker Basics

GPS trackers continually receive positioning signals broadcast by global navigation satellite systems (GNSS). These signals operate within frequency bands ranging from L1 to L5 [54], with L1 allocated for civilian positioning usages at a central frequency of 1575.42MHz [55]. The L1 signal contains time and location data, enabling GPS trackers to calculate real-time geolocations. The workflow of a typical GPS tracker involves several key stages, illustrated in Figure 2. Note that, quartz oscillators are either integrated inside the GPS chip [48, 49] or soldered on the Printed Circuit Board (PCB) as external components. For both cases, quartz oscillators share the same PCB with other circuits.

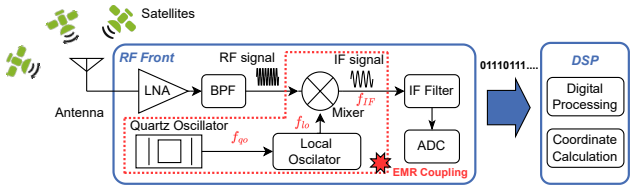


Figure 2: Simplified Architecture Used in COTS GPS Trackers.

The GPS tracker primarily comprises a signal processing module (RF front) for radio frequencies and a digital signal processing (DSP) module, packed as one mixed-signal system-on-chip (MSoC) circuit system. While the GPS tracker is receiving the positioning signals, the RF processing module first uses a low-noise amplifier (LNA) to enhance the signal strength received from the antenna. Second, it passes a band-pass filter (BPF) with a central frequency f_{L1} of 1575.42MHz to mitigate the RF noises while isolating L1 positioning signals. Third, the system utilizes a local oscillator (LO) to generate a reference frequency f_{lo} for preparing the signal mixing. **The L1 signal is mixed with the reference signal in order to be shifted to an intermediary frequency (IF), i.e.,** $f_{IF} = f_{L1} - f_{lo}$. The processed signal is then passed through an IF filter to selectively extract the useful signal frequencies while attenuating the others (i.e., RF noises). Finally, a built-in ADC of the MSoC converts this denoised analog signal into a digital signal, which is further sent to the digital signal processing (DSP) module. Following a standardized GPS protocol [54], the DSP module simply takes the digitized signal and performs code tracking, doppler frequency estimation, and data demodulation to derive real-time geographical coordinates.

Among the various signal processing steps delineated in the system architecture (refer to Figure 2), the frequency mixing emerges as the most pivotal one within the RF front section. It is accomplished by jointly incorporating the mixer, local oscillator (LO), and quartz oscillator (QO) circuit modules. The local oscillator plays a paramount role by multiplying the quartz oscillator's base frequency f_{qo} and producing the essential parameter $f_{lo} = N \times f_{qo}, N \in \mathbb{N}^+$, serving as a fundamental element for the mixer's conversion of the high-frequency positioning signal ($@f_{L1} = 1575.42$MHz) into an intermediate frequency f_{IF}.

In practical applications, quartz oscillators typically operate within the 10-52MHz frequency range. The local oscillator (LO) is structured as a phase-locked loop (PLL) frequency synthesizer, producing a reference signal ranging from 1570-1573MHz. The intermediate signal resulting from the mixer, denoted as $f_{IF} = f_{L1} - f_{lo} < 10MHz$, has a frequency significantly lower than that of the L1 raw GPS positioning signal received by the tracker's antenna. This transformation facilitates subsequent signal processing steps with increased efficiency. Following Nyquist's theorem [32], we learn that the lower frequency of the intermediate signal ($@f_{IF}$) necessitates a considerably reduced sampling rate for the ADC units during the conversion to digital signals. In addition, it also helps to alleviate the processing load on the IF filters.

4.2 EMR Coupling of MSoCs

Following Maxwell's equation and Lorentz force law [16], the intense fluctuations in the current signals of electronic devices give rise to time-variant electromagnetic fields, propagating into the open space, commonly known as EMRs. The evolution of printed circuit board (PCB) manufacturing techniques has led to the integration of RF fronts, DSPs, and power circuits into a singular signal chipset referred to as the MSoC chipset. This highly miniaturized architecture places different circuit modules closely and introduces unforeseen EMR coupling issues. EMRs emanating from distinct circuit components become coupled through their shared PCB substrates, resulting in unintended side-channel leakages. Previous studies in the RF research domain [8, 13] evidenced that **if the radiation frequencies of two EMR leakage sources are denoted as f_1 and f_2, respectively, the spectrum of their coupled EMR radiations can be expressed as $f_{rad} = n \times f_1 + m \times f_2$, where $n, m \in \mathbb{N}$.**

5 PRELIMINARIES OF EMR LEAKAGES

This section undertakes preliminary investigations to identify the specific circuit modules within the GPS tracker responsible for generating EMRs. Additionally, it explores the rationale behind leveraging emitted EMRs for detecting hidden GPS devices.

5.1 What are the EMR Characteristics of GPS Trackers?

We first focus on discerning the distinctive characteristics of EMRs emitted by GPS trackers. The primary objective is to validate the feasibility of exploiting these side-channel leakages for detection purposes.

Experiment Setups. We build the EMR sensory prototype by leveraging the HackRF One software-defined radio (SDR) device

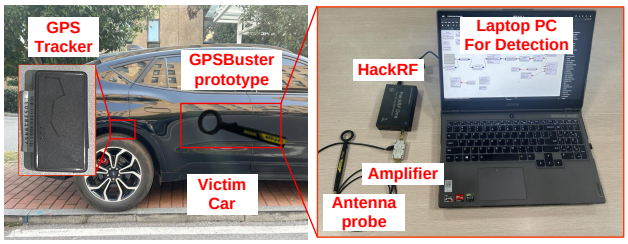
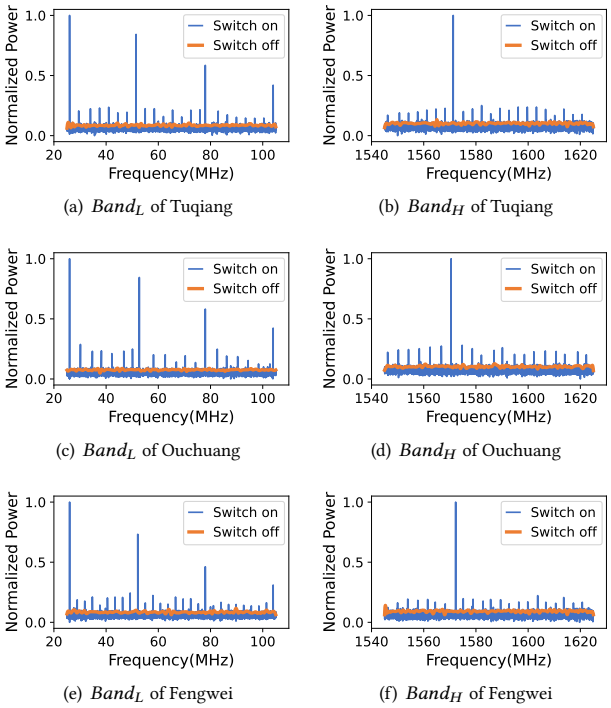


Figure 3: Prototype of GPSBuster.



(a) $Band_L$ of Tuqiang (b) $Band_H$ of Tuqiang

(c) $Band_L$ of Ouchuang (d) $Band_H$ of Ouchuang

(e) $Band_L$ of Fengwei (f) $Band_H$ of Fengwei

Figure 4: The emanated EMR spectrum of three GPS trackers, i.e., Tuqiang, Ouchuang and Fengwei.

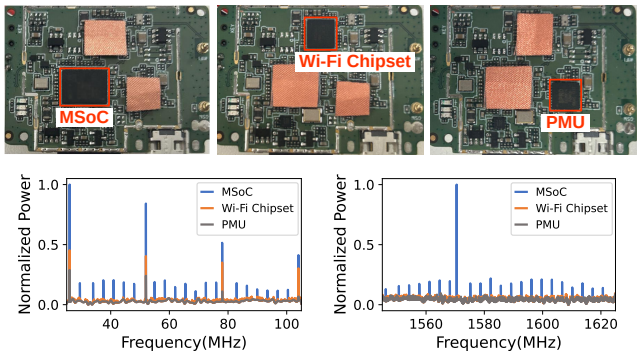
[29], an antenna probe, an amplifier and a laptop, as depicted in Figure 3. The HackRF One is designed with the capability to receive EMRs at the frequency range of 1MHz to 6000MHz, where the antenna pin of the HackRF One SDR is connected with a NFP-3 antenna and a low-noise amplifier (LNA) to enhance weak EMR signals by up to 35dB while mitigating ambient EM noises. HackRF adopts a sweeping manner to achieve wide-band scanning. It switches the scanning bands with a default bandwidth of 20MHz, which takes approximately 0.05148 seconds by average to collect a 20MHz-wide signal and compute its FFT results with a window size of 32768 samples. The prototype has a portable size, allowing users to hold the antenna and scan for potential hidden GPS trackers. Additionally, we believe it could be further miniaturized by replacing the signal analysis laptop with other small-sized and low-cost devices, e.g., Raspberry Pis.

To simulate real-world scenarios, experiments were conducted in a parking lot, employing the top-10 GPS trackers selected from a leading online retail platform[1]. To ensure the sample diversity, products from various manufacturers were selected, encompassing different MSoCs. Detailed information about the selected GPS trackers, including their models, sizes, and MSoC specifics, is presented in Table 2. In the experiments, we positioned the HackRF's antenna in close proximity (5cm) to the GPS trackers to obtain a clear spectrum and gain a thorough understanding of their characteristics.

Frequency Distributions. Three GPS trackers, namely Fengwei, Tuqiang, and Ouchuang, are chosen as representatives for the subsequent analysis. During the experiment, we investigated EMR emissions across a broad spectrum, ranging from 1MHz to 3200MHz, to characterize the distinctive frequency patterns exhibited by GPS trackers' EMRs. Figure 4 compares the EMR spectra of the selected GPS trackers, yielding the following key observations (KO).

