Disconnected and Still Visible: Permissionless Compromise of Location Privacy in Mobile Devices

Kenneth Block
Northeastern University
Boston, MA 02115
block.k@husky.neu.edu

Guevara Noubir
Northeastern University
Boston, MA 02115
noubir@ccs.neu.edu

ABSTRACT

Although privacy compromises remain an issue among users and advocacy groups, identification of user location has emerged as another point of concern. Techniques using GPS, Wi-Fi, NFC, Bluetooth tracking and cell tower triangulation are well known. These can typically identify location accurately with meter resolution. Another technique, inferring routes via sensor exploitation, may place a user within a few hundred meters of a general location. Acoustic beacons such as those placed in malls may have more finely grained resolution yet are limited by the sensitivity of the device's microphone to ultrasonic signals and directionality. In this paper we are able to discern user location within commercial GPS resolution by leveraging the ability of mobile device magnetometers to detect externally generated signals in a permissionless attack. We are able to achieve an aggregate location identification success rate of 86% with a bit error rate of 1.5% which is only ten times the stationary error rate. We accomplish this with a signal that is a fraction of the Earth's magnetic field strength.

We designed, prototyped, and experimentally evaluated a system where a location ID is transmitted via low power magnetic coil(s) and received by permissionless apps. The system can be located at ingresses and kiosks situated in malls, stores, transportation hubs and other public locations including crosswalks using a location ID that is mapped to the GPS coordinates of the facility hosting the system. We demonstrate that using Android phone magnetometers, we can correctly detect and identify the when and the where of a device when the victim walks at a comfortable pace while their device has all the aforementioned services disabled. In order to address the substantial signal fading effects due to mobility in a very-low power magnetic near field, we developed signal processing and coding techniques and evaluated the prototype on six android devices in an IRB-approved study with six participants.

ACM Reference format:
Kenneth Block and Guevara Noubir. 2018. Disconnected and Still Visible: Permissionless Compromise of Location Privacy in Mobile Devices. In *Proceedings of ACM WiSec conference, Stockholm, Sweden, June 2018 (WiSec'18),* 11 pages.
DOI: 10.1145/nnnnnnn.nnnnnnn

WiSec'18, Stockholm, Sweden

DOI: 10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Location tracking has achieved significant attention in the research community [14, 23, 25, 29, 30] and great notoriety in the news cycle. In late 2017, Quartz [7] reported that Android devices sent location data to Google when they were within range of a new cell tower. Although Google denied using this information for any malicious purposes and that Android devices would henceforth no longer transmit the data, it is yet another example of realizing the fear of being tracked. Uber [4] recently removed a feature that tracked riders for several minutes post ride termination. In an example of an unintended consequences, Strava [5] identified that US soldiers might be tracked via GPS coordinates available through a fitness app. The U.S. judicial system is now involved in the discussion as the Supreme Court agreed in 2017 to hear Carpenter v. United States [19] where the government was using cell phone records to identify locations where the phone had been, further demonstrating that tracking data is available and an evolving legal concern. In 2018, the Wall Street Journal published an article explaining the lucrative and expanding business of selling location data [22]. Each of these represent the potential for tracking and abuse of location information. Most disconcerting is the reluctance and / or slow response to preventing these compromises.

This paper presents a unique location compromise via a stealthy location attack built upon a smartphone magnetometer's ability to detect small coded magnetic field fluctuations while the device is in motion. The attacker generates location identification information which is transmitted from an innocuous physical source. A device resident app, listens to the sensor output, performs noise removal processing and decodes the resultant signal which represents the transmitter's location with commercial GPS accuracy. Combined with time, the attacker knows the when and where of the victim's device despite her efforts to be temporarily disconnected from 'the grid' by disabling Wi-Fi, cellular, NFC, Bluetooth and GPS services. Even within a building, its accuracy exceeds Wi-Fi and cellular triangulation with these services enabled. One of the significant challenges to this attack is extracting the low-level signal from system and motion induced noise. System noise results from the magnetometer reporting scheme where the Hardware Abstraction Layer in some cases generates reports in a quasi-return to zero format. Motion noise induced from victim movement causes the readings to shift relative to its reference orientation. We evaluate channel viability by reducing system noise and account for motion noise stemming from carrying the device in typical manner i.e., a belt or a shoulder bag. This initial work addresses only these two conveyance modalities.

The attack is unique as it is an out-of-band, unilateral, non-persistent communications pathway that is difficult to detect. This

permissionless attack is useful for commercial, law enforcement and unfortunately, malicious purposes with outgoing communications occurring asynchronously post data capture. Mitigation is challenging without modifying the Operating System to seek permissions for sensor use, changing the sampling rate or changing device sensitivity.

Our contributions to this Independent Review Board (IRB) approved research can be summarized as follows:

- To the best of our knowledge, we are the first to report the use of magnetic field communications to compromise a victim's location privacy.
- We designed, built, and evaluated a system that is transferable to real-world deployments and scalable to at least one million locations.
- The system is intended to identify location absent of Wi-Fi, cellular, GPS, Bluetooth and NFC services and the attack functions without the need for permissions, making detection difficult.
- We developed signal processing and coding techniques that address the substantial signal fading effects due to mobility in a very-low power magnetic near field.
- We evaluated the prototype on six android devices, in an IRB-approved study with six participants.
- We achieved an aggregate location identification success rate of 86% with a bit error rate of 1.5% which is only ten times the stationary error rate.
- The solution's position accuracy is controlled by the attacker rather than the mobile device's capabilities.

The remainder of this paper is constructed as follows. In Sections 2 and 3, we describe the background, motivation and threat model for the attack. Section 4 details the system design and some of the practical limitations for this attack type. Section 5 describes the testing methodology and results of the two walking tests. Section 6 describes mitigation options and we end with a related works discussion and conclusion in Section 7 and Section 8 respectively.

Figure 1: System Design

2 BACKGROUND AND MOTIVATION

Location identification as a means to compromise privacy is a significant concern. Deriving location via Wi-Fi, cell tower triangulation and sensor exploitation is well researched, with typical accuracies of a few hundred yards and at best, tens of feet. GPS, with better accuracy, has limited functionality within buildings. Despite the advantages of location services and the economic benefit that beacons may provide, fear of actors such as law enforcement [18] engaging in user tracking remains. Other permissionless forms of location compromises may involve the gyroscope and the accelerometer. However, absent the use of recorded dead reckoning data to infer position, there is little research involving magnetometer specific attacks. Some directly related attacks are:

Magnetic mapping, Gozick [10], is used to identify a physical structure's footprint by its magnetic fields. Assuming each building has a unique signature, the attacker can determine where a particular device has been. The limitations are the magnitude of collected data (device and site) and how effectively it correlates to known magnetic fingerprints.

In a short-range communications example, Matyunin [20] identified a communications channel using a PC's disk drive as the source and the magnetometer from a second device as the sink where both devices are stationary. They achieved a bit rate of 4 bps at a distance of 4 cm. Similarly, [31] uses radiation patterns to identify opening and closing of applications resident on adjacent platforms.

Although the magnetometer is used in Narain's [24] location inference attack, it is not the primary contributing sensor. The accelerometer and the gyroscope were used primarily to determine position using graph analysis referenced to the OpenStreetMap database. Its accuracy is limited to half the distance between map street junctions and cannot be applied in pedestrian, rail, ship or air travel contexts.

iBeacon™, an Apple technology, uses Bluetooth low energy (BLE) identifiers that a smartphone app can listen to, enabling device location and customer tracking etc. In this case, the user enables tracking services, clearly willing to be tracked to enhance the shopping experience.

An additional vector of recent interest involves facial recognition, Gunther [11], and presentation attacks, Ramachandra [26]. However, identity matching remains problematic primarily due to database completeness limitations. Unless access to law enforcement types of databases is available, the attacks have limited effectiveness unless the presentation attack involves scanning social media databases containing pictures and executing resource intensive activities.

