VENTRILOCATION

BY

JUNFENG GUAN

THESIS

Submitted in partial fulfillment of the requirements
for ECE 499 in Electrical and Computer Engineering
in the Graduate College of the
University of Illinois at Urbana-Champaign, 2017

Urbana, Illinois

Adviser:

Professor Songbin Gong

Abstract

Mobile phones can locate users' location through multiple methods. Even though privacy-conscious users can disable location services such as GPS and Wi-Fi access points, they are not able to prevent the leakage of location information through cellular based positioning. In this paper, Ventrilocation is presented. It is an RF dongle that provides location-spoofing service for LTE-enabled devices while preserving full voice and data functionality. Specifically, it affects the raw data and results of a standard multilateration positioning method in LTE networks, known as observed time difference of arrival (OTDOA). OTDOA measures the difference between the arrival time of signals from different base stations to obtain the relative location of the user equipment (UE) to the base stations. Ventrilocation changes the time difference of arrival (TDOA) by introducing different delays to signals from different base stations. It consists of directional antennas to isolate signals and a circuit to delay the downlink signals. The surface acoustic wave (SAW) technology allows a chip-size delay line component to generate a significant amount of delay in the LTE frequency bands. The first prototype of Ventrilocation uses SAW delay lines with fixed delay, but with programmable SAW delay lines, the spoofed location can be designed to follow certain routes to achieve more reliable spoofing results.

Keywords

Privacy protections; Network-based localization; Location spoofer; Observed time difference of arrival (OTDOA)

Contents

1. Introduction 1

2. Literature Review 2

2.1 Positioning Techniques in LTE networks 2

2.1.1 Cell ID and Enhanced Cell ID 2

2.1.2 Assisted Global Navigation Satellite Systems (A-GNSS) 3

2.1.3 Observed Time Difference of Arrival 3

2.1.4 Our Problem 4

3. Description of Research Results 5

3.1 Approach 5

3.2 System Design 6

3.3 Circuit Schematic 6

3.3 Circuit Components 8

Directional Antenna 9

Surface Acoustic Wave (SAW) Delay Line 10

Low Noise Amplifier (LNA) 11

Duplexer 11

Balun 12

Theoretical performance 12

3.5 Printed Circuit Board (PCB) Layout 13

Impedance Matching 13

Ground 15

Bends 16

3.6 Printed Circuit Board (PCB) Fabrication 16

4. Evaluation 17

4.1 Circuit Preliminary Test 17

4.2 Circuit Performance Test 18

4.3 System Level Experiments 20

4.3.1 Antenna Directionality Test 20

4.3.2 Access OTDOA Result 21

4.3.3 Experiment Procedure 22

5. Result and Discussion 23

5.1 Problems 23

Directionality of Log Periodic Yagi Antenna 23

Multiple Positioning Methods 23

5.2 Possible Improvements 24

6. Conclusion 25

References 26

1. Introduction

Mobile phones have been providing people with unprecedented levels of connectivity. The invention and rapid popularization of smart phones along with the evolution of data networks have made mobile phones more powerful and essential in people's lives. However, for all of their advantages, cell phones are something of a double-edged sword. The invasion of privacy is one of the biggest problems, and a prominent example is user location. Mobile devices enable wireless service providers, app developers, and even third parties to track users' location at a fine scale over time, often without users' knowledge or consent.

Privacy-conscious mobile phone users can turn off common location services such as GPS, Bluetooth, and Wi-Fi, but they can hardly disable any cellular based positioning techniques. The core functionality of a mobile phone – the act of communication with base stations – measures and leaks the location information of the user equipment (UE) to the cellular companies. Therefore, to provide thorough protection of users' location privacy, one needs to fully understand and manage to interfere with the network-assisted positioning technologies.

2. Literature Review

The development of network-assisted positioning technologies has been driven significantly by the FCC's E911 mandate in the US, which requires the cellular networks to provide the location of emergency callers. In response to E911 and demands in commercial applications, second and third generation networks started to provide several positioning technologies. Current LTE networks also support a couple of standard positioning techniques.

2.1 Positioning Techniques in LTE networks

There are three independent handset-based positioning techniques in LTE networks. They are Assisted Global Navigation Satellite Systems (A-GNSS), Observed Time Difference of Arrival (OTDOA), and Enhanced Cell ID (ECID). The performance of these techniques varies in accuracy and Time to First Fix (TTFF). [1]

2.1.1 Cell ID and Enhanced Cell ID

Cell ID (CID) positioning estimates the position of the UE to be the position of the base station it is camped on. This technique generates location estimation very quickly but with very low accuracy. Based on CID, Enhanced Cell ID (ECID) also measures the round trip time (RTT) of cellular signals between the base station and the UE to estimate the distance to the UE. Also, the relative directional of the UE to the base station is also obtained using the angel of arrival (AoA). However, among all three LTE positioning techniques, ECID still has the worst accuracy because the angle of arrival can rarely be measured at high enough resolution.

2.1.2 Assisted Global Navigation Satellite Systems (A-GNSS)

Global Navigation Satellite Systems (GNSS) refers collectively to multiple satellite systems, such as GPS and GLONASS. The GNSS receiver in the mobile device receives satellite signals and computes its location. This technique can provide accurate 3-D position, but its TTFF is long. Assisted GNSS speeds up the position of GNSS by using wireless network data as assistance data. However, since A-GNSS uses satellite signals, it requires a good view of the sky and reception of satellite signals. Its performance is poor in dense urban settings.

