Provider Side Cell Phone Forensics

Terrence P. O'Connor

Abstract- **An investigation was conducted into the behavior of particular cell phone towers and their respective directional antennas to determine the areas of coverage of each tower's directional antenna at the request of the Washington County, Indiana prosecutor. The areas of coverage were determined by the analysis of each of the towers and their antennas as to the center of each antenna's field, the azimuth pattern of the directional antennas, the surrounding terrain and the percentage usage of the antenna at times of particular concern. Further, a series of approximately 50 test calls were placed at various locations to determine by measurement the antennas' patterns. The Call Detail Records (CDR) of the test calls were attained by subpoena by the Indiana State Police. The CDRs contained the information to determine which tower and antenna each call was received on. The results of this data was compared to calls placed by the defendant to ascertain what area the call was placed from and therefore determine what area the defendant was located while placing that call. This information was analyzed and presented on behalf of the Washington County prosecutor in a criminal proceeding in March of 2007.**

Index Terms – **Call detail records, CDR, Cell phones, cell phone forensics.**

I. Introduction

TECHNOLOGY is already being used to furnish valuable information to law enforcement in numerous ways. Obtaining the Call Detail Records is one of the means by which an examiner can obtain useful information concerning cell phone calls placed by the user. This paper describes a method used to analyze the Call Detail Records (CDRs) of the cell phone company and compare those records to the results of a series of test calls. The CDRs contain information that can be used to determine the area from which a call was placed. Since the Cellular Telecommunications & Internet Association estimated that there were 233 million U.S. cell phone subscribers at year-end 2006 this use will almost certainly become very common in the near future [1].

As a cell phone call is placed it is received on one particular antenna on an individual tower. Each cell tower typically contains three directional antennas [2]. A directional antenna receives signals with much greater intensity in the direction which it is pointing and discriminates against the received signal strength in directions outside of its field. The three directional antennas on the cell tower nominally divide the 360 degree circumference around the tower into three 120 degree areas, one area for each antenna. Commonly a cell tower will have the first of the three antennas centered on due North or 0 degrees. This antenna has a nominal area 120 degrees wide which is 60 degrees each side of due north. This antenna's nominal field is from 300 degrees (-60 degrees) to 60 degrees and is called either the north facing antenna or the Alpha antenna. The second antenna is centered at 120 degrees and has a nominal coverage area from 60 degrees to 180 degrees, this antenna is referred to as the southeast facing antenna or the Beta antenna. The third antenna nominally covers the remaining area of the field; it is centered on 240 degrees and nominally covers from 180 degrees to 300 degrees, this antenna is called either the southwest facing antenna or the gamma antenna. A top view of a typical cell tower and its antennas is shown in Fig. 1.

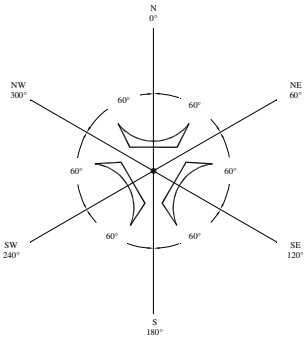

Fig. 1. Typical Cell Tower and Antennas

The tower and antenna which receives the call is determined by which antenna is receiving the signal from the mobile unit the strongest provided that tower is not already overloaded with calls. When a tower is in a period of very high use it may switch the incoming call to an alternate tower and antenna provided that the mobile unit is in the alternate antenna's field and therefore being received in adequate strength. The area of origin of a call placed by a cell phone can be determined by analysis of the cell towers, their respective directional antennas and by the analysis of the hourly usage data for each of the towers salient to the investigation.

II. The Procedure

The region of interest and particular locations of interest must be determined. In the particular case described in this paper, the region was the cities of Austin and Scottsburg, the area between the two and the rural area west of Austin on State Road 256. There were additionally ten particular locations of interest which included the several locations the defendant claimed to have been the night that the crime occurred and also the location at which the crime was believed to have been committed.

A cell phone was obtained that was serviced by the same provider as the defendant's cell phone. This cell phone was used to place a series of calls. The locations for each of the calls was determined in advance and marked on computer mapping software which showed the latitude/longitude reading of the location. Approximately 85% of the locations selected were at cross roads, the remaining were at landmarks such as a bridge or a storefront. A handheld GPS unit was used to drive from one location to another to speed up the process of finding the locations in unfamiliar territory. Furthermore the GPS receiver was useful in confirming that the location intended had indeed been arrived upon. This was useful because the roads were unfamiliar to the author and the some of the roads were marked by names rather than by their assigned county road number.