Each of these has limitations such as range, data size, resolution or enabling of location services. Our motivation is to, absent of such limitations, track the user despite her attempts to prevent such efforts. The solution is scalable, limited to the willingness of the tracking entity to install a system to perform this type of privacy invasion.

3 THREAT MODEL

This section describes the threat model.

3.1 Vulnerability

A vulnerability exists in the Android space where direct reading of sensor data is not restricted when using the SensorManager class and access is not encumbered by declaring their use in the AndroidManifest.XML file. With this permissionless access control, the user is not alerted to sensor use at installation time nor at run time. This allows magnetometer data to be accessed without security limitations. Furthermore, the attack involves only one-way communications with the magnetometer acting as a passive receiver without the need for permission dependent transmitting resources.

On the human side, we rely on social media and Google play ratings to convince users to download the app. The app must be well rated which is achieved by procuring high ratings, seeding a 'like' in social media via Facebook and utilizing other social means. The latter a result of a general willingness to try new apps based on reviews from unknown and untrusted sources [27]. In this manner, the illusion of app trust is established and propagated.

3.2 Threat

The threat is in obtaining position information despite the victim's efforts to avoid leaking this information. It is assumed that she disables Wi-Fi, NFC, GPS, Bluetooth and cellular services. The device however, remains powered on. This condition is consistent with placing the device in airplane mode in addition to disabling location supporting services. The victim installs a seemly innocuous app that functions even when placed in the background. All that remains is for the victim to move in proximity to the system.

3.3 Attack

The attack is driven by a select group of potentially malicious and benign actors. Those benefiting might include, governments, law enforcement, marketing and sales analysts and the hosting entity. Government and law enforcement interests are based on the desire to track any number of individuals for location history purposes. Notification of their activities to third parties and data usage would be subject to jurisdictional laws. Marketing and sales analysts would seek to identify drive-by individuals for campaign targeting. Supplemental means to contact the target(s) i.e., via text messaging and email, might occur subsequent to a 'hit'. Similarly, the hosting entity might desire to use this in support of in-store sales activities and broader campaigns.

The attack is enabled by placing a transmitter in high traffic locations. The target(s) enters the transmitter's field of view and if the malicious app is present, the attack should succeed.

The transmitter and the controller elements may be embedded in the floor, ceiling or a wall. The installation would be minor for new construction or store set-up and slightly more complicated for existing structures. The transmitter may also be located in kiosks, cross walks and bus, airplane and train terminals.

3.4 Exploit

The innocuous app, masquerading as a legitimate function, i.e., a tasker, file explorer, calendar etc., is a registered sensor listener that records magnetometer data. Upon synch frame detection, the data is processed, stored and subsequently transmitted to an off-board colluding application when Wi-Fi or cellular services are enabled.

3.5 Trust

Trust is presumed in two cases. First, the victim believes that her movements are not tracked when disabling location related services. Second, she has downloaded an app that provides valuable functionality and whose app store ratings meet her satisfaction.

4 SYSTEM DESIGN

4.1 Magnetometer Based Tracking System Overview

The system overview diagram is illustrated in Figure 1. We show a victim, oblivious to the platform beneath her feet, as she walks toward her destination. Alternatively, she is walking in proximity to an innocent looking kiosk. She is unaware that each of these structures house a subsystem that generates coded yet harmless magnetic fields strong enough for her smartphone's magnetometer to detect. She is also unaware that the 'really cool' app she downloaded is also recording this data unbeknownst to her.

We envision that each of these system types is potentially located in stores, malls, transportation hubs, cross-walks or in other locations where victims would patronize or be in close proximity. The smartphone's app functions include recording magnetometer data and exfiltrating semi-processed data.

The nature of this app could support malicious or non-malicious activities. In the former case, the app supports location exposure, violating user privacy. In the latter case, the app can support targeted shopping as a commerce-oriented beacon. It may also enhance law enforcement activities such as persons of interest tracking.

In all cases, the system is placed in a predetermined location, where each location is assigned a unique ID. Since this attack is expected to scale to one million instances, the coding approach is important. Code selection must also account for long continuous equal-bit value sub-streams to avoid frequency content similar to the victim's gait.

Each station issues its unique code in perpetuity, triggered by an external event such as depressing a pressure switch on the floor or interrupting an optical loop. This ensures that the victim's phone is within detection range of the coded electromagnetic (EM) field emissions from the platform coil(s). Based on anthropomorphic data [3], we set the transmission field strength at 37 to 41 inches above the plane of the coil(s) to be less than 30μT. Although the only platform limitations are size, this influences EM field strength. The former is driven by physical limitations of the deployment site while the latter is a function of current, turn count, coil dimensions and the permitted power ceiling.

The magnetometer data stream is filtered to remove device anomalies, high frequencies and the effect of the human gait. Automated Gain Control (AGC) is applied post filtering to compensate for uneven signal strength due to position within the magnetic field. The app either waits until it is within a Wi-Fi range and transmits the individual identification out to a participating server or data is aggregated and transferred in batch. In either case, the locations and times are now available from which further attacks may be launched.

Figure 2 illustrates the major transmit side elements: The controller, switching circuitry and the platform hosting the coils. The first two are described in Section 4.5 while the platform is addressed in Section 4.4.

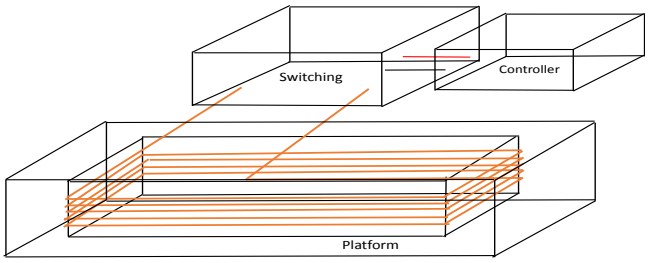


Figure 2: System Building Blocks

4.2 Magnetic Flux Determination

Due to the asymmetric nature or our platform, we derive the magnetic flux density **B** at a point in space $\mathbf{P_{x,y,z}}$ for a rectangular coil, Figure 3, of N turns. This vector consists of each of the axial flux density contributions $\mathbf{B_x}, \mathbf{B_y}, \mathbf{B_z}$ at **P** as the target device passes through the magnetic field. This coordinate system is consistent with the three axis Cartesian coordinate system found on smartphones.

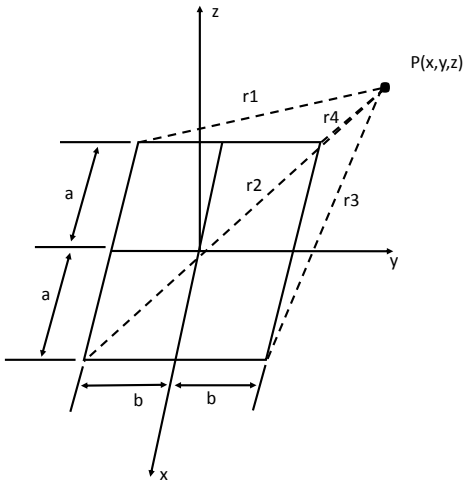


Figure 3: Point In Space Magnetic Flux

The magnitude is given by equation 1.