KO1: A robust correlation is evident between the status of the GPS trackers and the observed EMR signals. It can be observed that the Tuqiang tracker exhibits negligible EMR signals when switched off. Upon activation, distinctive power spikes appear in the spectrum, primarily distributed across two frequency bands: **Band_L: 26MHz-104MHz** and **Band_H: 1545MHz-1625MHz**. A similar pattern is observed with both the Ouchuang and Fengwei trackers. This leads us to infer that the process of the GPS tracker's circuit modules introduces EMR leakages.

KO2: In both **Band_L** and **Band_H** EMR spectrums, a notable observation is that there is one most prominent frequency peak and the other peaks are spaced with an approximately uniform interval. For instance, in **Band_L**, the Tuqiang tracker has the strongest EMR peak at 26Mhz while the remaining peaks are at 30.09MHz, 34.18MHz, ..., and 103.71MHz. Its average periodic peak interval is approximately 4.09MHz. Similar observations are found in the **Band_H** EMR spectrum, where the primary frequency peak is at 1571.33MHz, and the other peaks are spaced with an interval of approximately 4.09MHz. These fundamental characteristics in EMR spectra can be further leveraged for detecting those GPS trackers.



(a) $Band_L$ (b) $Band_H$

Figure 5: EMR spectrum of each module inside the GPS Tracker: MSoC, Wi-Fi Chipset and power management unit (PMU).

[1]We purchased via an online shopping website, i.e., "Tmall.com", which has comparable market-size to "Amazon.com".

KO3: As shown in Figure 5, we further removed the Tuqiang GPS tracker's packaging shell and conducted separate EMR measurements for the MSoC unit, power management unit (PMU), and Wi-Fi chipset modules, as they are potential sources of EMR. During the measurement, copper tapes are utilized to cover the other circuits, isolating the specific module of interest and facilitating the measurement of its corresponding EMRs. Notably, the copper tape serves as a shield, preventing the EMRs emitted from the covered circuit modules from interfering with the measurements. We find that the MSoC unit generates strong EMRs with notable spectrum peaks, while no observable EMRs are detected when measuring the EMRs of the other circuit modules.

In summary, we have analyzed the unique spectral features of the EMR emitted by GPS trackers. The EMR is distributed across two distinct frequency ranges: **Band_L** and **Band_H**. Within **Band_L** and **Band_H**, it has one strongest EMR frequency peak and a series of coupled EMRs with fixed intervals. By conducting separate measurements on each electronic component within the GPS Tracker, we have confirmed that the EMRs originate from trackers' MSoCs.

5.2 What are EMR Sources inside the Trackers?

Having experimentally confirmed and characterized the EMR spectra of GPS trackers, the focus of this part is to pinpoint the source of EMR within the device's MSoC and investigate its root causes. This exploration is crucial for developing effective detection methods to accurately identify and confirm the presence of hidden GPS trackers through their EMR leakages.

As discussed in Section 4.2, the integration of multiple circuit units in GPS trackers as one MSoC system induces radiation couplings between EMR signals emitted from different units. In the following discussions, we reveal that there are three major EMR sources inside the GPS tracker's MSoC: the quartz oscillator, local oscillator, and mixer. And, the EMR coupling among these components generates radiations observed at two distinct frequency bands, denoted as **Band_L** and **Band_H**.

Band_H EMRs. Taking the Tuqiang GPS tracker as an example, Figure 4 evidenced that during the processing of satellite signals for acquiring GPS coordinates, it emitted a prominent peak and a series of sequential frequency peaks spaced with similar intervals (**KO2**). By formalizing it, we have these spectrum peaks adhere to a mathematical equation of $n \times 1571.33MHz + m \times 4.09MHz$ ($n, m \in \mathbb{N}$) with small deviation errors. We note these deviations are caused by the electronics' spread-spectrum techniques [58], which are commonly used by the device's oscillators varying its output frequency with small deviations to the calibration frequency. It avoids the device generating high EMR emanations and helps to meet the EMC regulations.

Intriguingly, the sum of 1571.33MHz and 4.09MHz equals to the frequency of the GPS satellite's L1 positioning signal (raw signal received at the GPS tracker's antenna), denoted as f_{L1} = 1575.42MHz. Drawing from the GPS basics discussed in Section 4.1, tracker devices' mixer down-convert the raw positioning signal ($@f_{L1}$) to the intermediate frequency ($@f_{IF}$) by mixing it with the local oscillator with a frequency of f_{lo}, i.e., $f_{IF} = f_{L1} - f_{lo}$. Therefore, we infer that the 1571.33MHz radiation component is likely composed of the local oscillator, while 4.09MHz EMRs correspond with the

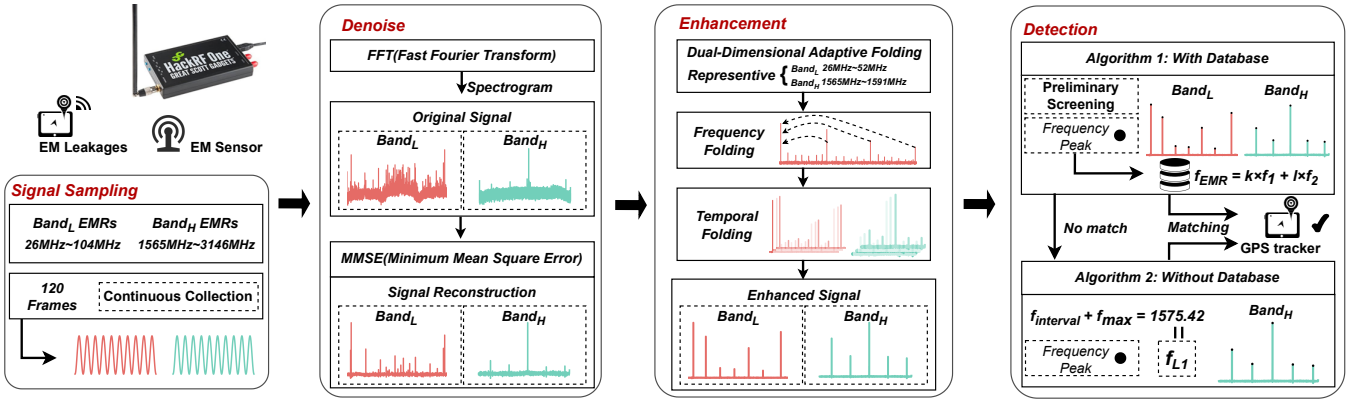
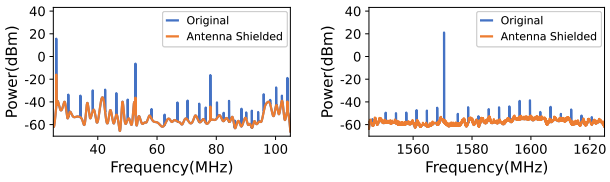


Figure 6: Framework of GPSBuster.

mixer's output frequency. **The radiation coupling between the GPS tracker's local oscillator module and mixer generates EMRs at the frequency of $\mathbf{Band_H}$ range following the pattern of $n \times 1571.33MHz + m \times 4.09MHz$.**

$\mathbf{Band_L}$ EMRs. In addition to the $\mathbf{Band_H}$ EMR spectrum, we find the Tuqiang tracker's $\mathbf{Band_L}$ radiation leakages following a mathematical formula of n×26MHz+m×4.09MHz, as shown in Figure 4. In particular, the Tuqiang GPS tracker is embedded with an MTK3333 MSoC, wherein its clock frequency of the quartz oscillator is 26MHz, and the mixer outputs a processed intermediate frequency signal f_{IF}=4.09MHz, as detailed in its datasheet[26]. **Thus, we infer that the $\mathbf{Band_L}$ EMRs originate from the coupling between GPS trackers' quartz oscillators and mixers.**



(a) $Band_L$ (b) $Band_H$

Figure 7: EMR spectrum changes with and without shielding the antenna.

To further validate the above hypothesis regarding the EMR sources, we conducted a comparative experiment. Note that both $\mathbf{Band_L}$ and $\mathbf{Band_H}$ EMRs were assumed coupling with the mixer's radiation signal (@f_{IF}). Meanwhile, as a down-covert version of the raw GPS positioning signal, the strength of f_{IF} is mainly determined by tracker's received GPS signal (@f_{L1}) strength. Thus, in the experiment, we enveloped the receiving antennas of the GPS trackers with a Faraday shielding bag, thereby attenuating its received satellite positioning signal (@f_{L1}) and subsequently reducing the signal power (@f_{IF}) converted by the GPS tracker's mixer unit. Such that, if the EMR is originated from the coupling among the quartz oscillator, local oscillator, and **mixer**(@f_{IF}), we should observe significant decreases of EMR's amplitudes.

We compared the strengths of the GPS tracker's EMR spectrum before and after shielding. Figure 7 illustrates a significant decrease in the strength of EMRs after shielding, compared to that of EMRs before shielding. This is because shielding the antenna decreases the received signal strength of GPS trackers, leading to a weaker mixed signal (@f_{IF}). Consequently, the coupled EMRs among f_{IF}, f_{qo}, and f_{lo} are also experiencing the signal attenuation with lower strengthens. These observations validate our assumptions regarding the EMR sources.

6 GPSBUSTER

Despite promising results demonstrating that hidden GPS trackers emit measurable EMRs during operation, several challenges persist in designing the corresponding detection system: ***Challenge 1:*** Environmental RF noises may pollute the GPS tracker's EMR spectrum. ***Challenge 2:*** EMR signals have weak amplitudes, leading to a short detection range. ***Challenge 3:*** The victim may have an MSoC database of target GPS trackers or may not have such prior information and the detection algorithm should be designed to handle both cases.

This section presents the detailed techniques employed to overcome these challenges and identify the presence of hidden GPS trackers from their EMR leakages. As illustrated in Figure 6, GPSBuster mainly consists of three procedures: *denoise*, *enhancement*, and *detection*. The *denoise* procedure utilizes the collected EMR signals measured at $\mathbf{Band_L}$ and $\mathbf{Band_H}$ spectra and applies a Minimum Mean Square Error (MMSE) method to eliminate environmental noises from the EMR measurements. The *enhancement* procedure then adaptively folds the signal in both time and frequency domains to acquire a clear EMR spectrum with high Signal-to-Noise Ratios (SNRs). Finally, the *detection* step takes the processed EMR signal to tentatively identify the suspected spectrum characteristics of a hidden GPS tracker. In our proposed method, we assume that the target GPS tracker to be detected is pre-recorded in the MSoC database. If the algorithm 1 successfully matches the target GPS tracker, it is considered detected. In the case of no match, the algorithm undergoes further validation in the "Without Database" scenario under algorithm 2 to obtain the final detection result.