As a call was placed the time on the cell phone used was recorded manually in a paper log as was the number that was called. Each call made was alternately placed to a time/temperature service or to the cell phone of the state police detective driving the vehicle. On conclusion of placing the calls a subpoena was issued by the state police for the call detail records of the phone used. The CDR showed the time the call was initiated, the tower the call was received on and the antenna on which that call was received. Additionally, the tower and antenna on which the call was transceiving upon termination was also indicated. An example of a partial call detail record is shown in table 1. Parts of the record were omitted for space considerations.

DLD_DGT_NO	(812)738-6483
SZR_DT_TM	8/25/06 10:27
SZR_DURTN_CNT	14
INIT_CELL_NO	19
INIT_CELL_19FACE_NO	Southwest
FINL_CELL_NO	19

Table 1: Transcribed portion of a Call Data Record (CDR)

When the CDR was returned from the provider each call was identified by the time stamp of when the call was initiated. This time stamp was then used to plot the location from where the call was placed on the mapping software. Each of the antennas had a mapping icon assigned to it. For example, the north facing antenna on tower 148 was assigned a red 'X' and the southwest facing antenna of tower 148 was assigned a red flag and so on. The sixty-five test calls were received on five different antennas, each antenna was assigned an icon. The icon assigned for each tower-antenna is shown in table 2.

Tower-antenna	**Icon**
Tower 148 North	Red Star
Tower 148 Southwest	Red Flag
Tower 19 Southeast	Green Star
Tower 19 Southwest	Blue Pin
Tower 134 Southeast	Yellow Box

Table 2: Icon assignment for tower-antenna pair

Each call was then marked by its appropriate icon on a map of the area of interest. The basic map with the towers and each call marked by an icon is shown in Fig. 2.

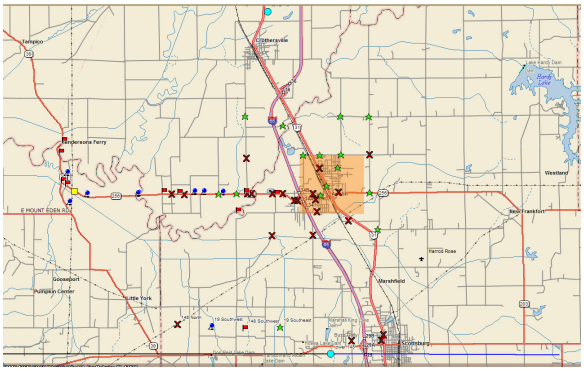

Fig. 2. Map of area of interest with icons

Further technical information was obtained from the cell phone provider by subpoena. It was necessary to obtain a statement as to the operating status of the towers and antennas in question both on the days the defendant placed the mobile calls of interest and the day that the author placed the test calls. It was considered critical that towers and antennas be checked for correct operation. Additionally the reports of cell usage, ineffective attempt and dropped call percentage were requested and supplied both on a daily and hourly basis for the days in question that the defendant used his phone and the date the test calls were placed. It was deemed important that the operating conditions of the towers be the same for the days of the test as the days in question. Also, the specifications of the cell tower's antennas were requested and supplied by the provider.

Each antenna nominally covers 120 degrees of the circumference, but each antenna crosses over into the adjacent antenna's field because the signal strength of received call would be nearly equal to the two antennas. This area of cross over is not instantaneous, but is rather a 40 degree wide area shared by the two antennas. For example, if a mobile phone were to move around the circumference of the circle around a cell tower starting at zero degrees and moving clockwise, as it approached 60 degrees there would be the expected switch from the north facing antenna to the southeast facing antenna. This change between antennas may occur as early as approximately 40 degrees and as late as approximately 80 degrees as each antenna crosses over into the adjoining antenna's field by approximately 20 degrees. This is due to the received signal strength being nearly equal in each antenna. The 20 degrees of crossover is an approximation derived from the measurements made on the test calls and analysis of the azimuth field specifications for the antennas used on the cell towers. An illustration of the shared fields between each antenna is shown in Fig. 3 below.