$$\mathbf{B} = \sqrt{\mathbf{B_x^2} + \mathbf{B_y^2} + \mathbf{B_z^2}} \tag{1}$$

where $\mathbf{B_x}, \mathbf{B_x}, \mathbf{B_x}$ are x,y and z plane flux contributions

$$\mathbf{B_x} = \mathbf{N}\frac{\mu_0 \mathbf{I}}{4\pi}\sum_{\alpha=1}^{4}\left[\frac{-\mathbf{1}^{\alpha+1}\mathbf{z})}{\mathbf{r}_\alpha[\mathbf{r}_\alpha + \mathbf{d}_\alpha]}\right] \tag{2}$$

$$\mathbf{B_y} = \mathbf{N}\frac{\mu_0 \mathbf{I}}{4\pi}\sum_{\alpha=1}^{4}\left[\frac{-\mathbf{1}^{\alpha+1}\mathbf{z})}{\mathbf{r}_\alpha[\mathbf{r}_\alpha + -\mathbf{1}^{\alpha+1}\mathbf{C}_\alpha]}\right] \tag{3}$$

$$\mathbf{B_z} = \mathbf{N}\frac{\mu_0 \mathbf{I}}{4\pi}\sum_{\alpha=1}^{4}\left[\frac{-\mathbf{1}^{\alpha+1}\mathbf{z}}{\mathbf{r}_\alpha[\mathbf{r}_\alpha + -\mathbf{1}^{\alpha+1}\mathbf{C}_\alpha]} - \frac{\mathbf{C}_\alpha}{\mathbf{r}_\alpha[\mathbf{r}_\alpha + \mathbf{d}_\alpha]}\right] \tag{4}$$

and α is a side (one of four), **N**, **I**, μ_0 are the coil turn count, current and permeability respectively and where:

$$C_1, -C_4 = a + x \quad \text{and} \quad C_2, -C_3 = a - x \tag{5}$$

$$d_1 = d_2 = y + b \quad \text{and} \quad d_3 = d_4 = y - b \tag{6}$$

$$r_1 = \sqrt{(a+x)^2 + (y+b)^2 + z^2} \tag{7}$$

$$r_2 = \sqrt{(a-x)^2 + (y+b)^2 + z^2} \tag{8}$$

$$r_3 = \sqrt{(a-x)^2 + (y-b)^2 + z^2} \tag{9}$$

$$r_4 = \sqrt{(a+x)^2 + (y-b)^2 + z^2} \tag{10}$$

a and b are half the length and half the width of the coil respectively and C_α and d_α are reference points enabling the derivation of r_α, the Euclidean distance of each corner to **P**. These equations are the foundation for the design/parametrization of our system prototype. The key point is that $\mathbf{B_{x,y,z}}$ is affected linearly with **N** and **I** and inversely proportional with r_α.

4.3 Challenges and Tradeoffs

There are seven factors that drive the system design.

- **Platform Size:** We are limited by the magnetic field size which is a function of platform size. Hosts will want to limit the system's physical footprint and make it imperceptible.
- **Magnetometer Sampling Rates:** We are limited by the device's sensor sample rates. Low rates necessitate larger signal pulsewidth, which in turn increases transmission and in-the-field times.
- **Speed:** The speed at which humans can walk affects attack viability. If the velocity is too high, the code pattern may not be received *in toto* as the device passes though the magnetic field.
- **Scale:** The system must scale to support a large set of deployments which drives the payload length.
- **Device Orientation:** The position ID must be resolvable without regard to device orientation.
- **Safety:** The system must not radiate magnetic fields large enough to cause harm.
- **Stealth:** The system attack must be stealthy and function without GPS, Wi-Fi, NFC, Bluetooth and cellular location supporting capabilities during execution.

4.4 Design Decisions, Observations and Parametrics

- **Scope:** Since we are in the initial stages of this effort, the testing scope was limited to a belt and a shoulder bag. Other transport modalities which are useful in completing this effort include in-clothing pockets, in-hand and armband modalities. In addition, the transmitter was limited for this current series of experiments to floor operations, whereas in-wall, in-ceiling, kiosk resident and security tower-like structures are viable deployment alternatives.
- **Sampling:** The largest sampling period of any evaluated device tested was 18.9 msec. This limits the lower bound signaling pulsewidth to approximately 37.8 msec to avoid aliasing effects. We utilize 45 msec to account for future target devices within our prototype's dimensions limits.
- **Data Frame Sizing:** We utilize a synchronization preamble and a payload consisting of an ID information field and a validation field. ID length must factor in the number of unique locations and any necessary coding overhead.

$$n = t \times 1/pw \tag{11}$$

$$t = L/v \tag{12}$$

We define the longitudinal velocity of the human passing through the magnetic file, v; the length of the platform, L; the time in field, t; the pulsewidth, pw; the number of bits that can be detected while in the magnetic field, $bits_r$; the number of bits transmitted once triggered, $bits_t$; the frame length, n; the number of deployed platforms p. Since Equations 11 and 12 must be solved simultaneous and if

$bits_t = bits_r = n$, then using t, the maximum time in field to solve for n, $t = n \times pw = L/v \rightarrow \mathbf{n = 1/pw \times L/v}$.

- **Device Velocity:** Velocity affects the time within the magnetic field. From Bohannon [6], the nominal comfortable gait speed is ≈ 4.6 feet/sec.
- **Physical Size:** We assume platform dimensions of 8.7 feet x 36 inches. Since the magnetic flux lines extend beyond the physical boundary of the coil and due to the test environment's physical constraints, we set the length as slightly less than 4.6 × pw × n which represents a balance of minimal intrusiveness, physical constraints and meeting performance needs.
- **Gait Amplitude Contribution:** We found in our experiments that the deviation in magnetometer readings attributable to the gait was approximately equal to ±15μT. This amplitude is similar to that induced by the signal.
- **Distinguishing Gait from Data:** Long contiguous snippets of equal valued data can be construed as a gait induced contribution. For example, 8 bits at 45 msec per bit is 360 msec, which in terms of frequency, is within the gait frequency band. As a result, the data must be coded to account for these occurrences. For this exercise, we intentionally shortened the permitted identical contiguous bit sub-streams and accepted the bit length penalty of a longer ID field.
- **Scale:** The key issue is determining the bit stream length to accommodate the limited time within the magnetic field and the sampling rate limitations while providing effective signal discrimination. We selected 1 million possible platforms, 20 bits uncoded, to provide a modest level of scaling.
- **Safety:** In a joint question and answer report [2], the U.S. National Institutes of Environmental Health Sciences and Health suggested that the levels associated with hair dryers (nominally 300μT) and electric razors (nominally 100μT) at operating distances are safe to humans in normal use. In a static position measurement taken below the knee, our maximum RMS field strength was approximately 44μT. At range, our worst-case field strength is ≈ 20μT. Exposure time in the appliance case is several minutes while less than 5 seconds with ours.
- **Stealth:** The attack is permissionless, making detection difficult. Exfiltration to a third party, albeit needing permissions, is not the objective of this study.

4.5 Coil and Electronics Design

4.5.1 Coil Design. Table 1 highlights coil parametric information for the hand wound, air-gapped coil using a wooden frame as a bobbin and magnet wire as the conductor. These parameters approximate a real-world deployment.

4.5.2 Electronics Design. The electronic circuitry, Figure 4, consists of an Arduino based Linkit Smart 7688 series controller, two linear power supplies providing ±12.5V voltage rails, voltage suppression / fly-back capability and solid-state switches, in a single pole, double throw configuration, which supplies current to the coil(s). The Arduino controller enables the switches on a per bit basis where each bit has a duration of 45 msec. Individual bits are coded in a non-return-to-zero (NRZ) format. We selected NRZ since the magnetic field's rise and fall time approached 10 msec which potentially increases aliasing at the sensor sampling rates. We switch between the voltage rails to support rapid charging and discharging of the coil(s), L1, without the need for AC coupling.