As the *GPSBuster* requires the knowledge of an MSoC database to perform the algorithm 1 during detection, we envision two practical approaches to collect and enlarge the database detailed in Table 2. The user can collect data through public sources, e.g., technical

documents[38] [26] [33] and manufacturer's websites[43] [17]. Alternatively, crowd sourcing techniques can be used to encourage the cyberspace security communities to measure the GPS tracker's EMRs on-the-market and record them into the database.

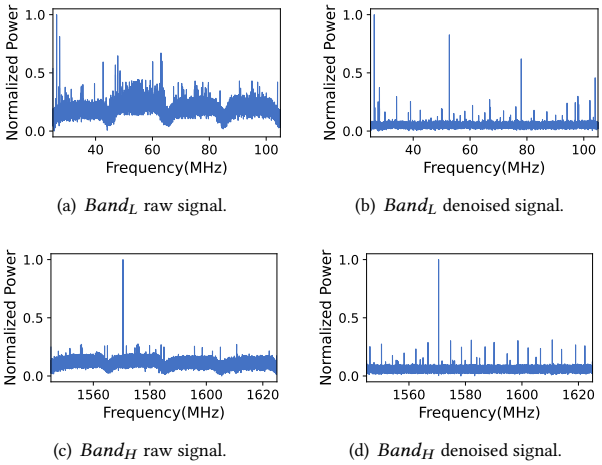
6.1 Denoise

Detecting hidden GPS trackers by exploiting their EMRs can be impeded by the presence of Radio Frequency (RF) noises radiated from nearby electronic devices. These noises are typically random and intermingled with the desired EMR spectrum. Conventional noise removal techniques utilizing frequency filtering designs fall short in addressing such interference. To address this challenge, we employ a Minimum Mean Square Error (MMSE) technique [10] to attenuate the noise components to a low amplitude level while strengthening the clean EMR frequencies of GPS trackers.

Specifically, before determining whether a target (e.g., a car) has been equipped with a hidden GPS tracker, we conduct a short-time scan of the environmental noise spectrum, denoted as $n_{est}(f,t)$, by positioning the HackRF prototype's antenna away from the victim. This scan helps us to roughly estimate the power spectrum of noises. Subsequently, we proceed to scan the victim and obtain a noisy EMR spectrum for detecting the hidden trackers, represented as

$$E(f,t) = Y(f_y,t) + n(f_n,t), f_y, f_n \in \cup f, \quad (1)$$

where $Y(f_y,t)$ represents the GPS tracker's EMR signal amplitude of frequency f_y at time t, and $n(f_n,t)$ stands for the corresponding noise component. The MMSE noise removal algorithm utilizes $n_{est}(f,t)$ as the referenced noise spectrum and computes the attenuation coefficient $G(f,t)$ for each frequency component of $E(f,t)$. The noises are then eliminated by applying the attenuation, i.e., $E(f,t) \times G(f,t)$. Ideally, $G(f,t) \approx 1$ if $f = f_y$, while $G(f,t) \approx 0$ if $f = f_n$. In practice, we adopted a classic algorithm proposed in [10] to compute the $G(f,t)$. Figure 8 shows the measured EMR spectrum of a Tuqiang tracker device in both $\mathbf{Band_L}$ and $\mathbf{Band_H}$ frequency ranges. It is observed that most of the environmental noises are removed from the raw measurements, and the denoised spectrums present clearer patterns.



(a) $Band_L$ raw signal. (b) $Band_L$ denoised signal.

(c) $Band_H$ raw signal. (d) $Band_H$ denoised signal.

Figure 8: Environmental noise removal.

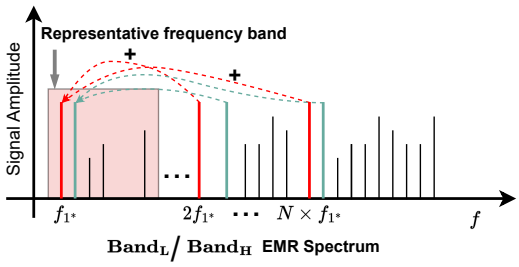


Figure 9: Frequency folding.

6.2 Enhancement

Radiated EMRs from hidden GPS trackers are typically weak, and their strength diminishes rapidly with increasing measurement distances. Therefore, an essential task for the detection system is to enhance the signal quality and extend the detection range. Some prior work [42, 57] applied frequency-folding techniques. However, GPS trackers' EMRs are extremely weak. In this context, we propose a dual-dimensional adaptive folding algorithm designed to improve the SNR in both the frequency and temporal domains.

Frequency Folding. The challenge of enhancing the spectrum strength of a radiating target is also a common consideration in the field of astronomical planet identification. In this context, the target is often distant from Earth, and its radiated signals are exceedingly weak. The fundamental strategy for enhancement involves grouping and summing the energy of all small signal segments of the target, i.e., radiated harmonic frequencies that periodically appear across a wide spectrum.

This insight motivates our approach. Specifically, as shown in Figure 9, we first select two short representative EMR frequency bands from the GPS tracker's original $\mathbf{Band_L}$ and $\mathbf{Band_H}$ EMR spectrum, separately. This representative spectrum is then utilized by the detection system to verify the suspected target is a hidden GPS tracker. To enhance the SNR of the representative spectrum and extend the detection range, we search all the frequency segments in the original $\mathbf{Band_L}$ and $\mathbf{Band_H}$ EMR spectrum, which are harmonics of those prominent frequency peaks in the representative band. Subsequently, we aggregate the energy of the identified harmonics with their corresponding frequency peaks in the representative band.

In practice, we empirically selected the frequency range of 26MHz-52MHz and 1565MHz-1591MHz as the representative bands for $\mathbf{Band_L}$ and $\mathbf{Band_H}$ EMRs, respectively. The core of the frequency folding algorithm is to search and align the harmonic frequency peaks and sum them correspondingly to the representative frequency bands.

Specifically, suppose the frequency components of $\mathbf{Band_L}$'s representative frequency band are denoted as $[f_1^L, f_{2^*}^L, ..., f_l^L, ...f_{l^*}^L, ...]$, where l^* denotes the index of a spectrum peak, and l denotes the index of the other frequency components. We then search for the harmonics $f_{l^*}^{har}$ of $f_{l^*}^L$ in the candidate spectrum peaks within the frequency range of 52MHz-104MHz. However, $f_{l^*}^{har}$ may not precisely equal $N \times f_{l^*}^L$, where $N \in \mathbb{N}^+$, due to devices' spread-spectrum techniques [9]. Therefore, we adopted an adaptive frequency folding algorithm to sum the energy of harmonics to the representative

frequency band, i.e.,

$$A(f_{l^*}^L) = A(f_{l^*}^{har}) + \max\{A(N \times f_{l^*}^L \pm \Delta f)\}, \quad (2)$$

where $A(\bullet)$ represents the amplitude of the frequency component $\bullet$, and Δf represents the measurement error in locating the harmonic frequencies. In practice, we empirically set Δf = 0.3MHz. The same frequency folding algorithm is applied to $\mathbf{Band_H}$ to enhance its spectrum quality by considering the 1565MHz-1591MHz EMRs as the representative frequency band and summing the frequency energy of searched harmonics within the range of 1591MHz-3146MHz.

Temporal Folding. To further refine the representative Electromagnetic Radiation (EMR) spectra, we employ a temporal folding algorithm by collecting the GPS tracker's EMR spectrum over 120 measurements. For each measurement, the frequency folding algorithm is initially applied to yield a preliminary spectrum enhancement. The set of enhanced frequency peaks for each EMR measurement is denoted as $F_i = \{f_{i,1^*}, f_{i,2^*}, ...\}, i \in [1, 120]$.

To distinguish genuine prominent frequencies from potential noise peaks, we compute the union of all candidate frequency peaks for enhanced spectrums as $F = \cup\{F_1, ...F_j, ..., F_{120}\}$. Subsequently, we count the number of occurrences O_j for each candidate peak $f_j \in F$ in the 120 EMR measurements. A higher O_j indicates a greater likelihood that the frequency peak is genuinely radiated from the GPS tracker, as it consistently appears over time. In practice, we select frequency peaks with $O_j \geq 100$ for enhancement. Specifically, we update the signal amplitude of each selected frequency peak f_j as the summation of its amplitudes measured over 120 times, while removing the amplitudes of other peaks. This approach ensures that genuine prominent frequencies are reinforced, while noise peaks are effectively minimized in the enhanced representative EMR spectra.

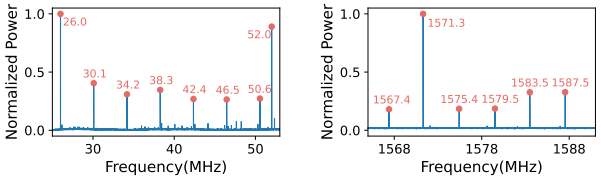
Table 1
Comparisons of the EMR's SNR before and after applying the dual-dimensional folding enhancement.

Distance	5cm	10cm	15cm	20cm	25cm	30cm
Original (dB)	3.16	2.08	1.78	1.12	0.88	0.52
Folded (dB)	41.40	30.82	22.37	20.02	11.12	8.15

Figure 10 illustrates an instance of normalized spectrums for the Tuqiang GPS tracker's representative EMR spectrums after employing the dual-dimensional folding algorithm. It is evident that the strength of prominent frequency peaks is concurrently enhanced compared to the results presented in Figure 8. Table 1 also evaluates such enhancement qualitatively by comparing the EMRs' SNRs measured at different distances. Even in the worst-case scenario, where EMRs are collected at a distance of 30cm from the tracker device, the signal is significantly boosted from SNR = 0.52dB (an extremely weak signal) to SNR = 8.15dB, representing an enhancement of over 15 times.