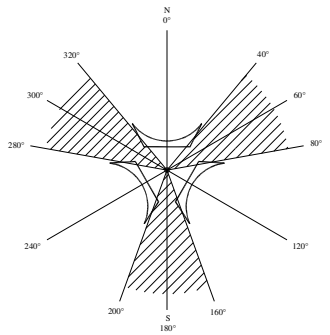

Fig. 3. Shared areas of antenna fields shown in cross-hatch pattern

An inquiry of the cell phone provider indicated that the antennas were not centered on 0, 120, and 240 degrees as described above. Based on where the largest population density in the area is located, the antennas will frequently be rotated to put the most populated area near the center of one of the antennas' fields. This is the case with the towers in this study; each tower has its antennas rotated 30 degrees toward the east so that the alpha antenna is centered on 30 degrees rather than 0, the beta antenna is centered on 150 rather than 120 and the gamma antenna is centered on 270 rather than 240. Fig. 4 illustrates each antenna's nominal field (without crossover). This information is critical and cannot be omitted to ensure an accurate analysis.

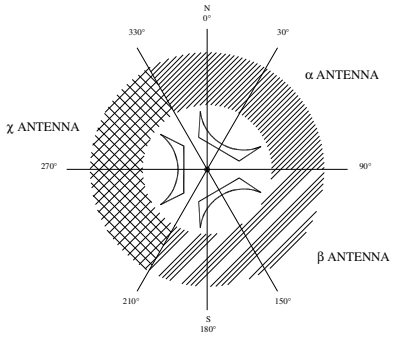

Fig. 4. Nominal fields of each antenna as actually situated with 30 degree rotation

The Washington County Prosecutor had a particular interest in one call that was placed this call was received and terminated on tower 19's southwest antenna. Any call received on a given tower-antenna must be in that antenna's field, there is no exception to this. Therefore it was important to indicate the area which tower 19 southwest covered. Cell phone towers in rural areas such as these in this study will have a much greater signal radius than those in urban areas. An urban area tower would have a signal radius close to two miles. In rural areas the nominal signal radius is approximately nine miles as is the case here. A call being received on tower 19 southwest antenna can fall into the antenna's main field which is 120 degrees wide or it can also fall into the crossover fields where the southwest antenna crosses over into the adjoining field of the north facing antenna and into the field of the southeast facing antenna. This would make the entire area of the southwest facing antenna 160 degrees wide. The area of that 160 degree wide pattern with a radius of nine miles is calculated as follows:

$$A = \Pi r^2 \frac{160}{360} \quad (1)$$

Area of 160 degrees of a circle

$$A = \Pi 9^2 \frac{160}{360} = 113.097 \text{ square miles}$$

Area of 160 degrees of a circle with a nine mile radius

It can be stated conclusively that any call received on tower 19 southwest facing antenna was placed from somewhere within that antenna's field. This statement is true for any call received on any given antenna; if the call was received on any given antenna the call was placed from somewhere in that antenna's field. The size of the antenna's field cannot be determined to exact dimensions, the radius of the tower is estimated and in a rural application such as this one the radius might extend to 12 miles which is generally considered maximum range for a mobile phone to its receiving antenna. Usually the range of the tower will be considerably less than twelve miles as a neighboring tower will receive calls in that region because it is much closer to the mobile phone. Additionally tower cover patterns vary slightly due to weather variation and foliage, or lack of, on the trees.

The concept described above is important to understanding the evidentiary value of call detail records. A call received on tower 19 southwest must be somewhere in its field, but that field is approximately 113 square miles. Therefore the use of call detail records in of themselves cannot be used to place a person at a given time and fixed point location and that limitation cannot be overlooked. However these records can be used to conclusively eliminate other locations as possible origins for the call. For example, in this study there are several locations of interest to the prosecution, these locations were either within the city limits of Austin, Indiana or with the city limits of Scottsburg, Indiana. Examination of the map shows that the city of Scottsburg is less than one-half mile from tower 148 and most of the city is in the center of tower 148 north facing antenna. Several test calls were placed in the city of Scottsburg and are marked with a red start indicating that the call was received on tower 148 north facing antenna.