Parameter	Value
Dimensions (Inches)	67.5 x 24.5
Turns	65
Height (Inches)	1.25
Inductance (Henries)	0.024
Wire Length (Feet)	993
Wire Nominal Resistance (Ohms)	6
Wire Guage (AWG)	18
Relative Permeability (μ/μ_0)	1.00000043

Table 1: Coil Parameters

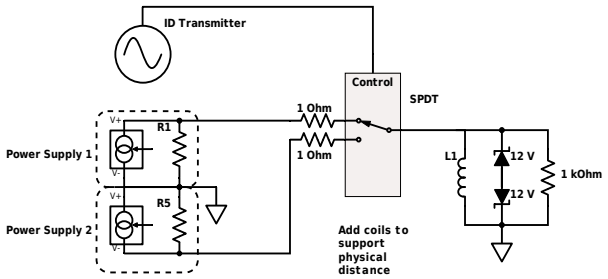


Figure 4: Single Coil Circuit Design

4.6 Code Selection and Payload Design

Coding selection presents a challenge since we are limited to 32 bits for data and checking based on the previously described physical constraints. Concatenating Hamming codes [13] is insufficient since, for example, in an 8-4-4 Hamming scheme, one needs eight bits to get four bits and the scale and payload conditions are violated. Gold codes [17] and Kasami codes [32] do not allow enough preferred pairs to satisfy the scale objective while simultaneously satisfying the number of bits available. Compounding this is the situation when either a stream of 0s or 1s bits occurs since these may be undifferentiated from gait attributed frequencies. To avoid this, we selected ID patterns that did not include identical bit sequences exceeding 3 bits. With a one million platforms target, we would need 23 bits in our code to get 20.

For demonstration purposes, we used an 8-bit parity sequence where each bit is the bit XOR of the corresponding bit derived from the 23-bit code sliced into three 8-bit words. We initially set the 24th bit to 0 in this calculation. Once completed, we set the 24th bit to the parity value of the 8-bit parity sequence itself. This allows us to perform a rudimentary check on the latter and allows us to detect small error counts. Of note, we violated the four identical bit rule for the 9-bit parity sequence, recognizing that this would potentially increase error rates. Consequently, the overall frame design consists of a synchronization header, the aforementioned ID field and a footer containing parity information.

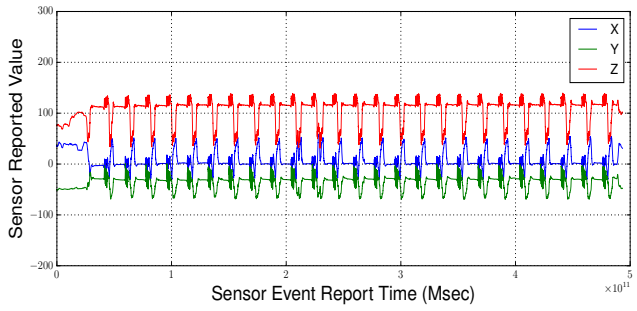
For synchronization, we adopted a spreading technique leveraging a Pseudo Noise (PN) sequence (MSEQ 15) in the header which represents a balance in achieving short synchronization lengths, signal gain and minimizing pattern duplication.

We could increase the frequency separation from the gait fundamental by limiting the number of contiguous identical bits to two. The number of such codewords follows a Fibonacci series with an n of 29 yielding a k of 20. These testing results are discussed in Section 5.2.5.

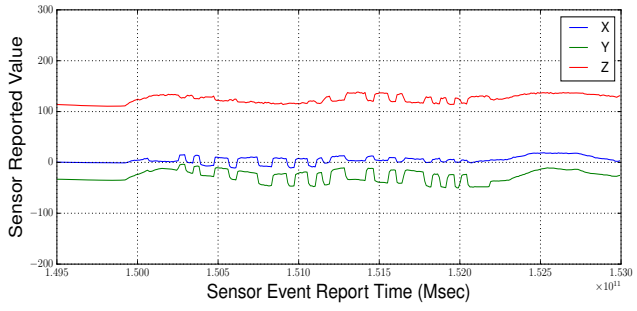
More aggressively, we could include error correction by changing the header to a Barker 7 code, utilize a Hamming [31, 26, 3] code correcting one bit, then break the 0/1 pattern by bit stuffing while including the two-bit limit. We leave the optimal coding scheme for a future study.

4.7 Signal Processing

Android smartphone sensors such as the accelerometer and gyroscope are intended to respond to motion while the magnetometer is intended to respond to orientation shifts relative to a magnetic reference position. These sensors may be sensitive to external non-motion driven stimuli such as ultrasonic signals in the cases of the accelerometer and gyroscope and in the case of the magnetometer, indigenous fields and external magnetic field manipulation. These, plus motion induced responses, are seen in Figure 5a and Figure 5b. The former illustrates all testing movement including the returns to the starting position while the latter shows the visible signal on the X and Y axes while the effect of the gait is visible predominately in the Z and to a lesser extent, the Y and X axes. This is expected as the distance off the platform plane varies within hip flexion and extension ranges while underway. From a signal strength view, the gait amplitude may reach twice that of the signal while its period exceeds the bit's pulsewidth. Figure 6 illustrates the process steps



(a) Dynamic Test - 25 Walks, Macro View Including Turns



(b) Signal, Code and Gait from Single Walk

Figure 5: Magnetic Fields, Galaxy S6

used to extract payload data. The sensor data is initially interpolated in increments of 1 msec since sensor reporting is non-uniform. In addition to the obvious sample rate differences, we found that among the LG, Nexus and ZETA devices, the Hardware Abstraction Layer reports a 'zero' post a scheduled sample. This behavior is observed in Figure 10 versus what is observed with the Galaxy S6, see Figure 5. We apply a concept of last reported value when this occurs in order to eliminate this condition. This condition is detected when the next sample changes by more than the mean signal value over the entire run. Moving average or equivalent filters are not suitable as they smooth the signal. Once completed, low frequency components sourced by the gait motion are identified by an FFT. These are used to set the filter cut-off frequencies which are typically below 2 Hz. A subsequent composite signal is generated and passed through an AGC process which compensates for signal strength variation due to differences in off-angle positions relative to the center of a coil. The AGC value at point s is shown in equation 13 where τ is the selected threshold, d_s is the post noise-cancelled value at s and ϵ_s is the energy at s.

$$AGC_s = f(d_s, \tau, \epsilon_s) \tag{13}$$

A synchronization preamble hunt occurs post AGC processing. Using a matched filter based on the MSEQ15 pattern, we slide the filter over the AGC output and correlate at each AGC point. Correlation is computed using Equation (14), where l is the encoding scheme length, $x[i]$ is the sensor measurement at i within l and $EE[i]$ is the encoding scheme's i^{th} code value within l, e.g., -1 or 1 for each chip as needed.

$$syncstart = |\sum_{i=1}^{l} (|x[i]|) \cdot EE[i]| \tag{14}$$

$$\hat{s} = \underset{s \in \{s_1, s_2, s_3, \ldots s_n\}}{\text{argmax}} \quad syncstart \tag{15}$$

$$D = \int_{i=t_s}^{t_e} AGC_i dt \tag{16}$$

$$Bits = \begin{cases} 1, & \text{if } D \geq \tau \\ 0 & \text{otherwise} \end{cases} \tag{17}$$

Once the start of the synchronization preamble $\hat{s}$ is determined, the preamble is stripped away and the payload is extracted. We apply discrimination processing in 16 and 17 where we integrate the AGC output over the interval t_s to t_e and apply the result against a threshold τ to get the bit value. Error processing is executed with ID error rates and bit error rates subsequently determined.