2.1.3 Observed Time Difference of Arrival

Observed Time Difference of Arrival (OTDOA) is a downlink positioning method in LTE networks. It is a multilateration method in which the UE measures the time of arrival (TOA) of signals received from multiple base stations (eNodeB's). "The TOAs from several neighbor eNodeB's are subtracted from a TOA of a reference eBodeB to form observed time difference of arrivals. Geometrically, each time (or range) difference determines a hyperbola, and the point at which these hyperbolas intersect is the desired UE location." [2]

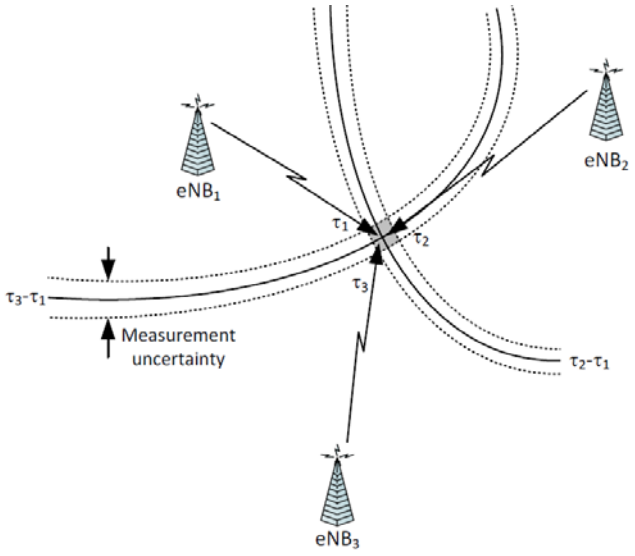

Figure 1 Multilateration in OTDOA positioning

2.1.4 Our Problem

Considering the specific requirement of good satellite signal reception for A-GNSS, and poor accuracy of ECID, we focus on spoofing the location measured by OTDOA technology. Because both OTDOA and ECID rely on the time of travel of cellular signals in positioning, it is possible that a spoofing system targeting OTDOA can also interfere with the ECID positioning results. However, when spoofing the location, it is necessary to preserve the quality of voice and data communication of the mobile phone.

3. Description of Research Results

3.1 Approach

Theoretically, to affect OTDOA, one can either change the raw signals for OTDOA positioning before the phone takes a measurement or edit the OTDOA results after the measurement. In the latter case, the observed time differences are computed by the baseband processor and retransmitted to the cellular network's location server---all without passing any information to the primary OS. Hence, any modifications of already-captured OTDOA measurements must take place in the baseband firmware. Although baseband firmware modifications are possible, they are difficult to execute; baseband firmware is closed-source and provided as a blob by the chipset manufacturer. Moreover, even if one were to modify the baseband firmware for one model of phone, the process would differ across phones with different chipsets. Another option is to modify the uplink measurements once they have been transmitted over the wireless channel. This is also difficult because of the encryption used on NAS signals; the spoofing device would have to effectively compromise the base station's ephemeral key. Hence, this approach is likely to pose significant challenges.

We avoid these problems by instead affecting the TOA of downlink signals before the measurements are taken by the UE. The idea is to add delay to the transmission line between the antenna of the UE and the baseband processor. Therefore, the internal antenna of the UE needs to be replaced by external antennas and the signal-delaying circuit. Besides, signals from different base stations are separated by directional antennas pointing to the target base stations, and then we selectively delay them by different amounts of time. By choosing these delays carefully, one can alter the output of OTDOA positioning algorithms to a user-specified location.

3.2 System Design

Ventrilocation consists of three functioning units: directional antennas, delay lines, and power combiner/splitter, as illustrated in Figure 2. First, we use directional antennas to isolate signals from different base stations. Second, we use an RF circuit to introduce different lengths of delay time to the isolated signals. Third, we recombine the delayed signals, and feed them into the device through its external antenna port. The same Ventrilocation hardware can be used to spoof the location of any mobile device operating in the target frequency bands.

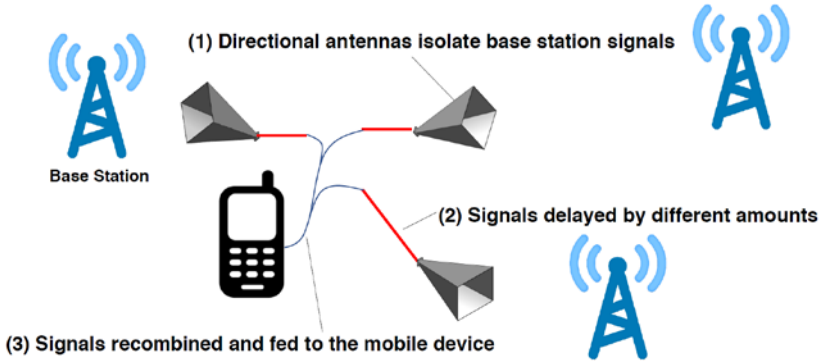

Figure 2 System overview of ventrilocation

3.3 Circuit Schematic

Figure 3 demonstrates the circuit schematic of our Ventrilocation prototype. This prototype supports three base stations, and the lengths of its delay are fixed, but it can be extended to support more base stations and programmable delay time.