The defendant claimed to have been at numerous locations within the city limits of Scottsburg and Austin during the time a call was placed and received on tower 19's southwest antenna. Analysis of the actual antenna performance shows that all calls placed in and around Austin, as marked with a orange square on Fig. 2, were received on tower 19 southeast antenna, shown by the green star icon, or on tower 148's north facing antenna shown by a red 'X'. Going yet to a wider area around Austin there were test calls placed in all four ordinal directions outside of the four square miles marked by the orange square. All of these test calls are marked with one of

three icons; the red 'X' for tower 148's north facing antenna , the green star for tower 19's southeast facing antenna or with a red flag for tower 148's southwest antenna. These test calls indicate that any call placed would necessarily have to be received on one of three tower and antenna combinations mentioned above therefore eliminating any possibility that any called placed in or around Austin could be received on tower 19's southwest facing antenna. Analyzing the city of Scottsburg to the south of Austin in Fig. 2 it is easily observed that the city is very close to tower 148 and it is in the center of tower 148's north facing antenna. At the short distance from tower 148 that the city of Scottsburg is, it can be easily ascertained that any call placed from there would be received on tower 148's north facing antenna. Additionally there were three test calls placed in different locations in Scottsburg and each of those three locations are marked with the red 'X' icon indicating that the call was received on tower 148's north facing antenna as expected. The locations of interest, or alibi locations provided by the defendant can all be eliminated as possible locations for the call received on tower 19's southwest antenna.

Any call received on tower 19's southwest antenna must be within its field as stated previously so it was deemed important to make test calls that would provide some measurement of that field. Test calls were placed on State Road 256 which travels in an east-west direction from Austin. Tower 19's southwest facing antenna is marked with the blue pin icon. The easterly-most call placed that was received on tower 19's southwest antenna is shown in Fig. 2. This call was placed approximately two miles west of the intersection of I-65 and State Road 256. No call received by tower 19's southwest antenna could be received east of that call adding the error and variability due to weather and possible foliage difference. It could be reasonably stated that, allowing for up to one half mile of error, that no call placed on tower 19's southwest antenna could have been done so outside of the area shown in Fig. 5.

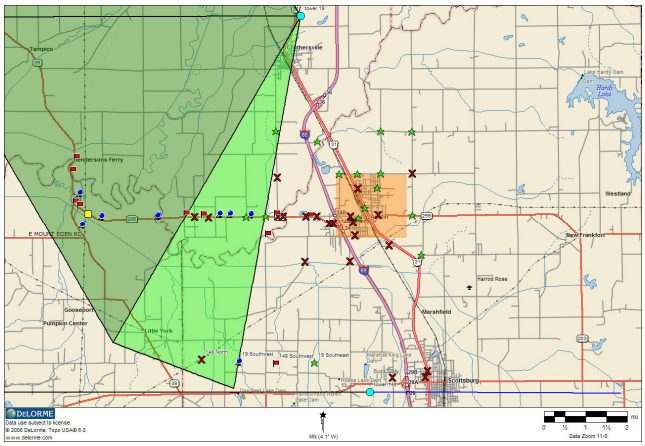

Fig. 5. Area of coverage for Tower 19's southwest antenna

III. Conclusion

The analysis of call detail records and the corresponding tower-antenna pairs can provide useful information as evidence in a criminal trial. Because this analysis can only allow the investigator to be able to state that the call was placed from an area and not a single address or small geographical area, this information is better suited to eliminate alibi locations. The defendant in this case stated that he was possibly at six different locations at the time and date that the prosecution asserted that the murder occurred and the particular mobile phone call was received and terminated on tower 19 southwest. In this investigation it was stated that the call received on tower 19 southwest could not have been originated from any of the locations given as alibis by the defendant to the state police investigator. This type of analysis can make elimination of alibi locations conclusive. However it cannot be concluded that the defendant made a particular mobile call from the alleged crime scene, it can only be concluded that he could have placed that call from that location, the location of the body of the decedent, where the crime was believed to have occurred.

Acknowledgements

The author wishes to thank Blaine Goode, Dustin Houchin, Cynthia Winkler, and William Wibbels, Jr. for choosing him to consult on this project.

References

[1] CTIA. Wireless Quick Facts. Year End Figures. (December 8, 2008). Available at http://www.ctia.org/media/industry_info/index.cfm/AID/10323

[2] Miller, C. The Other Side of Mobile Forensics. (July 2008). Available at http://www.officer.com/print/Law-Enforcement-Technology/The-other-side-of-mobile-forensics/1$42397

Terrence P. O'Connor is a graduate of Northern Arizona University where he received a B.S. in Engineering Technology in 1982 and received a Master of Science degree in Engineering Technology from West Texas State University in 1985. He is an Associate Professor of Electrical Engineering Technology at Purdue University. He teaches at Purdue University's College of Technology at New Albany where he teaches a wide array of courses including electronic communications, digital electronics and advanced microcontrollers. He has research interests in cell phone forensics and ELF/ULF terrestrial signal detection. He can be reached at: toconnor@purdue.edu or by phone at (812) 206-8387.