The Ewasko Cell Phone Ping, 6:50 AM on Sunday 6/27/2010
Tom Mahood

I wanted to put down in writing all I've learned about how Verizon's CDMA2000 cellular system does measurements of the distance from one of their cell towers to a mobile phone. I also wanted to see how it relates to the Bill Ewasko case and what, if any, additional info might be gleaned from phone ping records.

First, the following is ALL I have to date on the phone ping. It's direct quotes from the two emails I got from Investigator Mario Martinez with RSO's Palm Desert office

I asked him about the ping and this is what I got back last July 12th:

> According to Verizon, the cell tower located at 58-399 Serin Drive
> Yucca Valley, ca got a hit at 0650 hours on Sunday 06/27 the range on
> the hit was 10.6 miles and that particular tower faces north. Here is
> the catch, the tower is omni-directional meaning the actual signal
> could have originated from 360 degrees and it will indicate the
> signal is coming from the north. Note: mapping 10.6 miles in a
> south/east direction from the tower, places the signal in QUIAL
> MOUNTAIN. This is the location Ewasko indicate he was going to hike
> on 06/24 and consistent with his itinerary. Ewasko's vehicle was
> located at the entrance to Quail Mountain trail.

I immediately sent him a followup email asking if there was any data on the length of the ping or the quality of the signal? He responded the next day with this:

> When I spoke to the Verizon technician he told me that the length of
> the ping was extremely short, although the quality was good. I
> specifically asked regarding the accuracy and he told me it was 90%
> accurate. It seems to me that the 10.6 miles reading from the hand
> held unit to the cell tower is pretty accurate. We use pings in many
> of our investigations and they get us real close.
>
> I suspect that Ewasko's battery on his cell phone died rather quickly
> if it was searching for a signal. I think he probably turned on the
> phone attempted a call and it shut off due to a dead battery. That's
> the signal that was probably captured, just my opinion.
>
> I don't think Ewasko stayed put after the call didn't go through.

So that's it, everything we know about the cell contact. Of course on the basis of knowing where the cell tower we were able to make "splash maps" of what areas had line-of-sight to the tower and had coverage.

First of all, what's a "ping"?

A ping is the lay term for what's technically called a "registration". It's the procedure a cell phone goes through when connecting itself to the cellular system, and it is very involved. There's a whole pile of different data packets that get exchanged between the cell tower and mobile phone before registration is complete. Things like synchronizing time, serial numbers, channel to use, power levels, what other towers are around, is the one it's connecting to the best, and so on. Once that's done and the tower and handset are both happy, the phone is registered. And that's before a call is even made.

In the case of Verizon, there about 10 different ways a phone can do a registration. For example, a phone registers one way when it's first turned on, sort of like, "Hi world, I just turned on!! What's new?". Another type of registration occurs when a phone is turned off, when it says, "Good bye, my annoying owner is shutting me down!". There's also a timer-based registration where every 5 to 15 minutes (depending on the cell system's settings) the phone checks in and says, "Hey tower, just wanted to let you know I'm still here, ya know, just in case!". And the last registration I'll mention is zone based registration where the phone goes, "Ooooh, I hear a new tower! I just wanted to let you know, Mr. Tower, I'm new in your reception area and I'm eager and willing to please!", after which the phone goes into a standby mode doing the timer registrations.

What we don't know about the ping.

We don't know what sort of registration it was, and the registration type has implications. Realistically there are only two choices, either a turn on or a zone based registration. The timer registration would only have been possible had the phone previously signed in to the Serin Drive tower.

If it was a "turn on" registration, it means on Sunday morning Ewasko physically had to turn on the phone at that time, and the phone had to be in an area with coverage from the cell tower.

If it was a zone based registration, it means the phone was already on, and it was moved into an area with cell coverage. That is, Ewasko was ambulatory.

So, first question would be, “What sort of registration did Ewasko’s cell phone do?”

A quick second question follows, “Were there any records of partial or uncompleted registrations for the Serin tower or one of the other Yucca Valley towers?”

Why was the ping so brief?

This is speculation on my part from what I’ve learned, but detailed examination of the raw ping data could show what happened.

Ewasko started his hike on Thursday morning and the ping occurred at 6:50 AM on Sunday. That’s a long time if he had his cell phone on, and the battery could have been very low.