The circuit contains three two-way branches connecting the directional antennas and the device's external antenna port. The directional antennas are labeled as "Antenna 1/2/3" in the diagram while the external antenna port is shown as "phone". Each branch has an uplink and a downlink shown in red and blue in the diagram, respectively. In LTE networks, frequency division

duplexing is very common. A circuit component called a duplexer allows uplink and downlink at different frequency bands to use the same antenna but keeps them isolated with minimum leakage. Since OTDOA measures the TOA of downlink PRS signals only, we implement delay lines, a component that delays the input signal without otherwise altering it, on the downlinks only. To make the delay time different for each branch, we keep the first downlink a simple microstrip transmission line but add one and two delay lines to the other two branches. Hence assuming the length of delay added by a single delay line component is 450 ns, the three downlinks should correspondingly have 0 ns, 450 ns, and 900 ns delay. Along with every delay line, we also cascade a low noise amplifier (LNA) to compensate the insertion loss. Moreover, a pair of power splitter and combiner are connected to the uplink and downlink ports of the duplexer at the phone external antenna port, so that the combined received signals are transmitted to the phone similar to the signal received by the internal omnidirectional antenna. Last but not least, since the input ports and output ports of the circuit components are a mix of balanced and single-ended (unbalanced) signals, baluns are required to convert between these two types of signals.

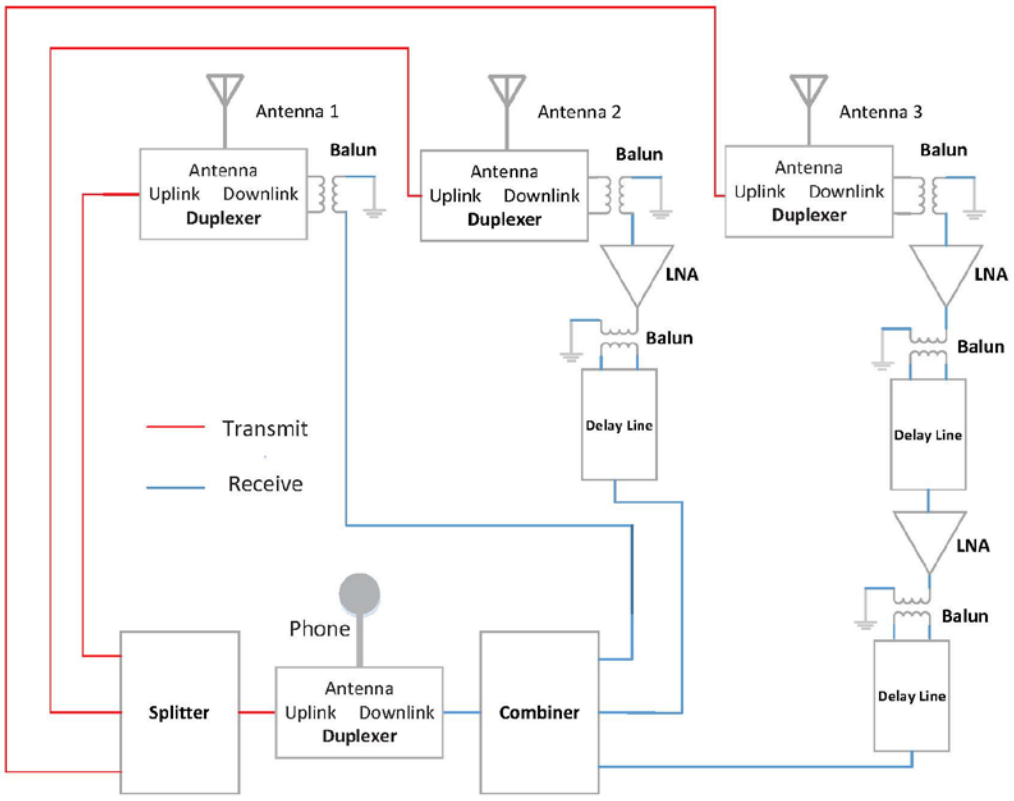

Figure 3 Circuit schematic

3.3 Circuit Components

We design the circuit for the T-Mobile LTE network with an LTE Band Number 4. This band has an Uplink frequency of 1710-1755 MHz and a Downlink frequency of 2110-2155 MHz. We chose this band to design and test the prototype because T-Mobile has the most base-stations in the Urbana-Champaign area. It is a relatively high-frequency LTE band, and at this frequency PCB design and fabrication are most challenging because of circuit parasitics. These operating frequency ranges determine the choices of circuit components and PCB layout.

Directional Antenna

Directional antennas are also of great importance in the Ventrilocation because the success of changing the difference in TOA depends on the complete isolation of signals from different base station. If an antenna receives signals from more than one base station with significant signal strength, these signals will be delayed by the same amount of time, so the difference of TOAs remains the same.

To achieve this isolation of signal, we use directional antennas that have significantly larger gain in one direction than in others. The antenna pattern of a Yagi antenna, a common directional antenna type, is shown in Figure 4. Considering signals from different antennas propagate from different directions, when we align every directional antenna toward a target base station, the signal from that base station will be received by the antenna with maximum gain. In contrast, signals from the other base stations experience minimum gain and can be ignored.