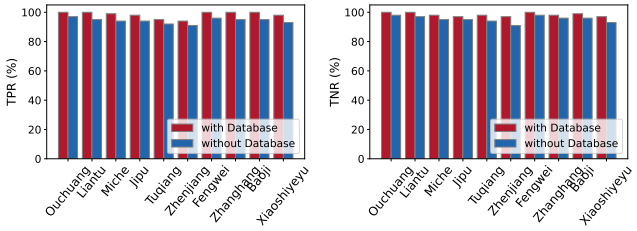
6.3 Detection

We denote the frequency compositions of the enhanced representative EMR spectra as $[f_{1^*}^L, ..., f_{l^*}^L ...]$ and $[f_{1^*}^H, ..., f_{h^*}^H ...]$ for the $\mathbf{Band_L}$ and $\mathbf{Band_H}$ EMRs, respectively, where $f_{l^*}^L$ and $f_{h^*}^H$ represent the frequency peaks. To determine whether these measured spectra potentially originated from a GPS tracker's EMR, we developed



(a) $Band_L$ Folded signal. (b) $Band_H$ Folded signal.

Figure 10: By applying the dual-dimensional folding, the measured EMRs of the Tuqiang GPS tracker present identifiable frequency peaks (marked as red dots) in the representative bands of $\mathbf{Band_L}$ and $\mathbf{Band_H}$.



(a) **TPR** (b) **TNR**

Figure 11: Comparison of detection performance with/without MSoC database.

two matching algorithms tailored for situations with/without an MSoC database. As suggested by prior work [34], detectors could collect the hidden devices' hardware specifics, i.e., f_{lo}, f_{qo}, and f_{IF}, via chips' handbooks, crowd-sourced measurements, or users' pre-measurements, and build a dataset to facilitate the detection. Nevertheless, to develop a practical GPS tracker detection system, we also consider the scenario where a tracker chip dataset is unavailable.

With Database. We match the frequency peaks with the MSoC database and check if they follow the distribution patterns:

$$f_{l^*}^L = Nf_{qo} \pm Mf_{IF}, \quad f_{h^*}^H = Nf_{lo} \pm Mf_{IF}, \quad (3)$$

where $N \in \mathbb{N}^+, M \in \mathbb{N}$. The MSoC database stores the values of f_{qo}, f_{lo}, and f_{IF} for each MSoC, as shown in Table 2. A confirmed match implies the presence of a GPS tracker around.

Without Database. In the case of lacking of a MSoCs' specifics database, we cannot use the Eq. (3) to perform the detection. However, as discussed in Section 4.1, we found that in the high-frequency band $\mathbf{Band_H}$, the EMR patterns show f_{lo} + f_{IF}=1575.42MHz (@f_{L1}) and can be used as the new detection rule. In particular, Figure 7 and 10 show that in $\mathbf{Band_H}$, the peak intervals $f_{interval}$ equals to the f_{IF} and the the maximum peak f_{max} among $f_{h^*}^H$ equals to f_{lo}. Thus, in the absence of MSoC information, we could employ this simplified rule for detection. If Eq. (4) is satisfied, we determine that a hidden GPS tracker is located nearby.

$$f_{interval} + f_{max} = 1575.42(MHz) \quad (4)$$

where $f_{interval}$ represents the interval, and f_{max} denotes the frequency of the maximum value within $\mathbf{Band_H}$.

Figure 11 presents the detection performance with/without MSoC database. For both cases, the distance between the tracker and the antenna is 10 cm, and each tracker is tested 100 times in a parking lot. Results reveal that, with support of an MSoC database, the

system performs well, achieving an average True Positive Rate (TPR) and True Negative Rate (TNR) of 98.1% and 98.7%, respectively. Additionally, in the absence of prior MSoC information, the system's performance marginally declines, with an average TPR and TNR of 94.2% and 95.3%. This is because, for targets not included in the database, GPSBuster perform the detection with only the $\mathbf{Band_H}$ spectrum. Overall, GPSBuster demonstrates acceptable performance under both conditions.

7 EVALUATIONS

Experiment Setup. We constructed the EMR measurement system for *GPSBuster* as depicted in Figure 3. The system incorporates a HackRF One, a Low-Noise Amplifier (LNA), and an NFP-3 antenna. In the experiments, we evaluate the performance of *GPSBuster* in terms of its ability to detect hidden GPS trackers (as shown in Figure 12) installed on victims' possessions under different settings. Various impact factors are examined, including tracker heterogeneity, EMR sensory distances, tracker placements, and environmental dynamics. A total of 25 volunteers (including 16 males and 9 females aged between 19 and 45) participated in the experiments, playing the roles of victims or human inspectors. Prior to each experiment, detailed instructions regarding the experimental procedures were provided. The collected data are anonymized and stored locally to prevent potential leakage. The Institutional Review Board (IRB) office of our institute has approved the entire research.

Default Scenarios. We use the following attack scenarios by default unless specific changes are mentioned. Without loss of generality, we use Ouchuang, Tuqiang, and Fengwei GPS trackers as the detection targets to represent the devices with different MSoCs (detailed in Table 2). During the experiments, the attacker was allowed to hide the GPS tracker at any random places on a Jeep SUV car, where he considered it was a safe place and hard to find for the victim. The goal of *GPSBuster* is to perform the EMR scans and bust out the hidden GPS trackers.

Evaluation Metrics. The detection performances are evaluated via the following metrics: TPR, TNR, Max. Distance, Accuracy, and SNR. In particular, **TPR** (True Positive Rate) and **TNR** (True Negative Rate) indicate the probabilities that the system correctly detects and ignores the hidden GPS trackers, respectively. **Max. Distance** is defined as the maximum distance that the system can identify a GPS tracker with a probability at least higher than 50% (random guess). **Accuracy** characterizes the system's correctness by computing $\frac{TP+TN}{\sum \text{samples}}$. **SNR** is also selected as the basic metric to quantify EMR signal quality. A larger value represents the signal is clear with limited noise interference and vice versa.

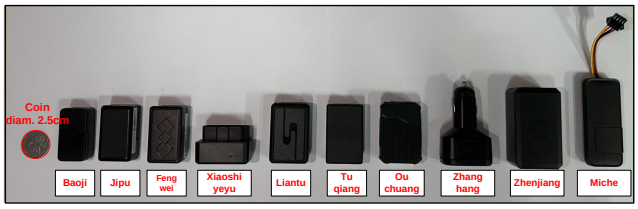
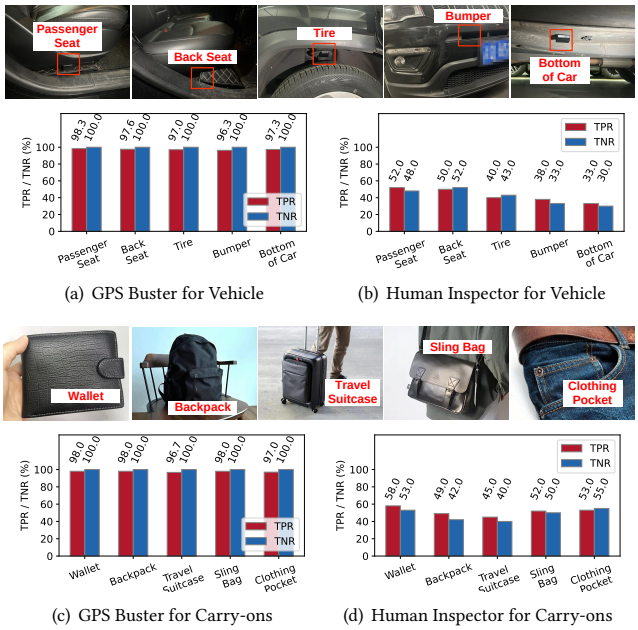


Figure 12: The appearance of the selected 10 GPS trackers. To highlight the small size of the GPS trackers, a coin is utilized as a reference.



(a) GPS Buster for Vehicle (b) Human Inspector for Vehicle

(c) GPS Buster for Carry-ons (d) Human Inspector for Carry-ons

Figure 13: Comparison of GPS Buster and Human Inspectors Performance in Real-World Scenarios

7.1 Real-World Case Study

Before proceeding to the detailed evaluations presented in the subsequent sections, we initially conduct two case studies to provide a brief demonstration of the effectiveness of *GPSBuster* in detecting hidden GPS trackers. In these case studies, the attacker is tasked with concealing the tracker device at random locations on the target, while *GPSBuster* scans the EMR spectrum to identify them. For comparison, we involve 10 volunteers to serve as human inspectors, visually searching for suspected GPS trackers. To avoid data basis, volunteers are only required to perform the best-effort searches and get no feedbacks about the detection results. Two real-world cases were considered. The experiment was repeated 100 times for each GPS tracker, with 80 trials being positive (GPS trackers were present) and 20 trials being negative (GPS trackers were absent).

Case 1: Vehicle. We asked one volunteer to act as the victim. He parked his car at the university's parking lot. The attacker chose to hide GPS trackers on the car at five different places, i.e., passenger seat, back seat, tire, bumper, and chassis. As shown in Figure 13 (frist row), the GPS tracker was well concealed intentionally avoiding being spotted by the victim. Both the human inspector and *GPSBuster* user are authorized to fully search or scan the vehicle to find suspected GPS trackers, i.e., Fengwei, Tuqiang, and Ouchuang.

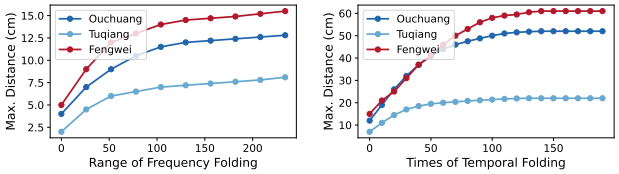
Case 2: Carry-ons. In this experiment, we asked the attacker to place hidden GPS trackers on the victim's daily carry-ons, i.e., wallet, backpack, travel suitcase, sling bag, and clothing pocket. We use miniaturized GPS trackers, i.e., Baoji (2.3×4.0 cm), Fengwei (2.8×4.8 cm), and Ouchuang (3.0×5.0 cm), that are hard to be spotted by the victim. The other settings remain unchanged and follow the above experiment with the victim's vehicle.