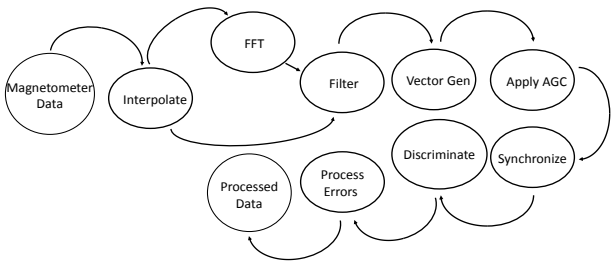


Figure 6: Signal Processing

5 TESTING AND EVALUATION APPROACH

We successfully obtained IRB approval for human-in-the-loop experiments, enabling the use of test assistants to transport the test devices from differing manufacturers in proximity to the magnetic field. These assistants encompassed three men and three women of varying heights, weights and walking gait patterns.

5.1 Testing Methodology

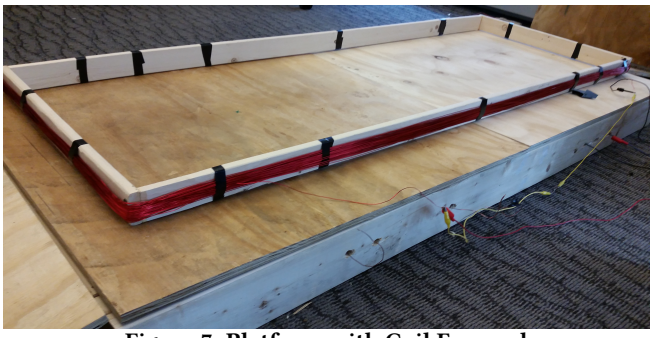


Figure 7: Platform with Coil Exposed

We deployed an app in each device that recorded the magnetometer readings in each of the X, Y and Z directions. Each assistant carried all devices simultaneously and were tested twice, once with a tool belt and once with a shoulder bag. Orientation was not explicitly controlled although in the case of the tool belt, the general orientation was vertical with the face pointing toward the participant's torso. With the shoulder bag, the general orientation was horizontal with the face pointed up. There was no intention for any axis to be precisely parallel or perpendicular to the platform surface. These positions were selected to reflect commonly used orientations.

After enabling sensor recording with the test app, each assistant walks over the platform, Figure 7, 25 times while carrying all of the devices concurrently. A new ID position code, Table 2, was transmitted for each pass, yielding a total of 25 unique codes per assistant per device per test. The same position code sequences were used for each test. Each walk pass consisted of a synchronous series of events. Initially, the assistant would wait for a fixed period of time (seconds) until visually cued with warning signals followed by a 'go' signal. The assistant would subsequently traverse the platform, return to the starting position and wait for the next series of cues. This sequence is more stressing than with a real deployment since the emissions would be triggered by a pressure switch / optical sensor such that emissions would occur while the victim was within the coil boundaries whereas in these tests, we relied on reaction time. After all walk passes were complete, the data was post processed to ascertain solution effectiveness.

We do not evaluate the effect of gender. Tests were performed on both sexes independent of vehicle. Our focus was to identify differences in performance with respect to noise where one noise contributor might be gender related gait.

5.1.1 Magnetic Field Characteristics. Magnetic field strength varies relative to position as devices move over the coil. Figure 8, illustrates the X,Y and Z readings of the measured field values at

Table 2: Data Pattern

Pattern #	Bit Pattern
0	00110111010001000100111100111101
1	00100010101001101010101000101110
2	00011011101010111001101100101010
3	00011000111010111001000001100011
4	10101000101011011100010111000001
5	11011001100100111011101011110000
6	11001001010011101101000101010111
7	01100011101000101001101101011011
8	11000111001011010101101110110000
9	01011000110011011101110101001001
10	11100010011100011010001100110001
11	01001010101000110001001111111011
12	11010100101100110111010100010011
13	10101010001101001011000000101110
14	10111011101101110101011001011010
15	10001100011100011010100001010101
16	01101001000100110110011100011100
17	10100111001010001010101100100101
18	11100011011011000111011011111001
19	11001101110001110010010000101110
20	10101011100011101000111110101011
21	00101010111011001100111000110111
22	11010100011010110110010011011011
23	10011001000101001000101100000111
24	00101110111001001001010101011110

16 inches above the center of coil moving from the edge closest to the starting position, 'Start' to the ending position, 'End'. Measurements were taken by sliding the device along the parallel plane while the coil is transmitting signals. Positions 1st Q, Mid and 2nd Q denote the midpoints of the first half, overall platform and second half of the platform respectively. The measuring device was parallel to the surface of the platform and rotated 90°. The Z position was flat with the face up. In general, the symmetry is clear with the worst-case max-to-min ratio approaches 3 : 1.

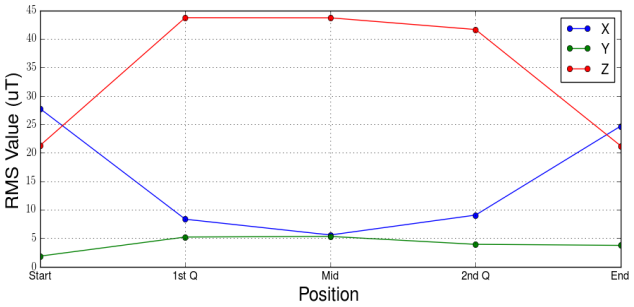


Figure 8: Axial Static Position Readings

5.2 Testing Results

This section describes our test results. Of the six devices evaluated, four produced satisfactory results. The two failures were the Samsung Galaxy S7 and the Nexbit Robin.

5.2.1 Sampling Rates. Device sample rates are provided in Table 3. Aliasing was not a concern except in the case of the Robin

where the standard deviation equaled the pulsewidth. Otherwise, the worst-case sample rates were greater than twice the 18.92 Hz signaling bit rate (45 msec pulsewidth).

Table 3: Sampling Rate Statistics (Msec)

Mfr.	Device Model	Mean	Max	Min	STD
LG	4	8.39	18.92	4.18	0.0724
ZTE	Blade V8 Pro	5.01	6.84	4.92	0.0143
Nexus	5	4.93	9.86	3.88	0.216
Samsung	S6	4.41	10.66	1.5	1.4217
Samsung	S7	4.73	6.23	4.62	0.0087
Nexbit	Robin	7.41	1009.8	4.92	45

5.2.2 Processing. We show in Figure 10, the magnetometer response for a given pass of the ZETA Pro device, with and without signaling. In the sequence times between 2000 and 8000 msec in Figure 10a, the straight-line periodicity of the gait is observable without signal emissions. The deviations after this range are test specific as the subjects were asked to return to the starting position. The presence of signal is shown in Figure 10b between 3000 and 5500 msec for a similar walk. Note that the latter imposes a minor amplitude deviation while underway and the signal rides on top of the ambient (including gait) readings.

The RZ signature is eliminated prior to interpolation which is followed by the removal of gate related components and the turns contributions as shown in Figure 11a using a multi-stage filtering scheme. The gait frequency spectrum for each DUT for a sample test assistant is provided in Figure 9. Although these frequencies are less than 5Hz, the content is more noticeable at lower frequencies.