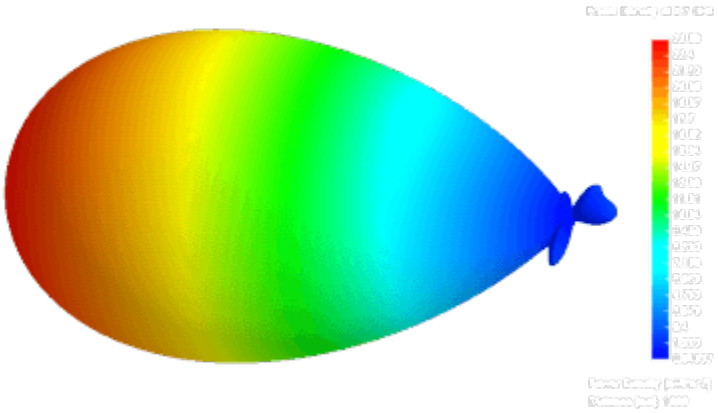

Figure 4 3D representation of the antenna pattern of a Yagi antenna having 8 elements including folded dipole fed with a power of 11 dBm [3]

In this prototype, the directional antenna we choose is a Wide-Band Log Periodic Yagi antenna TS221072 manufactured by Top Signal. Even though it does not have the narrowest beam, it covers the entire common LTE spectrum for 700 MHz to 2700 MHz. [4]

Surface Acoustic Wave (SAW) Delay Line

An ideal delay line for Ventrilocation figures long delay time and tunability, because the spoofing distance has an upper limit of:

$$Distance\ of\ spoofing \leq Delay\ time \times Speed\ of\ light$$

In other words, one μs delay time will lead to at most 300 m difference in OTDOA. Considering the high frequency of operation and long delay time, as well as the compatibility with other circuit components, we use surface acoustic wave (SAW) delay lines.

Surface acoustic waves (SAWs) are mechanical waves whose associated particle displacements are bounded to the surface. On piezoelectric substrates, SAWs can be transduced to and from electromagnetic waves through electrically connected interdigital transducers (IDTs). This property is referred to as the piezoelectric effect. An electrical microwave input signal at the transmitting IDT stimulates a microacoustic wave that propagates along the surface of the elastic solid body. Because of the low velocity of the acoustic waves, significant delay times can be achieved in a small chip with relatively low attenuation and wide bandwidths. Then at the output port, SAW propagates through another IDT and generates an electric charge distribution at the receiving IDT and an electromagnetic output signal [5].

Unfortunately, tunable SAW delay lines are rare while off the shelf tunable delay lines typically only add tens of nanoseconds of delay, so we choose a static SAW delay line module, TriQuint 856649, which has an absolute delay of 450 ns at the cost of 27 dB insertion loss. This module has balanced input ports with 100 Ω port impedance and a single-ended output port [6].

Low Noise Amplifier (LNA)

In addition to the amplifier gain, the noise level is the most important concern when amplifying the received signal on the downlink because the increase of noise level will decrease the signal-to-noise ratio and degrade the communication channel. The noise level of an amplifier is the amplified noise level at the input port plus the additional noise in the amplifier. The low-noise amplifiers (LNAs) are designed to minimize additional noise so that they amplify very low-power signals without significantly degrading the SNR. In this work, we use Mini-Circuits TAMP-242GLN+ LNA with a gain of 30 dB, whose noise figure is only 0.85 dB [7]. For the same reason, we cascade the LNA and delay lines in a way that the input signals are amplified first by the LNA and then they go through the delay line because in this way the SNR is greater than that of the other cascading sequence.

Duplexer

The duplexer is an essential part in RF transceivers. It is a three-port network that allows the transmitter and receiver to use the same antenna but at two different frequency ranges. The RX port outputs the received signal to the downlink while the TX port inputs the uplink signal to the antenna for transmitting. An ideal duplexer has low insertion loss in both TX-Antenna path and Antenna-RX path. Besides, it also isolates the TX and RX ports to prevent undesirable leakage. In our circuit, we use TDK SAW Duplexer B7959 that operates in W-CDMA Band 4 as wanted. The balanced RX port also has a port impedance of 100 Ω [8].

Balun

The circuit components we pick have either single-ended or balance ports, so baluns are required to convert between these two types of signals as well as to transform impedances. We use Mini-Circuits TCM2-43X+ RF transformer, which operates in a frequency range from 10 MHz to 4 GHz. It also has 50 Ω and 100 Ω port impedance on unbalanced and balanced ports respectively [9].

Theoretical performance

Table 1 shows the features important circuit components. Tables 2 shows the theoretical insertion loss in three downlinks and uplinks as well as the delay time of downlinks.

Table 1 Circuit component properties

Component	Part Number	Operating Frequency (GHz)	Input/Output Port Type	Insertion loss/Gain (dB)
Duplexer(TX)	B7959	1.71-1.755	Single-ended/Single-ended	-1.6
Duplexer(RX)	B7959	2.11-2.155	Single-ended/ Balanced	-2
LNA	TAMP-242 GLN+	1.99-2.20	Single-ended/Single-ended	30
Delay Line	856649	2.11-2.17	Balanced/Single-ended	-27
Combiner/Splitter	SCN-3-28+	2.20-2.20	Single-ended/Single-ended	-5.66~-5.48
Balun	TCM2-43X+	0.01-4.00	Balanced↔Single-ended	-1.3

Table 2 Theoretical downlink and uplink performances

Downlink	Insertion Loss	Delay	Uplink	Insertion Loss
Ant 1 - Phone	12.1 dB	0 ns	Phone – Ant 1	8.7 dB
Ant 2 – Phone	9.55 dB	450 ns	Phone – Ant 2	8.85 dB
Ant 3 - Phone	6.7 dB	900 ns	Phone – Ant 3	8.7 dB

3.5 Printed Circuit Board (PCB) Layout

At a frequency as high as 2.1 GHz, the electromagnetic wavelength is comparable to the physical dimension of the circuit. Hence problems like impedance matching and parasitic capacitance need to be taken into account.