Detection Results. Figure 13 shows the detection results. It is observed that *GPSBuster* successfully detects hidden GPS trackers

with the average TPRs as high as 97.3% and 97.5%, respectively for the case 1 and 2. However, human inspectors have the detection TPR around 33%-52%, whereas the TNR is around 30%-52%, across all test cases. It indicates that human inspectors fail to correctly identify the hidden GPS trackers and its detection results are no better than random guesses. In addition, *GPSBuster* takes 8.9 seconds by average to generate one detection result of the target area, which is more efficient than the human searches.

7.2 Comprehensive Evaluation of *GPSBuster*

In this section, we evaluate the performance of *GPSBuster* comprehensively by investigating the impact of different experiment settings.



(a) **Impact of ε** (b) **Impact of γ**

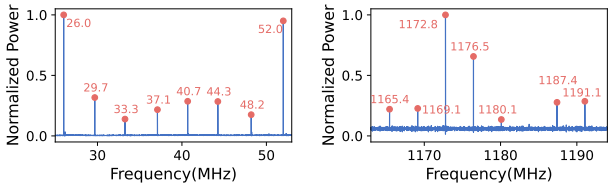
Figure 14: Impact of system parameters.

Impact of System Parameters. The main parameters affecting the performance of GPSBuster are the range of frequency folding and the times of temporal folding, denoted as ε and γ respectively. To choose them, we measure the Max. Distance of detection under different ε ranging from 0 MHz to 260 MHz with a gradient of 26 and γ ranging from 0 times to 200 times with a gradient of 10. A broader frequency range within $\mathbf{Band_L}$ and $\mathbf{Band_H}$ provides more harmonics distributed at fixed intervals for the frequency folding, and more folding times in the temporal domain further concentrates the energies of harmonic components. Nonetheless, optimizing these settings involves a compromise, as increasing the parameters ε and γ also leads to a corresponding increase in the system's runtime. During the experiment, we first set the γ to zero to evaluate the impact of ε as shown in Figure 14(a). We choose 104MHz as a compromise value for ε because once it reaches 104MHz, further increases yield only marginal improvements in Max. Distance of detection while the time cost rises sharply. We then fixed the ε at 104MHz to select the γ. We obtained an optimal value at approximately 120 as shown in Figure 14(b)[.

Impact of Devices' MSoC Diversity. In this experiment, we evaluated the proposed detection system over a wide range of GPS trackers embedded with different MSoCs. Table 2 summarizes the device's radiated EMR patterns and benchmarks of *GPSBuster* in detecting these GPS tracker devices. Among them, the maximum detection distance is derived by increasing the distance between the EMR sensor (HackRF One) and its target device from 10cm to 70cm. For each experiment, the distance is increased gradually by 1cm. We set the system's maximum detection system as the one when its accuracy drops lower than 50%. It is observed that GPS trackers with the same types of MSoC share similar performances in terms of Max. Distance. The longest detection distance is up to 61cm measured on an MTK2503D MSoC device, i.e., Fengwei. And, the Zhenjiang GPS tracker has the shortest detection range, i.e., 20cm. We believe such disparities are caused by the differences of their MSoC designs. For example, the Fengwei device could have a stronger LNA embedded within the MSoC, which amplifies the processed raw GPS positioning signals and leads to an intensified intermediate signal($@f_{IF}$). As a result, its coupled EMRs with quartz oscillator ($@f_{qo}$) and local oscillator ($@f_{lo}$), i.e., $\mathbf{Band_L}$ and $\mathbf{Band_H}$, are both enhanced. It causes high SNRs in the measured EMR signals (as shown in Table 2) and helps the *GPSBuster* to achieve longer detection distances.

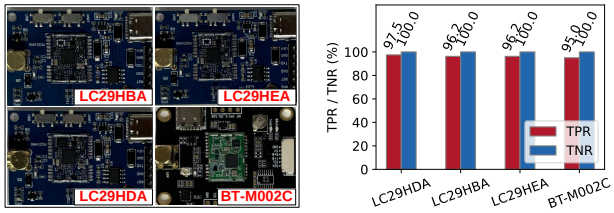
GPSBuster allows the user to hold the EMR sensory antenna and perform a scan-to-detect manner to search for suspicious GPS trackers. Table 2 also demonstrates the benchmark results of detecting the trackers at a distance of 10cm. The results are promising with an average TPR and SNR equal to 98.4% and 23.6dB respectively, which verifies the robustness of *GPSBuster* in detecting heterogeneous tracker devices with different shapes, sizes, and MSoC models.

L1+L5 Dual-band GPS Trackers. As suggested by [47], L1 GPS trackers are cost-effective solutions for most civilian applications since 1983. Some advanced GPS trackers may support both L1 and L5 band signal samplings, in which L5 GPS signals provide more accurate location coordinates. Nevertheless, L1+L5 GPS trackers also contain the critical components, i.e., the quartz oscillator, mixer, and local oscillator, which generate EMRs when processing GPS signals. To evaluate the effectiveness of GPSBuster in detecting L1+L5 dual-band trackers, we selected four popular GPS modules with different MSoCs, i.e., LC29HBA, LC29HEA, LC29HDA, and BT-M002C. As shown in Figure 15, we use the LC29HDA tracker as an example to demonstrate its EMR spectrum. It is observed that its signal patterns are similar to those of L1 GPS trackers as shown in Figure 4, but with different basic frequency compositions, i.e., f_{qo} = 26MHz, f_{lo} = 1172.8MHz, and f_{IF} = 3.65MHz. We found that the summation of f_{lo} and f_{IF} equals the frequency of GPS signal's L5 band f_{L5} = 1176.45MHz. This follows the same principles discussed in Section 4.1. Thus, *GPSBuster* is also effective in detecting L1+L5 dual-band GPS trackers. Figure 16 shows that the system achieves a TPR of 96.25%.



(a) $\mathbf{Band_L}$ (b) $\mathbf{Band_H}$

Figure 15: The EMR spectrum of LC29HDA.

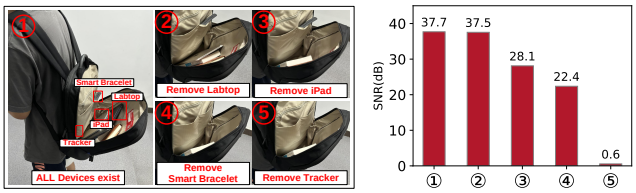


(a) L1+L5 Dual-band GPS Trackers. (b) TPR&TNR

Figure 16: Impact of Dual-band GPS Trackers.

Table 2
Detection Performances of *GPSBuster* on 10 Top-selling GPS Tracker Devices.

GPS Tracker	Size (cm)	MSoC	EMR Coupling Sources			Max. Distance (cm)	d = 10 cm	
			f_{qo}(MHz)	f_{lo} (MHz)	f_{IF}(MHz)		SNR(dB)	TPR
Ouchuang	5.0 × 3.0	AT 6558R	26	1570.58	4.26	52	33.16	100%
Liantu	5.0 × 3.0	AT 6558R	26	1570.58	4.26	50	29.58	100%
Miche	7.0 × 2.8	AT 6558R	26	1570.58	4.26	48	30.16	99%
Jipu	5.0 × 3.0	AT 6558R	26	1570.58	4.26	45	29.25	98%
Tuqiang	5.0 × 3.0	MTK 3333	26	1571.33	4.09	21	18.92	95%
Zhenjiang	7.0 × 2.8	MTK 3333	26	1571.33	4.09	20	16.25	94%
Fengwei	4.8 × 2.8	MTK 2503D	26	1572.25	3.07	61	30.82	100%
Zhanghang	7.0 × 4.0	MTK 2503D	26	1572.25	3.07	55	22.67	100%
Baoji	4.0 × 2.3	MTK 2503D	26	1572.25	3.07	45	25.21	100%
Xiaoshiyeyu	4.8 × 2.8	MTK 2503D	26	1572.25	3.07	32	20.12	98%

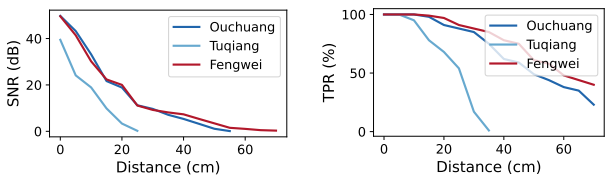


(a) Real-World Setup (b) SNR

Figure 17: Impact of different GPS modules.

Impact of Different GPS Modules. In this experiment, we placed different types of GPS modules in a victim's carry-on backpack as shown in Figure 17(a). The backpack contains a smart bracelet (Xiaomi 8 Pro), an iPad (Apple Air 6), an Ouchuang GPS tracker, and a laptop (Huawei Matebook 14). Among these, the first three devices have GPS modules while the laptop does not. *GPSBuster* detects all types of GPS devices, generating alerts when scanning the backpack area. To isolate Ouchuang tracker from the others, we removed the suspected devices one-by-one as shown in Figure 17(a). Figure 17(b) shows that when the laptop is removed, the received EMR SNR barely changes, implying it has no GPS module. However, when the bracelet and iPad are removed, the system receives weaker EMRs. Eventually, by further removing the suspected tracker device, we observe that EMRs are barely measurable with the SNR of 0.6dB, indicating that all tracking devices have been removed. By applying this detection strategy, the system acheives a TPR of 97.08% in detecting the Ouchuang tracker.