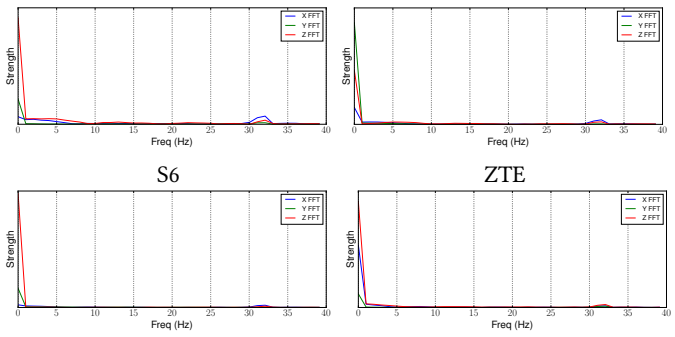
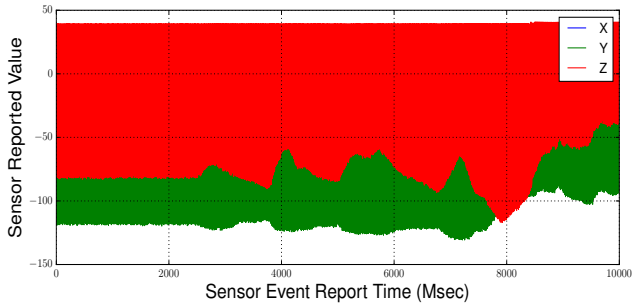
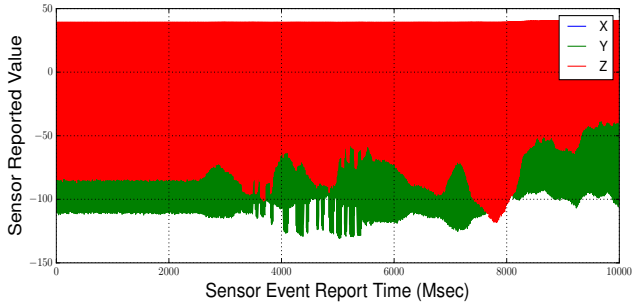


Figure 9: FFT - Low Frequency Content

We transpose the resultant tri-axial data, Figure 11a, into the composite signal, see Figure 11b in both Cartesian and Spherical coordinate systems from the measured values associated with Section 4.2 as vector $\mathbf{B}$, inclination $\arccos(\mathbf{B_z}/\mathbf{B})$, and azimuth $\arctan(\mathbf{B_y}/\mathbf{B_x})$, representations and select the output with the most fidelity prior to the application of AGC to create the final data. Since the orientation is neither controllable nor predictable and the axial sensor readings vary with orientation and position within the magnetic field, computing all three composite signals is needed. This is evident from Figure 5b where the Z axis has a strong gait and little signal, X and Y have severe and moderate edge attenuation respectively due to slow fading of the near-field channel and each exhibits asymmetrical yet opposing gait elements. Figure 11c illustrates an AGC output example superimposed on the composite signal.



(a) Signal-less Walk



(b) Walk with Signal

Figure 10: Single Walk Magnetometer Readings

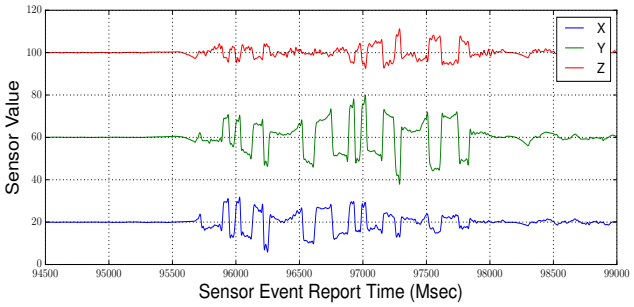
Table 4: Static Error Rate Summary

Mfr.	Device Model	BER
LG	4	1.67×10^{-3}
Nexus	5	6.25×10^{-3}
Samsung	S6	0
ZETA	Blade V8 Pro	1.67×10^{-3}

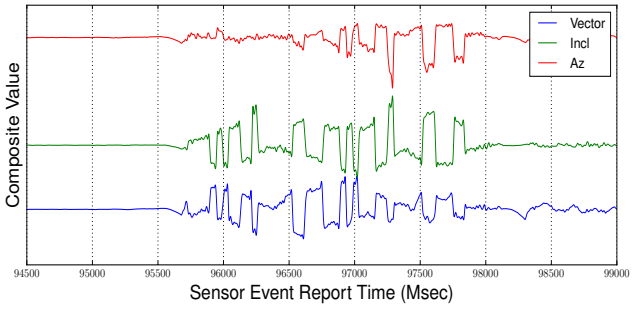
5.2.3 Stationary Testing. Table 4 summarizes device static error rates for a 4800-bit test. The worst-case error rate is 6.25×10^{-3}.

5.2.4 Walking Results. Table 5 summarizes the testing results. Columns IDE and BE indicate the number of errors for a given device with respect to the 25 possible IDs (IDE) and 800 bits (BE). The worst-case ID error rate is 9 out of 25 which occurred on only one device type. This suggests a good confidence level that we can determine the precise location of a device that is in range of our coil. The S6 and Zeta are the best performers where the worst-case correct identification rate between the two is 88%. The LG and Nexus follow with worst-case values of 72% and 64% respectively. Although gender breakout is intentionally hidden from the reader, the results appear inconclusive with respect to gender orientation and locomotion.

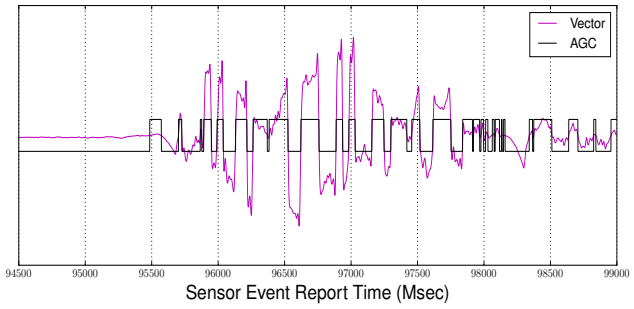
Initially, we thought that there might be a bias based on gender due to physical and traditional conveyance modality. Although the mean height for men moves device distances ≈ 5.5 inches further away from the surface of the platform, pocket book / shoulder bag use may offset this gap as the bottom of the book / bag is usually several inches above the iliac crest, which itself is estimated to be 2 inches above the location of a belt carried device. The use of high heels further reduces the gap. Second, a bag provides additional device tilt such that the data may show an increased contribution



(a) Gate Removed



(b) Composite Signals



(c) Automated Gain Control

Figure 11: Signal Processing Chain

from previously non-dominant axes. One might attempt to infer gender from axial data but once 'vectorized', the belt vs. bag results are indistinguishable. See Frimenko et.al, [9] for more information on gender gait differences.

In some cases, there are low IDEs with large BEs. These typically occur when synchronization fails. Some failures may be attributed to the testing scheme which is dependent on visual cues to initiate a walk. Any delays by the test assistant may cause a partial preamble loss due to emissions starting prior to acceptable proximity to the coils. In a true deployment which would rely on physical detection methods for presence within the anticipated field, proximity induced synchronization failures would be mitigated.

The results validate our approach to identifying location despite the presence of static environmental magnetic fields and system noise sources such as those associated with actively carrying the device. With one exception, the non-stationary error rates are an order of magnitude worse than the corresponding stationary ones. We have included two additional columns, single bit errors (SBE) and double bit errors, DBE where we track the occurrence of each