Impedance Matching

In RF systems, impedance matching is essential to reduce return loss.

$$\Gamma = \frac{Z_L - Z_S}{Z_L + Z_S}$$

In all of the circuit components, the single-ended ports have an impedance of 50 Ω, while all the balanced ports have an impedance of 100 Ω. Therefore, the widths of the microstrip lines should be specifically designed so that their characteristic impedances match those of the ports. In this work, we use a 20-mil thick RO4350B substrate for its bigger dielectric constant so that microstrip line widths are thin enough to connect to the footprint of the surface-mounted components.

With the help of LineCalc function in ADS, we can find the right widths of microstrip lines with a characteristic impedance of 50 Ω and 100 Ω, which are 43 mil and 10 mil respectively.

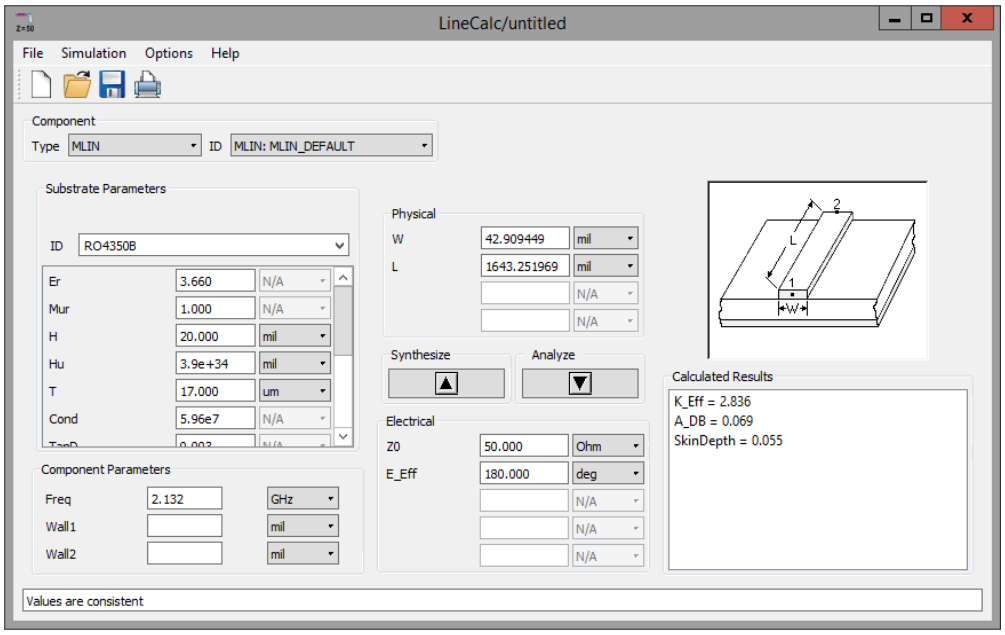

Figure 5 ADS LineCalc result example for impedance matching

Table 3 Microstrip widths for impedance matching

Frequency (GHz)	50 Ω	100 Ω
1.7325	42.9 mil	10 mil
2.1325	42.9 mil	10 mil

Because of the size of the contact pins of some circuit components. Discontinuity of microstrip line width cannot be avoided at some places on the circuit. To minimize the return loss caused by the discontinuity, we design multi-section impedance matching circuits.

Ground

There are two major considerations of the grounding of the surface-mounted components. For most passive devices, anything but the LNA, it is desired to minimize the area of the top layer copper, so the ground pins are connected to the bottom layer copper through vias. In this way, the parasitic capacitance is minimized. Also in order to obtain a uniform ground plane, we implement multiple vias spread symmetrically on every ground plane. In contrast, for the only active device, LNA, it is necessary to have one large top layer ground plane for better heat dissipation. Again, a number of vias are spread all over the ground plane for the same reason. In general, the top layer ground planes and vias are designed to imitate the evaluation board layout provided by the vendor for minimum parasitic effects.