Impact of Measurement Distance. In the experiment, we vary the measurement distance from 0cm to 70cm and evaluate the detection performance under each setting. As shown in Figure 18, the EMR signal's SNR is negatively correlated with the growth of the distance. A longer distance leads to weaker EMR received by the detection system, such that its TPR also decreases accordingly. In addition, we find that the maximum detection distance of GPS trackers is more than 20cm, while the longest one can reach 61cm. It validates that our detection system can effectively handle the most usage cases of GPS trackers, e.g., the real-world cases presented in Section 7.1. Especially, considering the user can move around the



(a) SNR (b) TPR

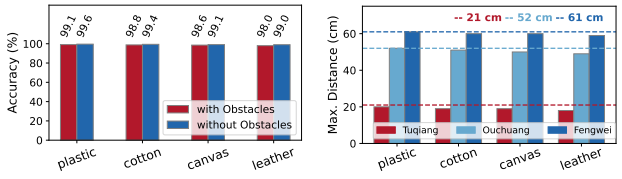
Figure 18: SNR and TPR of detection at different distances.

system's EMR receiving antenna, it is easy for him to find a close spot within 20cm to the suspected target. Extending the system's detection range to a super long range, e.g., ≥ 10m, may not be helpful. For example, there could be multiple GPS trackers hiding on the victim's vehicle. A long-range detection system could trigger the warning alert at very far distances, and the user may not be able to locate where the tracker is and remove it correctly.

Impact of Electronic Interference. Following the Lorentze force law, electronic devices unavoidably generate EMR emanations while they are functioning. Thus, it is necessary to evaluate the impact of different electronic interference on the system detection performances. In the experiment, we selected 5 electronic devices with 5 different types, including smartphones, earphones, laptops, e-mouses, and speakers. And, the smartphone's GPS functionality was not turned off. Table 3 summarizes their hardware specifics and EMR patterns, and we denote these devices as 'A' to 'E'. It is observed that electronic devices have unique EMR patterns and frequencies. However, none of them share similar EMR coupling

Table 3
Impact of Electronic Interference.

Type	Case	Prominent EMR Frequency	TPR	TNR
A	Huawei Mate50	0.27–26.16MHz	96%	98%
B	Airpods pro	2.11MHz	100%	100%
C	HP OMEN 9	0.34–28.10MHz	97%	97%
D	Logitech M720	1.25MHz	100%	100%
E	Xiaomi Play	24.12 MHz	100%	100%



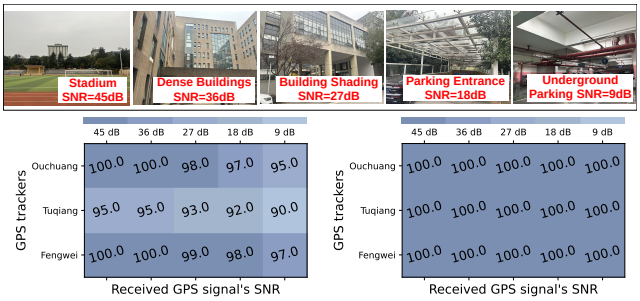
(a) Accuracy (b) Max. Distance

Figure 19: Impact of physical obstacles.

results to the GPS trackers. Among them, smartphones and laptops present a wide spectrum of EMR emanations ranging from 0.27MHz-26.16MHz and 0.34MHz-28.10MHz, respectively. It may inference with the GPS trackers' EMR spectrum. Results reveal that when these two types of devices are within the system's detection range, they indeed cause a decrease in detection performance. However, as discussed in Section 6.3, *GPSBuster* makes its final determinations by integrating the characteristics of both $\mathbf{Band_L}$ and $\mathbf{Band_H}$. Therefore, even under the electronic interference, the average TPR and average TNR remain above 96% and 97%, respectively.

Impact of Physical Obstacles. Usually, attackers believe that hiding GPS trackers behind physical obstacles creates non-line-of-sight conditions for the victims, such that the trackers cannot be found easily via visual inspections. In this experiment, we demonstrate the effectiveness of the detection system by covering the tracker devices with 4 different physical obstacles made of different materials, i.e., plastic, cotton, canvas, and leather. Note that, we do not consider the obstacles made by metal. This is because tracker devices need to receive the GPS positioning signal from the satellite to retrieve location coordinates. If the attacker covers the GPS tracker with a metal object, it will cause an RF-shielding effect blocking the positioning signals. And, the GPS tracker cannot compute meaningful geo-coordinates. Figure 19 compares the *GPSBuster*'s detection accuracy and Max. distance with and without covering the obstacles. We find that there are no significant decreases in terms of both evaluation metrics. For example, the system achieves 99.6% detection accuracy on average when the GPS trackers are not covered. It turns to 99.1% when the GPS trackers were covered by plastic obstacles. In the case of the Fengwei tracker device, its maximum detection distance is around 61cm with less than 3.0cm variations with and without the coverage of obstacles. Thus, these obstacles have a negligible effect on the detection performances. The reason is that they have low conductivity, such that EMR signals can penetrate them without significant energy loss.

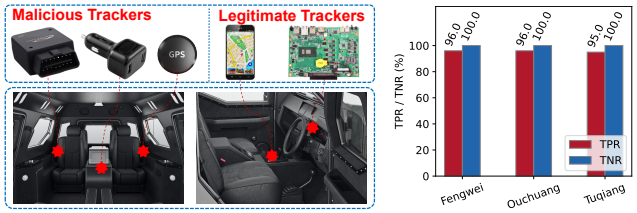
Impact of Environmental Dynamics. The victim may carry a hidden tracker device at various places experiencing variant GPS signal quality. To evaluate the impact of environmental dynamics, we perform the detection tests by asking the victim to carry the tracker device and move around in 5 test sites, including Stadium, Dense Buildings, Building Shading, Parking Entrance, and Underground Parking. The received GPS signal SNR at the sites on average is 45dB, 36dB, 27dB, 18dB, and 9dB, respectively. As shown in Figure 20, the system has lower detection TPR under the testing sites with weak GPS signals. For example, the Ouchuang tracker device can be detected with an average TPR equal to 100% when the victim is at the stadium, while it drops to 95% for the underground parking testing site. It meets our analysis presented in Section 5.1, i.e., weaker GPS signals diminish the amplitude of its intermediate



(a) TPR (b) TNR

Figure 20: Impact of environmental dynamics.

frequency signals ($@f_{IF}$), thus its coupled EMRs are diminished in both $\mathbf{Band_H}$ and $\mathbf{Band_L}$ ranges. Accordingly, the system has lower detection accuracy. Still, we find that it achieves at least 90% TPR and 100% TNR for all tested GPS trackers.

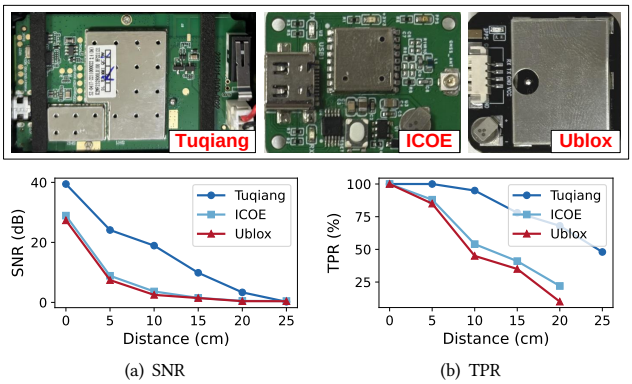


(a) Real-World Setup (b) TPR&TNR

Figure 21: Impact of Legitimate Trackers.

Impact of Legitimate Trackers. In real-world cases, hidden GPS trackers placed by the malicious attackers may coexist with legitimate GPS modules. To evaluate the impact of these GPS trackers, we set up the testing scenario as shown in Figure 21(a), in which it contains three malicious hidden GPS trackers, one iPhone 15 mobile device, and one built-in vehicle navigation system. *GPSBuster* adopts a scan-to-detect manner to search for all GPS trackers and remove the malicious ones. For example, if the system detected the phone's GPS, we would turn off the phone's GPS and proceed to detect the next target. We believe that it could not be a tough decision for the user to determine if a detected GPS tracker is a legitimate one. Users may search online or contact the manufacturer to verify if an electronic device contains legitimate GPS modules. Figure 21(b) shows that the system achieves an average TPR of 95.6% and a TNR of 100% by applying the proposed detection design.

Impact of Metal Shielding. Some manufacturers cover GPS chips with metal cases to mitigate electromagnetic interference. As shown in Figure 22, we evaluate the impact of metal shielding on three GPS trackers: Tuqiang, ICOE, and Ublox. In these experiments, we vary the EMR measurement distances to assess the detection performance under each setting. Figure 22(a) illustrates that the system still receives measurable EMRs. However, these signals have relatively lower SNRs compared to GPS trackers without metal shielding, such as Ouchuang. For example, at a distance of 10 cm, the Ouchuang tracker emits an EMR with an SNR of 33.16 dB (Table 3), while the EMR strengths of the Tuqiang and Ublox trackers are 18.92 dB and 2.51 dB, respectively. This reduction is because metal cases impede a portion of the EMR signals. Nevertheless, since GPS chips are soldered onto the PCB substrate, some EMR signals might leak



(a) SNR (b) TPR

Figure 22: Impact of Metal Shielding.

from the PCB's connected wires. Figure 22(b) shows that the system remains effective but with shorter detection ranges, such as a Max. distance of 21 cm for the Tuqiang tracker. It is also noteworthy that if a GPS tracker's entire PCB is perfectly shielded with metal cases, the detection system may fail to obtain meaningful EMR measures and thus fail to detect the hidden trackers. However, perfect shielding could disrupt the heat exchange of the PCB substrate, potentially causing the circuits to overheat and malfunction.

8 DISCUSSIONS

In this section, we discuss several considerations for practical deployment of *GPSBuster*.

Detection Range. In general, a longer detection distance is favored by most systems. However, for our case, a super long detection range may not be helpful for the user. For example, if the detection range reaches 10m, even though the system might successfully identify the presence of a GPS tracker from a far distance, users need to search for a larger area to find its accurate position and remove it correctly. Especially in the scenarios such as a large parking lot or a crowded street, a wide search will be an extremely difficult task for users. As a future work, we plan to use amplifiers with higher signal gains to extend the detection range. Additionally, users are allowed to adjust the system's signal enhancement abilities, enabling long-range detection for initial warning of the hidden trackers, and short-range detection for accurate localization.

Extensions. *GPSBuster* exploits the device EMRs to detect hidden GPS trackers. In practice, attackers may also track victims' routines under indoor scenarios, where the GPS trackers cannot function. The indoor trackers, such as RFID tags, Air tags (Bluetooth based), and Wi-Fi based trackers, are also passive location sensors. However, we believe that their embedded positioning circuits may also induce EMR side-channel leakages, which can be leveraged to perform the detection.