When a phone registers with a tower, all sorts of data gets exchanged, including the strength of the signal. The phone listens to the tower and sees how strong the tower signal is (sort of how many bars it’s getting). Then the phone sets its transmit power to what it thinks will reach the tower, but not be too “loud” so the signals from other phones are swamped out. The tower then

goes, “Hmmmm, Ewasko phone, your signal is too low, turn up your power 1 click. Nope, still too low, turn it up another click”, and so on. This phone transmit power increase or decrease can happen 800 times per second, and is controlled by the tower.

If Ewasko’s battery was very weak, and the phone had been on standby, suddenly having to transmit at higher power to the tower could have killed it. But before that happened, it registered. It’s also possible it was in Ewasko’s pack, turned on, and he never knew it even connected. Had it stayed on, it would have then used lots of power to start processing all the voicemails that had been put in his mailbox.

What sort of clues could be gained from this? Examination of the raw ping data would show what the signal strength the phone had from the tower was (how many bars), and it could also show what the tower was telling the phone to do. If the phone was reporting the tower’s signal strength was good, and the tower was reporting a weak signal from Ewasko’s phone and was telling it to turn up its power as it faded away, that would be consistent with his battery dying. But if Ewasko’s phone reported that the tower’s signal was fading, and the tower recorded the phone’s signal also as fading, it suggests Ewasko went through a small area of cell coverage and was still moving.

So the question to be asked here is, “What tower signal strengths were being reported by the phone back to the tower, what was Ewasko’s phone’s signal strength, and what was the tower telling the phone to do, power-wise?”

Distance from the tower to the phone

Turns out the phone’s measurement of the tower’s signal strength, which it dutifully reports back to the tower is a really big deal. That’s how the measurement (guesstimate?) of 10.6 miles was determined. But before getting into that critical item, a brief diversion into how cell phone locations are determined by a system like Verizon’s.

By law, cell providers must determine to a good level of accuracy a phone’s position. This is primarily for 911 response. The newest phones have a built in GPS chip, which makes it pretty easy. In cases where there’s no GPS chip or no GPS fix, the cell system can roughly triangulate by measuring the slight differences in time the signal from a specific phone arrives at multiple cell towers. Same signal, but VERY slightly different times. This is called Time Difference of Arrival or TDOA. It’s reasonably accurate. The next notch down in accuracy is when the cell phone reports its time out and is received by several towers, and the towers compare the phone’s time to the tower time. That’s known as Time of Arrival, or TOA. I know it sounds like TDOA, but it’s slightly less sophisticated and accurate. But with both of these methods, the signal needs to be hitting multiple towers, usually at least 3 towers. With Ewasko there was only one tower. So how does that work? It works via the crudest method, Signal Strength.

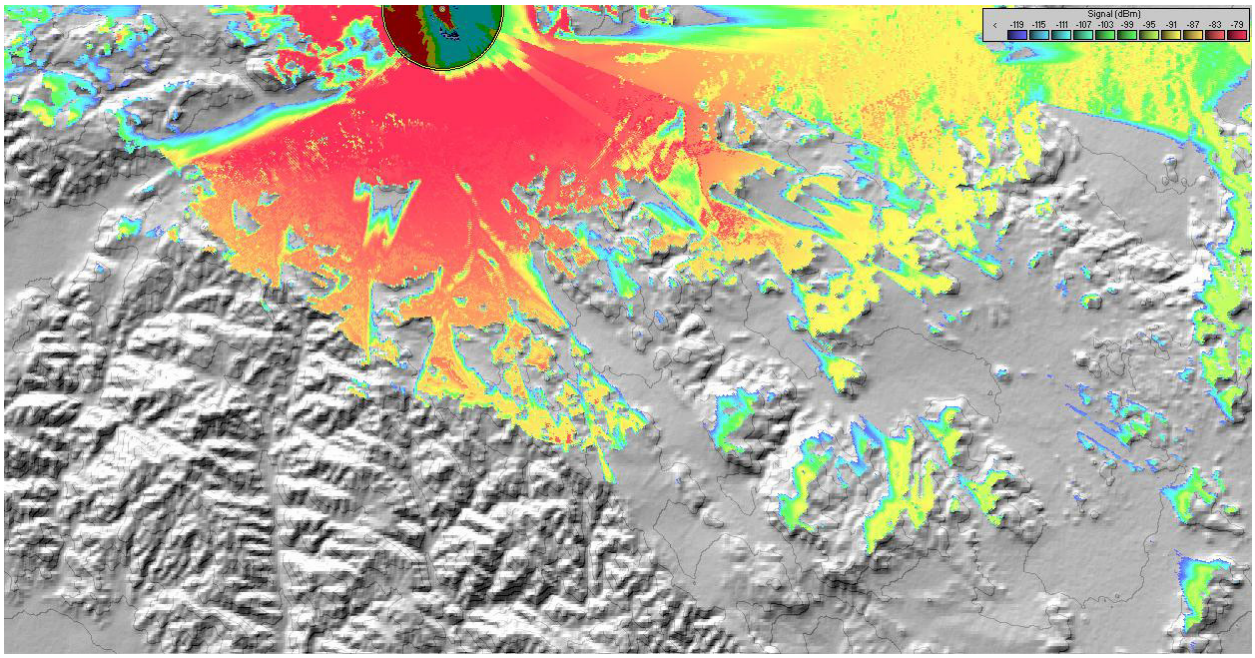
As the cell tower is going about its business, it’s beaming out a Pilot Signal at a known power. The further a phone gets from the tower, the lower the signal strength recorded by the phone will be. While to normal people this might be the number of bars displayed by the phone, to engineers a term they use is RSSI or Radio Signal Strength Indicator. As the phone gets further from the cell tower, the signal it receives from the tower is smaller and so is the RSSI.