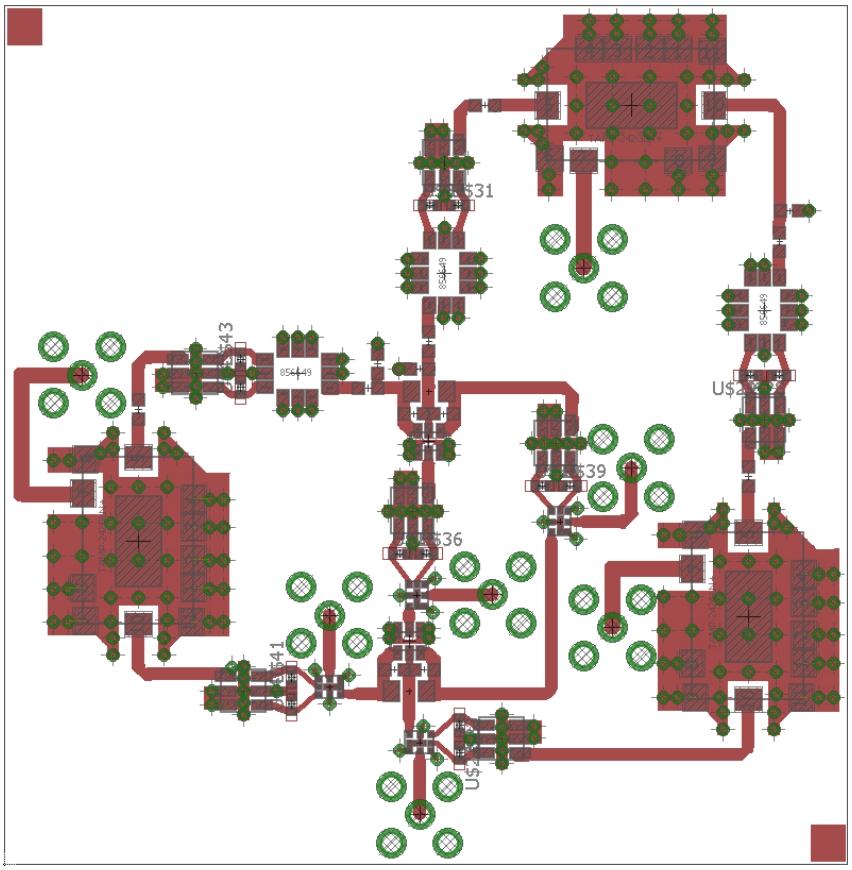

Figure 6 PCB layout in Eagle

Bends

Because of the discontinuity in microstrip line width where the transmission line meanders, the line characteristic impedance changes and causes reflections. We replace ninety degree bends by mitered bends to chop off some capacitance and keep the characteristic impedance constant.

3.6 Printed Circuit Board (PCB) Fabrication

PCBs for preliminary tests and prototypes are fabricated in house using LPKF ProtoMat S103 milling machine. However, this milling machine is unable to make vias, so short-cut copper wires are soldered through the holes. These low-quality vias are unable to provide ideal grounding on the top layer, and this problem may degrade the circuit performance.

Figure 7 LPKF ProtoMat S103 [10]

4. Evaluation

Our evaluation of Ventrilocation prototype consists of circuit preliminary test, circuit performance test, and system level field test. By gradually increasing the complexity of the package under test, we manage to detect and eliminate problems such as impedance mismatch and parasitic capacitance in the PCB layout. The circuit level tests are conducted by measuring the S-parameters of the device under test (DUT) with a vector network analyzer (VNA).

S-parameters, also known as scattering parameters, describe the response of an N-port network to signals incident to any or all of the ports. The magnitude of S-parameters suggests the insertion loss of signal transmission from one port to another, as well as the reflection loss of the ports. The phase of S-parameters can be used to obtain the group delay of the signal through a transmission line. S-parameters are also imported to the Advanced Design System (ADS) to simulate the frequency response of a larger network.

The system level experiments have an ultimate goal to find the OTDOA algorithm that measures a spoofed location while preserving voice and data communication.

4.1 Circuit Preliminary Test

In the basic preliminary tests, evaluation boards are fabricated with the same layout, and matching networks appear in the circuit prototype. We first measured the S-parameters of every circuit component as well as the transmission line and mitered bends. We focused on the reflection loss at all ports to detect and minimize any impedance mismatches that cause reflections. After that, we examined the insertion loss of passive components and the gain of the LNA to make sure the insertion losses, isolations, and gains are similar to those provided by the vendor.

From the single component tests, we confirmed that the insertion losses and isolations of the duplexers, combiners/splitters, and baluns are comparable to the reference values. However, the insertion losses of the delay lines are about 7 dB higher which may due to a non-ideal matching network. Besides, gains of the LNAs are also about 3 dB lower because of the imperfect vias. These errors together lead to an expected higher insertion loss of the delay line-LNA package.

Later on, two or more components were cascaded into packages and measured. For example, the delay line-balun combination was tested to examine the impedance matching for the balanced ports.

4.2 Circuit Performance Test

When the PCB layout was optimized through a series of preliminary tests, a thorough circuit performance measurement was conducted. In this test, we focused on return loss at every port and the insertion loss in every link in the frequency domain. We also measured the group delay of the downlinks in the time domain. The measurement results are shown in Figure 9 and Figure 10.

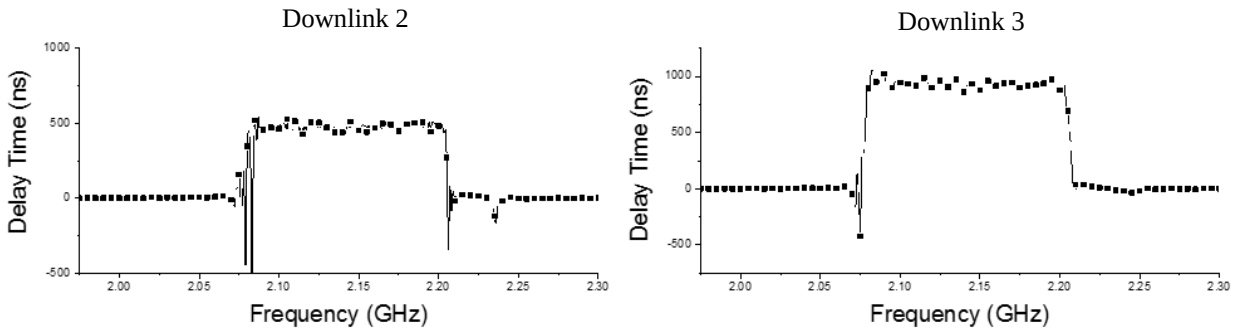

Figure 9 Downlink group delay

In Figure 9 we can see that the group delay of Downlink-2 is about 450 ns while that of Downlink-3 is about 900 ns. Therefore, we are confident to say the time domain response of the circuit matches the expectation.