Periodically Inactive Trackers. Some GPS trackers may adopt a periodically-active sampling design to acquire the victim's coarse location information. However, when the GPS tracker is remotely powered off or set as an inactive one, it will acquire no location information, thus posing no threat to the victim in such status. Due to their limited circuitry activities, it could be challenging to detect these devices. Nevertheless, users could deploy multiple detectors to continuously monitor the target area and detect the trackers instantly once they start actively collecting GPS data.

9 CONCLUSION

This paper presents the first attempt of leveraging EMRs for the purpose of tracker detection. In particular, we find that GPS tracker's MSoC circuit induces coupled radiation spectrums demonstrating unique frequency peaks in two fixed ranges, i.e., $\mathbf{Band_L}$ and $\mathbf{Band_H}$. Further studies identify the EMR sources inside tracker's MSoC are the quartz oscillator, local oscillator, and mixer. Their EMRs are coupled with each other. Accordingly, we formalize the distributions of these EMRs and develop a dual-dimensional folding algorithm for enhancing the EMR SNRs. To accommodate scenarios where the victim may or may not have an MSoC database for the targets, we develop and integrate two matching algorithms to enhance the reliability of our detection results. We build the detection system, *GPSBuster*, with HackRF SDRs. Our evaluations show the system has the detection accuracy of 98.4% on average, under various testing scenarios. The maximum detection range is 0.61m. We hope our design can inspire advancements in cybersecurity tools to thwart malicious secret-stealing attacks.

10 ACKNOWLEDGEMENT

We would like to express our sincere gratitude to the anonymous reviewers for their valuable comments. Additionally, we would like to recognize the partial support for this work provided by the National Key R&D Project (2022YFB3103500), National Natural Science Foundation of China (Grant No. 62202150, 62302162, 62102175, 62372166, U20A20174, U22A2030), Hunan Provincial Key Research and Development Program (2024AQ2041), China Postdoctoral Science Foundation General Funding (2023M741123), Aid Program for Science and Technology Innovative Research Team in Higher Educational Institutions of Hunan Province, and Fundamental Research Funds for the Central Universities.

REFERENCES

[1] Monjur Alam, Haider Adnan Khan, Moumita Dey, Nishith Sinha, Robert Callan, Alenka Zajic, and Milos Prvulovic. 2018. One&*Done* : *ASingle* − *DecryptionEM* − *Based* Attack on OpenSSL's Constant-Time Blinded RSA. In *Proccedings of the 2018 USENIX Security Symposium (USENIX Security)*.

[2] Ryota Birukawa, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. 2019. A study on an Effective Evaluation Method for EM Information Leakage without Reconstructing Screen. In *Proceedings of the 2019 International Symposium on Electromagnetic Compatibility (EMC EUROPE)*.

[3] Rose Ceccio, Sophie Stephenson, Varun Chadha, Danny Yuxing Huang, and Rahul Chatterjee. 2023. Sneaky Spy Devices and Defective Detectors: The Ecosystem of Intimate Partner Surveillance with Covert Devices. In *Proceedings of the 2023 USENIX Security Symposium (USENIX Security)*.

[4] Anadi Chaman, Jiaming Wang, Jiachen Sun, Haitham Hassanieh, and Romit Roy Choudhury. 2018. Ghostbuster: Detecting the presence of hidden eavesdroppers. In *Proceedings of the 2018 Annual International Conference on Mobile Computing and Networking (MobiCom)*.

[5] Huiling Chen, Wenqiang Jin, Yupeng Hu, Zhenyu Ning, Kenli Li, Zheng Qin, Mingxing Duan, Yong Xie, Daibo Liu, and Ming Li. 2024. Eavesdropping on Black-box Mobile Devices via Audio Amplifier's EMR. In *Proceedings of the 2018 Annual International Conference on Network and Distributed System Security (NDSS)*.

[6] Yushi Cheng, Xiaoyu Ji, Tianyang Lu, and Wenyuan Xu. 2018. Dewicam: Detecting hidden wireless cameras via smartphones. In *Proceedings of the 2018 ACM International Conference on Asia Conference on Computer and Communications Security (ASIACCS)*.

[7] Yushi Cheng, Xiaoyu Ji, Juchuan Zhang, Wenyuan Xu, and Yi-Chao Chen. 2019. Demicpu: Device fingerprinting with magnetic signals radiated by cpu. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS)*.

[8] Jieun Choi, Hae-Yong Yang, and Dong-Ho Cho. 2020. Tempest comeback: A realistic audio eavesdropping threat on mixed-signal socs. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS)*.

[9] Takayuki Daimon, Hiroshi Sadamura, Takayuki Shindou, Haruo Kobayashi, Masashi Kono, Takao Myono, Tatsuya Suzuki, Shuhei Kawai, and Takashi Iijima. 2003. Spread-spectrum clocking in switching regulators for EMI reduction. *IEICE transactions on fundamentals of electronics, communications and computer sciences* 86, 2 (2003), 381–386.

[10] Yariv Ephraim and David Malah. 1984. Speech enhancement using a minimum-mean square error short-time spectral amplitude estimator. *IEEE Transactions on acoustics, speech, and signal processing* 32, 6 (1984), 1109–1121.

[11] Yuichi Hayashi, Naofumi Homma, Mamoru Miura, Takafumi Aoki, and Hideaki Sone. 2014. A threat for tablet pcs in public space: Remote visualization of screen images using em emanation. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS)*.

[12] Yan He, Qiuye He, Song Fang, and Yao Liu. 2021. MotionCompass: pinpointing wireless camera via motion-activated traffic. In *Proceedings of the 2021 ACM International Conference on Mobile Systems, Applications, and Services (MobiSys)*.

[13] Ahmed Helmy and Mohammed Ismail. 2006. The chip-A design guide for reducing substrate noise coupling in RF Applications. *IEEE Circuits and Devices Magazine* 22, 5 (2006), 7–21.

[14] Jiahao Huang, Haiyang Zhang, Lin Wang, Zilong Zhang, and Changming Zhao. 2021. Improved YOLOv3 Model for miniature camera detection. *Optics & Laser Technology* 142 (2021), 107133.

[15] Wenqiang Jin, Srinivasan Murali, Huadi Zhu, and Ming Li. 2021. Periscope: A keystroke inference attack using human coupled electromagnetic emanations. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS)*.

[16] Jin Au Kong. 1975. Theory of electromagnetic waves. *New York* (1975).

[17] LCSC ELECTRONICS. 2024. LCSC Suppliers. https://www.lcsc.com/supplier/.

[18] Zhijing Li, Zhujun Xiao, Yanzi Zhu, Irene Pattarachanyakul, Ben Y Zhao, and Haitao Zheng. 2018. Adversarial localization against wireless cameras. In *Proceedings of the 2018 International Workshop on Mobile Computing Systems & Applications (HotMobile)*.

[19] Qianru Liao, Yongzhi Huang, Yandao Huang, Yuheng Zhong, Huitong Jin, and Kaishun Wu. 2022. MagEar: eavesdropping via audio recovery using magnetic side channel. In *Proceedings of the 2022 ACM International Conference on Mobile Systems, Applications, and Services (MobiSys)*.

[20] Chun Liu, Changming Zhao, Haiyang Zhang, Zilong Zhang, Zitao Cai, and Zhipeng Li. 2019. Spectrum classification using convolutional neural networks for a mini-camera detection system. *Applied optics* 58, 33 (2019), 9230–9239.

[21] Chun Liu, Changming Zhao, Haiyang Zhang, Zilong Zhang, Yanwang Zhai, and Yali Zhang. 2019. Design of an active laser mini-camera detection system using cnn. *IEEE Photonics Journal* 11, 6 (2019), 1–12.

[22] Tian Liu, Ziyu Liu, Jun Huang, Rui Tan, and Zhen Tan. 2018. Detecting wireless spy cameras via stimulating and probing. In *Proceedings of the 2018 Annual International Conference on Mobile Systems, Applications, and Services (MobiSys)*.

[23] Ziwei Liu, Feng Lin, Chao Wang, Yijie Shen, Zhongjie Ba, Li Lu, Wenyao Xu, and Kui Ren. 2023. Camradar: Hidden camera detection leveraging amplitude-modulated sensor images embedded in electromagnetic emanations. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)* 6, 4 (2023), 1–25.

[24] Zhuoran Liu, Niels Samwel, Léo Weissbart, Zhengyu Zhao, Dirk Lauret, Lejla Batina, and Martha Larson. 2020. Screen gleaning: A screen reading TEMPEST attack on mobile devices exploiting an electromagnetic side channel. *arXiv preprint arXiv:2011.09877* (2020).

[25] Henrique Teles Maia, Chang Xiao, Dingzeyu Li, Eitan Grinspun, and Changxi Zheng. 2021. Can one hear the shape of a neural network?: Snooping the GPU via Magnetic Side Channel. *arXiv preprint arXiv:2109.07395* (2021).

[26] MediaTek. 2024. MT2503 Design Notice. https://d86o2zu8ugzlg.cloudfront.net/mediatek-craft/documents/mt3333/MT3333_Datasheet.pdf.

[27] Saeed Mirzamohammadi and Ardalan Amiri Sani. 2016. Viola: Trustworthy sensor notifications for enhanced privacy on mobile systems. In *Proceedings of the 2016 ACM International Conference on Mobile Systems, Applications, and Services (MobiSys)*.

[28] Department of Defense (DoD). 2024. Consumer privacy & identity quarterly. https://www.soc.mil/IdM/publications/CPIQ/quarterly2_3.pdf.

[29] HackRF One. 2024. HackRF one. https://greatscottgadgets.com/hackrf/one.

[30] Sanghoon Park, Lawrence E Larson, and Laurence B Milstein. 2010. An RF receiver detection technique for cognitive radio coexistence. *IEEE Transactions on Circuits and Systems II: Express Briefs* 57, 8 (2010), 652–656.