Now this ain’t perfect. What if the signal is going through brush or other stuff to reduce it? In that case the phone would think it’s further away from the tower. What if the phone picks up a

reflection of the tower's signal off a rock and gets a stronger total signal? Then it thinks it's closer to the tower. And what if a phone is in a backpack, partially shielded from the tower? It will think it's further away from the tower. Now part of this error can be cleared up because the signal is being sampled many times, and changes can be averaged out. But it's still rough. It's also the only thing we have for a cell tower distance and a <u>really</u> important clue.

I'm back into speculation mode here, but I think what the Verizon tech who examined the ping did was to look at the RSSI levels and said, "That recorded tower signal strength corresponds to a distance of 10.6 miles". I then took that information and drew a 10.6 mile radius around the tower's location. But unless we were in flat Kansas, what I did was completely wrong.

What was actually needed was a signal strength map, which is a much more sophisticated version of a splash map. It shows the signal strength in great detail, but based upon the terrain. And I just happen to have one, below:



This map was created by a guy who has some cellular industry experience. It is centered on the Serin Drive Verizon tower and shows where the tower's signal goes and how strong it should theoretically be. It's like a rainbow, with the strongest signal area being red, then orange, yellow, green and blue. In the upper right there's a legend which equates the signal strength with color, but it's probably not readable in this copy. Verizon would have a much more detailed version of this map for that tower, but we can use this for discussion.

So what signal strength did Verizon use to come up with 10.6 miles? We don't know, but could arrive at an educated guess based upon this chart. If you look across the top part of the plot, the signal heads towards the east past the town of Joshua Tree then into 29 Palms. This is pretty much a clear shot and is line of sight. I previously plotted 10.6 miles out along this, and I came to where the color transitions from green to yellow.

This suggests (and this should be verified with Verizon), that Ewasko's phone was measuring a signal that was at a location somewhere very near a yellow-green boundary on this map. But these occur as close as maybe 6 miles to the tower, and as far out as maybe 17 miles (Ryan

Mountain). And I hate to say it, but that would include parts of Lang Canyon. The 10.6 miles was too over simplistic.

And while it seems this doesn't narrow things down, it does. We can tell precisely what areas are possible and which are not. And any areas that were visible to other cell towers can be excluded since apparently no other pings were recorded. Finally Ewasko's itinerary should help to exclude some areas. There appear to be great areas to explore!

Recapping the questions that could be asked of Verizon:

1. What sort of registration did Ewasko's cell phone do with the Serin Drive tower?
2. Were there any records of partial or uncompleted registrations for the Serin tower or one of the other Yucca Valley towers?
3. What could have accounted for a very short ping?
4. What tower signal strengths were being reported by the phone back to the tower, what was Ewasko's phone's signal strength, and what was the tower telling the phone to do, power-wise?
5. How, precisely, did Verizon compute the tower to handset distance?
6. Can Verizon produce a map showing what geographic areas would experience the signal strengths reported back to the tower?