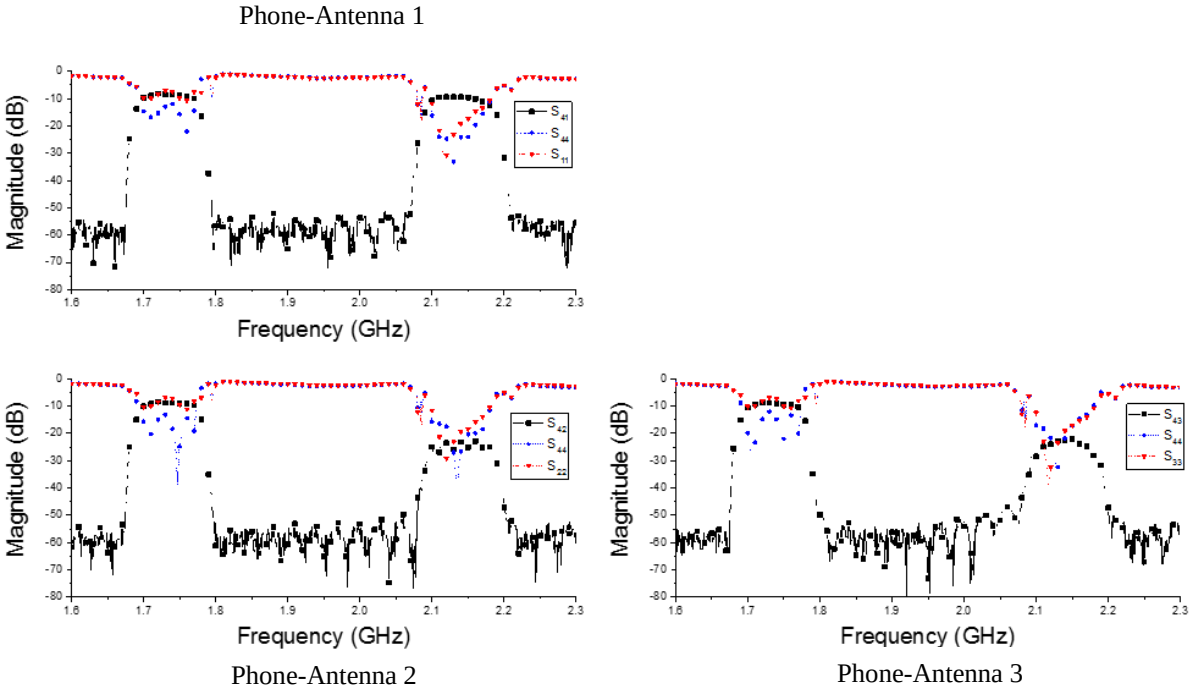

Figure 10 Circuit frequency response

However, the frequency domain response is not as ideal. Although all three uplinks have about 9.2 dB insertion loss which is slightly over the theoretical value, the insertion losses on Downlink-2 and Downlink-3 are significantly higher because of the uncompensated insertion loss of the delay lines. Downlink-2 has an insertion loss of 19.12 dB while that of Downlink-3 is 26.9 dB.

Even though the impedance matching of the delay line can be improved to decrease the insertion loss, higher loss on downlink that has longer delay time matches the actual signal property in the wireless network. The wireless channel communicating with a farther base station has a longer

delay and more attenuation in the atmosphere. As long as the signal strength is acceptable and the right amount of delay time is added, the location spoofing function of this circuit should be complete. Besides, since the mobile phone only communicates with the base station with the highest signal strength and shortest delay time, the voice and data communication will not be affected by the insertion loss on the delayed downlinks.

Therefore, the circuit performance test has successfully demonstrated desired functions of the PCB, and the prototype can be assembled and tested systematically.

4.3 System Level Experiments

4.3.1 Antenna Directionality Test

Before the system is assembled and the location measured, we test the isolation of signals from different base stations by the directional antennas. Once the location of the system is determined, we can look up a cell tower map as shown in Figure 11 on https://www.cellmapper.net/map [11] and estimate the alignment of antennas to maximize the gain of every antenna to the direction of a base station. Then we disable the internal antenna on the phone and connect a directional antenna to the external antenna port of the phone. With the help of apps like “Network Cell Info Lite” [12], we read the Cell ID or eNB ID of the base station the phone is communicating with and the signal strength.

When antennas with different point direction are communicating with different base stations with optimized signal strength, we are confident to assume that in every downlink, the signal from the target base station is much stronger than those from the other base stations.