[31] Yihua Peng, Jiemin Zhang, Jian Mao, and Mengmeng Cui. 2023. A USB Keyboard Electromagnetic Information Detection Algorithm Based on Deep Learning. In *Proceedings of the 2023 IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS)*.

[32] Emiel Por, Maaike van Kooten, and Vanja Sarkovic. 2019. Nyquist–Shannon sampling theorem. *Leiden University* 1, 1 (2019), 1–2.

[33] Quectel. 2019. Quectel MC20 Hardware Design V1.0. https://sisoog.com/wp-content/uploads/2019/12/Quectel_MC20_Hardware_Design_V1.0.pdf.

[34] Soundarya Ramesh, Ghozali Suhariyanto Hadi, Sihun Yang, Mun Choon Chan, and Jun Han. 2022. TickTock: Detecting Microphone Status in Laptops Leveraging Electromagnetic Leakage of Clock Signals. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS)*.

[35] Muhammad Salman, Nguyen Dao, Uichin Lee, and Youngtae Noh. 2022. CSI: DeSpy: Enabling Effortless Spy Camera Detection via Passive Sensing of User Activities and Bitrate Variations. *Proceedings of the ACM International Conference on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)* 6, 2 (2022), 1–27.

[36] Sriram Sami, Sean Rui Xiang Tan, Bangjie Sun, and Jun Han. 2021. Lapd: Hidden spy camera detection using smartphone time-of-flight sensors. In *Proceedings of the 2021 ACM Conference on Embedded Networked Sensor Systems (SenSys)*.

[37] Nader Sehatbakhsh, Alireza Nazari, Haider Khan, Alenka Zajic, and Milos Prvulovic. 2019. Emma: Hardware/software attestation framework for embedded systems using electromagnetic signals. In *Proceedings of the 2019 Annual IEEE/ACM International Symposium on Microarchitecture (MICRO)*.

[38] Sekorm. 2024. AT6558R Design Notice. https://en.sekorm.com/doc/1440132.html.

[39] Rahul Anand Sharma, Elahe Soltanaghaei, Anthony Rowe, and Vyas Sekar. 2022. Lumos: Identifying and Localizing Diverse Hidden IoT Devices in an Unfamiliar Environment. In *Proceedings of the 2022 USENIX Security Symposium (USENIX Security)*.

[40] Cheng Shen and Jun Huang. 2021. EarFisher: Detecting Wireless Eavesdroppers by Stimulating and Sensing Memory EMR. In *Proceedings of the 2021 USENIX Symposium on Networked Systems Design and Implementation (NSDI)*.

[41] Cheng Shen, Jun Huang, Guangyu Sun, and Jingshu Chen. 2022. Electromagnetic Fingerprinting of Memory Heartbeats: System and Applications. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)* (2022).

[42] Cheng Shen, Tian Liu, Jun Huang, and Rui Tan. 2021. When LoRa meets EMR: Electromagnetic covert channels can be super resilient. In *Proceedings of the 2021 IEEE Symposium on Security and Privacy (S&P)*.

[43] SHENZHEN YITUOWULIAN SYSTEM CO., LTD. 2024. GPS Tracker Locator. https://www.gpstrackerlocator.com/.

[44] Akash Deep Singh, Luis Garcia, Joseph Noor, and Mani Srivastava. 2021. I Always Feel Like Somebody's Sensing Me! A Framework to Detect, Identify, and Localize Clandestine Wireless Sensors. In *Proccedings of the 2021 USENIX Security Symposium (USENIX Security)*.

[45] Colin Stagner, Andrew Conrad, Christopher Osterwise, Daryl G Beetner, and Steven Grant. 2011. A practical superheterodyne-receiver detector using stimulated emissions. *IEEE Transactions on Instrumentation and Measurement* 60, 4 (2011), 1461–1468.

[46] Yang Su, Daniel Genkin, Damith Ranasinghe, and Yuval Yarom. 2017. USB Snooping Made Easy: Crosstalk Leakage Attacks on USB Hubs. In *Proceedings of the 2017 USENIX Security Symposium (USENIX Security)*.

[47] U-Blox. 2024. Modern GNSS/GPS signals. https://content.u-blox.com/sites/default/files/documents/GPS-signals-migration-wp.pdf.

[48] U-BLOX. 2024. U-BLOX LEA-NEO-MAX-6. https://content.u-blox.com/sites/default/files/products/documents/LEA-NEO-MAX-6_HIM_(UBX-14054794)_1.pdf.

[49] U-BLOX. 2024. U-BLOX MIA-F10Q. https://content.u-blox.com/sites/default/files/documents/MIA-F10Q_ProductSummary_UBX-23010023.pdf.

[50] Veronica Valeros and Sebastian Garcia. 2017. Spy vs. Spy: A Modern Study Of Microphone Bugs Operation And Detection. In *Proceedings of the 2017 Chaos Communication Congress*.

[51] Ruize Wang, Huanyu Wang, and Elena Dubrova. 2020. Far field EM side-channel attack on AES using deep learning. In *Proceedings of the 2020 ACM Workshop on Attacks and Solutions in Hardware Security*.

[52] Ruize Wang, Huanyu Wang, Elena Dubrova, and Martin Brisfors. 2021. Advanced far field EM side-channel attack on AES. In *Proceedings of the 2021 ACM on Cyber-Physical System Security Workshop*.

[53] Kevin Wu and Brent Lagesse. 2019. Do you see what i see? detecting hidden streaming cameras through similarity of simultaneous observation. In *Proceedings of the 2019 IEEE International Conference on Pervasive Computing and Communications (PerCom)*.

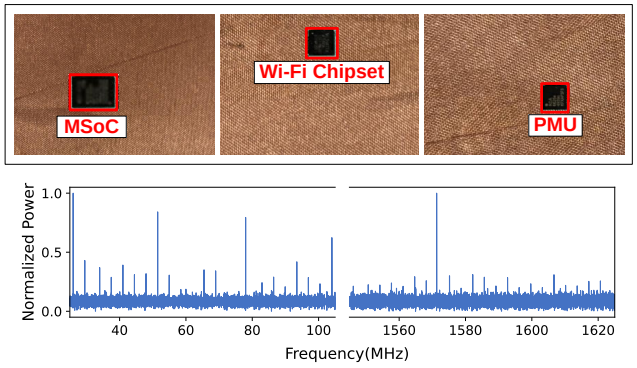
[54] www.gps.gov. 2024. GPS Protocol. https://www.gps.gov/technical/ps/2020-SPS-performance-standard.pdf.

[55] www.gps.gov. 2024. New Civil Signals. https://www.gps.gov/systems/gps/modernization/civilsignals/.

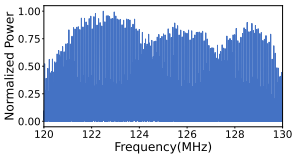
[56] Honggang Yu, Haocheng Ma, Kaichen Yang, Yiqiang Zhao, and Yier Jin. 2020. DeepEM: Deep Neural Networks Model Recovery through EM Side-Channel Information Leakage. In *Proceedings of the 2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*.

[57] Zihao Zhan, Zhenkai Zhang, Sisheng Liang, Fan Yao, and Xenofon Koutsoukos. 2022. Graphics peeping unit: Exploiting em side-channel information of gpus to eavesdrop on your neighbors. In *Proceedings of the 2022 IEEE Symposium on Security and Privacy (S&P)*.

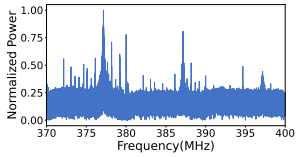
[58] Ruochen Zhou, Xiaoyu Ji, Chen Yan, Yi-Chao Chen, Wenyuan Xu, and Chaohao Li. 2023. DeHiREC: Detecting Hidden Voice Recorders via ADC Electromagnetic Radiation. In *Proceedings of the 2023 IEEE Symposium on Security and Privacy (S&P)*.



(a) **MSoC**



(b) **PMU**



(c) **Wi-Fi Chipset**

Figure 23: EMR spectra of each module inside the GPS Tracker

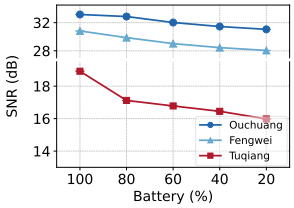
11 APPENDIX

11.1 EMR Spectra of GPS Tracker's Each Module

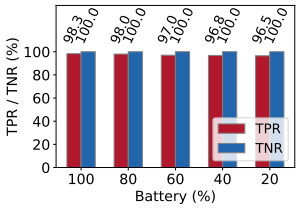
Intuitively, each circuit components inside the GPS trackers could generate a unique EMR spectrum. As shown in Figure 23, we cover the Tuqiang tracker's majority PCB circuits with copper materials while leaving one critical module exposed during each EMR measurement. Figure 23(a)-(c) show the EMR spectra of MSoC, PMU, and WiFi-Chipset, respectively. It is observed that PMU and WiFi-Chipset have distinct EMR spectra patterns compared to the MSoC. This is because that they are built with different signal processing circuits. However, we cannot use the EMR spectra of PMU or WiFi-Chipset to detect the hidden GPS trackers, as these circuits components are commonly found in wide range of electronics, leading to a high likelihood of false alarms. In contrast, as discussed in Section 4.1, trackers' MSoCs are specifically designed to process GPS signals. Their EMR spectra would be a more reliable source for identifying hidden GPS trackers.

11.2 Impact of Battery Level

Similar to most modern electronic devices, the GPS trackers will adjust their performance based on the battery state. Such adjustments can lead to variations in EMR signal strength at different levels of power consumption. Accordingly, we measured the EMR SNR, TPR and TNR of three GPS trackers at distances of 10 cm, with battery levels at 100%, 80%, 60%, 40%, and 20%. As shown in Figure 24, different battery levels indeed cause fluctuations in EMR signal strength, and these changes differ among GPS trackers. However, even in a low battery state, the EMR SNR remains above 15 dB, which is sufficient for the system to detect, thereby maintaining average TPR at 97.32% and average TNR at 100%. This suggests that *GPSBuster* is capable of accurate detection even when the GPS trackers are in a low-power state.



(a) EMR SNR



(b) TPR&TNR

Figure 24: Impact of battery level.