Table 5: Error Summary

Test Subject	Belt/Bag	Device	IDE	BE	SBE	DBE
A	Bag	LG-D41521	5	8	4	0
A	Bag	Nexus522	4	6	3	0
A	Bag	SM-G920T23	5	36	2	1
A	Bag	Z97823	1	1	1	0
A	Belt	LG-D41521	2	2	2	0
A	Belt	Nexus522	9	15	5	2
A	Belt	SM-G920T23	2	2	2	0
A	Belt	Z97823	0	0	0	0
B	Bag	LG-D41521	1	1	1	0
B	Bag	Nexus522	7	9	6	0
B	Bag	SM-G920T23	5	57	1	0
B	Bag	Z97823	1	1	1	0
B	Belt	LG-D41521	4	46	1	0
B	Belt	Nexus522	4	6	3	0
B	Belt	SM-G920T23	1	2	0	1
B	Belt	Z97823	0	0	0	0
C	Bag	LG-D41521	2	4	1	0
C	Bag	Nexus522	6	9	5	0
C	Bag	SM-G920T23	3	32	1	0
C	Bag	Z97823	0	0	0	0
C	Belt	LG-D41521	1	1	1	0
C	Belt	Nexus522	6	8	4	2
C	Belt	SM-G920T23	2	2	2	0
C	Belt	Z97823	2	2	2	0
D	Bag	LG-D41521	7	8	6	1
D	Bag	Nexus522	7	12	4	2
D	Bag	SM-G920T23	2	3	1	1
D	Bag	Z97823	1	2	0	1
D	Belt	LG-D41521	5	53	2	0
D	Belt	Nexus522	9	12	6	3
D	Belt	SM-G920T23	1	1	1	0
D	Belt	Z97823	0	0	0	0
E	Bag	LG-D41521	5	7	3	2
E	Bag	Nexus522	6	56	3	0
E	Bag	SM-G920T23	2	3	1	1
E	Bag	Z97823	0	0	0	0
E	Belt	LG-D41521	7	9	5	2
E	Belt	Nexus522	8	11	5	3
E	Belt	SM-G920T23	3	34	1	0
E	Belt	Z97823	2	2	2	0
F	Bag	LG-D41521	2	2	2	0
F	Bag	Nexus522	9	14	5	3
F	Bag	SM-G920T23	5	48	1	1
F	Bag	Z97823	0	0	0	0
F	Belt	LG-D41521	5	8	3	1
F	Belt	Nexus522	4	6	3	0
F	Belt	SM-G920T23	4	33	2	0
F	Belt	Z97823	0	0	0	0

for a given test. The ID success rate would exceed 94.8% if the coding scheme selected supported single bit error correction and 97% for double bit error correction.

Although the Galaxy S7's sample rates were well within our operational parameters, it appears that the issue is poor sensitivity as it did not exhibit the dynamic range seen in the four attack prone devices. At this juncture we are unable to identify the sensor part number to examine its specifications.

5.2.5 Contiguous Identical Bit Assessment. The above results reflect data patterns prohibiting four or more contiguous identical bits. Table 6 summarizes the results when reduced to two, providing greater separation from the gait fundamental frequency. The overall Bag result improves slightly versus the Belt which improves substantially. In the latter, errors are either non-existent or correctable with single bit correction schemes. We suspect that a belt offers greater structural coupling to the body vs. a bag which floats,

anchored at one spot and may be susceptible to other noise sources.

Table 6: Two Bit Limit Summary

Test Subject	Belt/Bag	Device	IDE	BE	SBE	DBE
B	Bag	LG-D41521	2	4	1	0
B	Bag	Nexus522	5	6	4	1
B	Bag	SM-G920T23	6	93	0	0
B	Bag	Z97823	0	0	0	0
B	Belt	LG-D41521	0	0	0	0
B	Belt	Nexus522	3	3	3	0
B	Belt	SM-G920T23	0	0	0	0
B	Belt	Z97823	0	0	0	0

6 MITIGATION

Since Wi-Fi, GPS, Bluetooth, cellular and NFC are assumed to be disabled, the attack surface is reduced to the magnetometer. In the current Android security framework, the user is not notified of magnetometer usage. As such, the practical mitigation strategy scope is limited, short of power cycling.

Other than removal of the magnetometer, sampling rate modification may provide the most effective mitigation scheme. The mean sampling rates for the magnetometer were in the 150 Hz range. Decreasing this rate still allows non-malicious functionality while limiting the magnetometer as a covert or side channel medium due to the effectively reduced Nyquist frequency. A less aggressive approach is to randomize the sampling rate which increases the ID and bit error rates in fixed length pulsewidths. To sustain this type of channel, the attacker would need to increase the pulsewidth, causing either a reduction in payload length or migrating to a larger physical footprint making the attack more challenging.

Adopting the overdamped scheme of analog compasses of the prior century is interesting. This provides low pass filtering, exhibits non-linear behavior and reduces the signal-to-noise ratio. What is compelling is the difficulty in envisioning the need for a critically / under damped sensor.

Another possibility is to eliminate the magnetometer altogether although some would suffer as no alternative is available. Those who can communicate with the GPS constellation might not need this feature. Placing the phone next to a permanent magnet would limit the magnetometer's ability to act as a receiver and unfortunately severely limit utility. A more practical solution is to reduce sensor sensitivity to approach 100μT/LSB or less rather than 1μT/LSB which significantly degrades magnetometer resolution while retaining functionality.

Attenuating magnetic fields is challenging as it is affected primarily by the shielding material. In a first order approximation from [1], the attenuation α equals $permeability \times (T_S/D_S)$ where T_S/D_S is the ratio of the shield thickness to the length of the diagonal sheet or diameter of the shield circle depending on geometries. Since the latter is less than one, the permeability of the material must be very high to provide effective shielding as is the case with materials such as ferromagnetic alloys containing high Nickel concentrations. Materials suitable for RFI shielding such as Aluminum are ineffective in magnetic shielding applications.

Monitoring sensor content is resource intensive. A defender could monitor frequencies between 5 Hz and 50 Hz in $\approx$ 2 second segments. However, mitigation in real-time is unlikely either in identifying the participating app or disconnecting all registered Listeners which is currently not a feature. Finally, querying the user for permission to use the sensor is an option albeit unlikely due to the lack of action taken historically when highlighted in prior works.

7 RELATED WORK

Jin [16], developed a file sharing scheme which used the magnetometer to reduce the probability of proximate Man in the Middle attacks and limit eavesdropping from prospective attackers. Static device EMF readings are exchanged as a seed for secure communications. The operating range is less than 20 cm, far less than needed in our attack and inappropriate for dynamically controlled signals.

In Jiang[15], the authors use Amplitude Shift Keying (ASK) encoding for the 'Pulse' application intended for near field communications. They use multiple coils and ASK yet this channel fails to operate at distances higher than 2 cm and stationary devices are assumed. Although the field strength is similar, ASK is challenging in our attack due to position driven non-linearity of coil emissions.

Son's [28] work demonstrated the effect of radiating acoustic energy at drones with power levels near 100 dBSPL, disrupting flight patterns by stimulating the gyroscope at its resonance frequency. In addition to the concern for the unprotected victim, additional power might be needed to penetrate clothing, leather pouches, pocketbooks etc. which offer significantly greater acoustic shielding at sensor resonant frequency(ies), making this attack implausible.

In Guri [12], data is transmitted via controlling a desktop computer's resources (i.e., memory bus) at GSM, UMTS and LTE frequencies which are received by a smartphone at a distance in the 1 to 5.5-meter range. This requires the use of cellular services which we must avoid due to its location tracking capability.

Other sensor inter-device communications were demonstrated by Farshteindiker [8] whose covert channel utilizes an 'implant' to transmit ultrasonic waveforms, stimulating a smartphone's gyroscope. Since the devices must be touching in a position-sensitive location to function, this application is impracticable.

Michalevsky et al. [21], developed PowerSpy which used power levels and Dynamic Time Warping to yield 80% user route inference accuracy. There are two issues with this approach. Since the attack requires a-priori, known road structures overlaid with surveyed power levels, the data collection is substantial. Most importantly, active cellular services are needed which is prohibited in our attack.

8 CONCLUSION

We demonstrated a zero permission, location identification attack of an Android device. By constructing a low power transmitter that emits GPS mapped location data, we leverage the magnetometer to bypass location privacy protection schemes. With motion compensation, we can determine location 86% of the time with a BER of 1.5% which is only ten times the stationary error rate. Future work includes improving our understanding of this attack's potential by including other devices, improving coil switching time for size reduction, experimentally evaluating suitable mitigation techniques and extending the data-collection using other modalities and transmitter configurations.