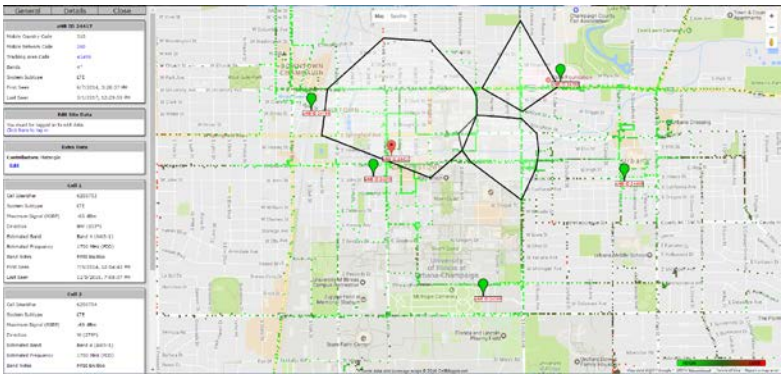

Figure 11 Cell tower map of Urbana-Champaign area [11]

Figure 12 Network Cell Info Lite App [12]

4.3.2 Access OTDOA Result

To observe the prototype successfully spoofing the location measured and sent to the wireless service provider, we need to first get the access to the location information. Even though the OTDOA results are not provided to the users, nor could we hack into the firmware, T-Mobile has a service called “FamilyWhere” [13] that helps users locate their family members’ devices using T-Mobile network. We tried to locate the phone when GPS, Wi-Fi, and Bluetooth are all disabled, but this app can still precisely locate the phone’s location with a range of uncertainty of 15 yards. Hence, it is reasonable to assume that “FamilyWhere” uses cellular network data. When this app locates mobile phones in the LTE network, it should use OTDOA technique to locate the UEs.

4.3.3 Experiment Procedure

We tested the system prototype in the following steps:

(1) Measure the location of the phone with “FamilyWhere” as a reference.

(2) Disable GPS, WiFi, and Bluetooth functions of the phone.

(3) Disable the phone’s internal antenna by wrapping the phone with aluminum foil.

(4) Align directional antennas.

(5) Connect antennas, circuit, and the external antenna port on the phone.

(6) Bias the LNAs on the PCB.

(7) Measure the location of the phone with “FamilyWhere”

(8) Switch the downlink that connected to each antenna and repeat the measurement.

(9) Test the voice communication quality and data rate.

The system setup is shown in Figure 13.

Figure 13 System level experiment setup

5. Result and Discussion

Ventrilocation prototype has been tested in two locations. However, unfortunately, with ventrilocation connected to the phone, the positioning results of FamilyWhere were still quite accurate, but the range of uncertainty increased from 15 yards to over 100 yards. We are analyzing the sources of error and trying to fix the problem.

5.1 Problems

Directionality of Log Periodic Yagi Antenna

The directionality of the antennas could be the biggest problem. Because if the side lobes of the direction antenna pick up signals from base stations other than the targeted one, the same amount of delay will be introduced to these signals, and as a result, the difference of TOA will not change.

Multiple Positioning Methods

Considering LTE networks collectively use three independent position technologies to locate the UEs, it is possible that the localization results of FamilyWhere are not equal to the OTDOA measurements. Besides, the distribution of cell towers in Urbana-Champaign area is very sparse so that techniques other than multilateral positioning are utilized in this region.

5.2 Possible Improvements

Further improvements of Ventrilocation are necessary to make its location spoofing performance more appealing to users. For example, a programmable trace of travel can prevent stokers detecting suspicious results of positioning. Besides, smaller antenna power source sizes are also required to make Ventrilocation portable with mobile phones. Last but not least, a longer delay time that does not degrade voice and data communication will enlarge the range of location spoofing.

6. Conclusion

Cellular based localization technologies are so powerful that to completely spoof the UEs' location requires interference with multiple positioning methods. Ventrilocation has shown its potential but more investigation and trouble shooting are necessary to make it a reliable solution to protect the location privacy of mobile phone users in the LTE networks.

References

[1] *An Overview of LTE Positioning*, SPIRENT, 2012.

[2] S. Fischer, *Assisted Global Navigation Satellite Systems (A-GNSS)*, Qualcomm Technologies, Inc., 2014.

[3] http://www.radartutorial.eu/06.antennas/Yagi%20Antenna.en.html

[4] http://www.wpsantennas.com/TS221072-Top-Signal-700MHz-2700MHz-Wide-Band-Log-Periodic.aspx

[5] L. Reindl, C. Ruppel, *Surface Acoustic Wave Delay Lines*, John Wiley & Sons, Inc., 2005.

[6] *B856649 2140 MHz SAW Delay Line Data Sheet*, TriQuint Semiconductor, 2007.

[7] *TAMP-242GLN+ Low Noise Amplifier Data Sheet*, Mini-Circuits

[8] *B7959 SAW Wireless LAN/Bluetooth Filter Data Sheet, TDK*

[9] *TCM2-43X+ RF Transformer Data Sheet*, Mini-Circuit

[10] http://www.lpkf.com/products/rapid-pcb-prototyping/circuit-board-plotter/protomat-s103.htm.

[11] https://www.cellmapper.net/map

[12] Network Cell Info Lite App, https://play.google.com/store/apps/details?id=com.wilysis.cellinfolite&hl=en

[13] T-Mobile FamilyWhere App, https://support.t-mobile.com/docs/DOC-4258