REFERENCES

[1] *How Do Magnetic Shields Work.* Technical Report. Magnetic Shield Corporation. http://www.magnetic-shield.com/pdf/how_do_magnetic_shields_work.pdf

[2] 2002. *Electric and Magnetic Fields Associated with the Use of Electric Power.* Technical Report. National Institute of Environmental Health Sciences,National Institutes of Health. https://www.niehs.nih.gov/health/materials/electric_and_magnetic_fields_associated_with_the_use_of_electric_power_questions_and_answers_english_508.pdf

[3] 2006. Anthropometric Data. (2006). https://multisite.eos.ncsu.edu/www-ergocenter-ncsu-edu/wp-content/uploads/sites/18/2016/06/Anthropometric-Detailed-Data-Tables.pdf

[4] 2017. Uber Ditches Tracking Feature After Concern Over Customer Privacy. (2017). http://fortune.com/2017/08/29/uber-app-privacy-location-data/

[5] Eoin Blackwell. 2018. Fitness App Strava Published 'Heat Map' Details About Secret Military Bases. (Jan 2018).

[6] Richard W Bohannon. 1997. Comfortable and maximum walking speed of adults aged 20 to 79 years: reference values and determinants. *Age and ageing* 26, 1 (1997), 15–19.

[7] Keith Collins. 2017. Google collects Android users' locations even when location services are disabled. (2017). https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled/

[8] Benyamin Farshteindiker, Nir Hasidim, Asaf Grosz, and Yossi Oren. 2016. How to Phone Home with Someone Else's Phone: Information Exfiltration Using Intentional Sound Noise on Gyroscopic Sensors. In *10th USENIX Workshop on Offensive Technologies (WOOT 16)*.

[9] Rebecca Frimenko, Cassie Whitehead, and Dustin Bruening. 2014. *Do Men and Women Walk Differently? A Review and Meta-Analysis of Sex Difference in Non-Pathological Gait Kinematics.* Technical Report. INFOSCITEX CORP DAYTON OH.

[10] Brandon Gozick, Kalyan Pathapati Subbu, Ram Dantu, and Tomyo Maeshiro. 2011. Magnetic Maps for Indoor Navigation. *IEEE Transactions on Instrumentation and Measurement* 60, 12 (2011), 3883 – 3891. https://doi.org/10.1109/TIM.2011.2147690

[11] Manuel Gunther, Laurent El Shafey, and Sebastien Marcel. 2017. 2d Face Recognition: an Experimental and Reproducible Research Survey.

[12] Mordechai Guri, Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, and Yuval Elovici. 2015. GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies. In *24th USENIX Security Symposium (USENIX Security 15)*. USENIX Association, Washington, D.C., 849–864. https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/guri

[13] W. C. Huffman and Richard A. Brualdi. 1998. *Handbook of Coding Theory.* Elsevier Science Inc., New York, NY, USA.

[14] K. Huguenin, I. Bilogrevic, J. S. Machado, S. Mihaila, R. Shokri, I. Dacosta, and J. P. Hubaux. 2018. A Predictive Model for User Motivation and Utility Implications of Privacy-Protection Mechanisms in Location Check-Ins. *IEEE Transactions on Mobile Computing* 17, 4 (2018).

[15] Weiwei Jiang, Denzil Ferreira, Jani Ylioja, Jorge Goncalves, and Vassilis Kostakos. 2014. Pulse: Low Bitrate Wireless Magnetic Communication for Smartphones. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '14)*. ACM, New York, NY, USA, 261–265. https://doi.org/10.1145/2632048.2632094

[16] R. Jin, L. Shi, K. Zeng, A. Pande, and P. Mohapatra. 2016. MagPairing: Pairing Smartphones in Close Proximity Using Magnetometers. *IEEE Transactions on Information Forensics and Security* 11, 6 (June 2016), 1306–1320. https://doi.org/10.1109/TIFS.2015.2505626

[17] M. N. S. Swamy Ke-Lin Du. 2010. *Wireless Communication Systems From RF Subsystems to 4G Enabling Technologies.* Cambridge University Press, New York, NY, USA.

[18] Eric Lichtblau. 2012. Police Are Using Phone Tracking as a Routine Tool. *The New York Times* (2012).

[19] Jennifer Lynch and Andrew Crocker. 2017. The Supreme Court Finally Takes on Law Enforcement Access to Cell Phone Location Data: 2017 in Review. (2017). https://www.eff.org/deeplinks/2017/12/2017-review-supreme-court-finally-takes-law-enforcement-access-cell-phone-location

[20] N. Matyunin, J. Szefer, S. Biedermann, and S. Katzenbeisser. 2016. Covert channels using mobile device's magnetic field sensors. In *2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC)*. 525–532. https://doi.org/10.1109/ASPDAC.2016.7428065

[21] Yan Michalevsky, Aaron Schulman, Gunaa Arumugam Veerapandian, Dan Boneh, and Gabi Nakibly. 2015. PowerSpy: Location Tracking Using Mobile Device Power Analysis. In *USENIX Security Symposium*, Jaeyeon Jung and Thorsten Holz (Eds.). USENIX Association, 785–800. http://dblp.uni-trier.de/db/conf/uss/uss2015.html#MichalevskySVBN15

[22] Christopher Mims. 2018. Your Location Data Is Being Sold—Often Without Your Knowledge. (Mar 2018). https://www.wsj.com/articles/your-location-data-is-being-soldoften-without-your-knowledge-1520168400

[23] A. Mosenia, X. Dai, P. Mittal, and N. Jha. 2018. PinMe: Tracking a Smartphone User around the World. *ArXiv e-prints* (Feb. 2018). arXiv:cs.CR/1802.01468

[24] S. Narain, T. D. Vo-Huu, K. Block, and G. Noubir. 2016. Inferring User Routes and Locations Using Zero-Permission Mobile Sensors. In *2016 IEEE Symposium on Security and Privacy (SP)*. 397–413. https://doi.org/10.1109/SP.2016.31

[25] A. M. Olteanu, K. Huguenin, R. Shokri, M. Humbert, and J. P. Hubaux. 2017. Quantifying Interdependent Privacy Risks with Location Data. *IEEE Transactions on Mobile Computing* 16, 3 (March 2017), 829–842. https://doi.org/10.1109/TMC.2016.2561281

[26] Raghavendra Ramachandra and Christoph Busch. 2017. Presentation Attack Detection Methods for Face Recognition Systems: A Comprehensive Survey. *ACM Comput. Surv.* 50, 1 (March 2017).

[27] Ashley Sefferman. 2016. Mobile Ratings: The Good, the Bad, and the Ugly. (2016). https://www.apptentive.com/blog/2016/06/23/mobile-ratings-good-bad-ugly/

[28] Yunmok Son, Hocheol Shin, Dongkwan Kim, Youngseok Park, Juhwan Noh, Kibum Choi, Jungwoo Choi, and Yongdae Kim. 2015. Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors. In *Proceedings of the 24th USENIX Conference on Security Symposium (SEC'15)*.

[29] Ping Xiong, Lefeng Zhang, and Tianqing Zhu. 2016. Semantic analysis in location privacy preserving. *Concurrency and Computation: Practice and Experience* 28, 6 (April 2016), 1884–1899.

[30] Sameh Zakhary and Abderrahim Benslimane. 2018. On location-privacy in opportunistic mobile networks, a survey. *Journal of Network and Computer Applications* 103 (2018), 157 – 170. https://doi.org/10.1016/j.jnca.2017.10.022

[31] Zhuangdi Zhu, Hao Pan, Yi-Chao Chen, Xiaoyu Ji, Fan Zhang, and Chuang-Wen You. 2016. MagAttack: remote app sensing with your phone. In *Proceedings of the 2016 ACM International Joint Conference on pervasive and ubiquitous computing (UbiComp '16)*. ACM, 241–244.

[32] K. Sh Zigangirov. 2004. *Theory of Code Division Multiple Access Communication.* Wiley-IEEE Press, USA and Canada.