MODERN CELLPHONE TRACKING

2012 August 22

Roger L. Boyell, www.boyell.com
Digital and Multimedia Sciences Section

The police are working on an arson-murder, and they arrest a suspect . The suspect's alibi is that he was “with friends on the other side of town”, and the other people present all confirm his story. However, a subpoena to his mobile telephone provider obtains data showing the suspect was using his phone to make and receive calls and text messages at different locations than “with friends”.

From the data an expert derives the suspect's surreptitious travel to the scene of the crime and back to the “with friends” location. The expert is able to show the actual track of the suspect as a function of time including when he crossed a major bridge, and surveillance video of the bridge approach proves the case. Result: alibi demolished, defendant guilty.

This article is a simplified explanation of how mobile telephone records are used to localize a suspect or to confirm an alibi location. Yes, alibis can be just as easily supported as crime locations themselves. The topic of this article is retrospective or historical localization of the phone user, not real-time tracking.

Trail of Electronic Evidence

An intrusive examination of the suspect’s phone is not necessary. Even if it is an old "dumb" phone that has since been shredded, its use to make or receive calls has left a trail of electronic evidence about the user’s locations.

A cellular telephone is actually an advanced radio transmitter/receiver. When a user makes or receives a cellphone call, his cellular telephone “handset” sends out a radio signal and simultaneously receives a mating radio signal in an authorized frequency band. When two-way communication is established with a nearby “base station”, the call is connected, and the voice path is enabled.

Cellphone voice communication is usually full duplex mode, meaning either party is able to speak and interrupt the other just like a landline telephone call. Many phone models also have capability for sending and receiving text messages, photographs, and video recordings.

Base Station Ubiquity

Each base station consists of installed radio equipment and its associated antennas, located and oriented to cover one or more geographic cells. The base stations accessed by cellular telephones are called cellular wireless sites or

“cellsites”. The existence of a cellsite permits all the cellular telephones which are within radio range (a few miles) to connect voice calls to each other and to the public telephone network.

Hundreds of cellsites typically dot the large metropolitan areas of the country, so a user’s handset is almost always within range of one – sometimes of many – candidate cellsites. In large cities the cellsites may be only blocks apart, while in rural areas they may be several miles apart. Coverage overlaps are intentional, and the supposed cells have rigid boundaries only in theory.

Establishment of Two-Way Communication

A cellsite that is available for service transmits a signal identifying itself and its provider network – e.g. Sprint, AT&T, Verizon, Rogers, Comcast, T-Mobile, Cox, etc. The handset initially communicates with only one cellsite to establish the communication link. The user's handset selects, at any instant, the site which offers it the most favorable signal, considering received signal strength, freedom from distortion and multipath effects, and network availability. When the handset makes an outgoing call, it uses the cellsite on which it is camping to make the initial connection.

The most favorable cellsite signal is typically the strongest on whichever network(s) the handset is programmed. The strongest signal is usually the closest, but hilly terrain and buildings can block the radio signals. Sometimes the nearest sites are overloaded and nonresponsive, and on occasion they are down for maintenance.

Thus the cellsite which is accessed by a handset for any call at any instant, may or may not be the geographically closest to the user’s handset. However, every time the handset selects a different cellsite, it registers with the network as being accessible from that cellsite for incoming calls. As with outgoing calls, the initial connection is made through the cellsite on which the handset is camping.

Handover from Site to Site

While a call is in progress, the network instructs the handset which site to use. When the handset changes location, the cellsite being accessed can be unobtrusively changed to maintain communication. The handover from site to site during a voice call is handled through a signaling channel associated with the voice path established.

Handover is usually transparent to the user and can occur several times per minute for fast-moving trains or cars. The network and the handset coordinate the handover so that the two-way voice communication appears solid to the user. Of course anyone who has experienced unexpected dropped calls knows that the handover can fail on occasion.

The cellsites actually accessed by the handset give geographic locations from which the track of the phone can be deduced. The provider networks maintain records, in particular listing the cellsites accessed at the beginning and at the end of almost every call. This, along with call date and time, is the metadata.

Records Used in Tracking

The cellular network providers keep records of calls made and received for billing and other business purposes. The call detail record (CDR) of any specific call typically shows that the handset (by unique phone number) was in radio range of the (uniquely numbered) cellsite initially accessed. This may be several miles in any direction from the cellsite.

Records from several successive calls to or from the same handset (the same phone number) can be used to establish a sequence of locations forming the ground track of the phone's user. The cellsites can be mapped by referring to the cellsite location listing (CLL) of the network provider for the geographic area of interest. Although no individual call can precisely localize a user's handset, a time sequence of calls showing cellsites successively accessed forms a track.

Given sufficient call detail records and cellsite location listings, the phone user's track can be reconstructed to indicate where he was at any time, along with his speed and direction of travel. Referring to a roadmap might allow the frequent phone user's exact route to be plotted including his timeouts for fuel and meals.

Further, the records show the telephone number to or from which the call was made, along with other information that may be incriminating or exculpatory. Nevertheless, the records do not reflect anything about the content of the voice call or text message, or picture, or video recording

Court Requirements

In the courtroom the call detail records and the cellsite location lists are generally admitted as evidence when vouched for by an authorized employee of the provider. Because these files can be voluminous, they are frequently maintained as electronic spreadsheets rather than computer printouts. A user may make or receive dozens, sometimes hundreds, of calls per day, and a geographic area may contain hundreds of, sometimes a thousand, cellsites

Interpretation of the records and lists must be performed by a qualified expert who is trained to take account of:

-- the cellsite naming and number aberrations which result from the Topsy-like proliferation, reorganization, and abandonment of cellsites

-- the actual locations and directivity patterns of the base station antennas, which may not be reflected in the current cellsite location listings,

-- effects on radio propagation caused by topography and man-made structures,

-- the many different format and coding schemes used by the network providers in compiling their thick computer printouts and spreadsheets.

As one example, the street address for a cellsite in San Diego placed it a block away from a road intersection. That would imply the user's handset when accessing that cellsite was near the intersection. However, the street address was only for an access road, and the actual cellsite was a tower half a mile away, up on a hill, where it offered coverage of several different roads. Simply reading the call detail records and tying them to the cellsite location lists did not represent correct interpretation.

An older cellsite in North Carolina bore the name of a town, and that could be interpreted as being its location. However, newer cellsites were built within the town, and the cellsite bearing the town name was actually in another county entirely. Cellsite naming and numbering aberrations can give opposing counsel a basis for disputing the validity of user localization.

The proponent of cellphone records in the courtroom usually attempts to make convincing arguments that the named or expected user of the handset really was in possession of it at the time of the alleged crime. That is, the localization of the handset implies localization of the user. Ear-witnesses to the calls may be offered as evidence of user identity.

Prosecutors and defendants throughout the world are learning to use cellphone technology to track suspects and to exonerate the innocent. The major network providers have developed departments whose only task is compliance with subpoenas seeking their business records in order to localize cellphones..

Avoidance of Being Tracked

The way to prevent your phone from being tracked, should you want to do so, is to power it completely OFF. If you are paranoid, take out the battery as well.

Incidentally, the foregoing technology description does not mention tracking by Global Positioning Satellites, nor is any GPS capability in the phone required for tracking as described above.

GPS is a different tracking methodology altogether, but the same principle holds: A fully OFF cellphone cannot be electronically tracked. As soon as you turn it ON, however, you begin leaving a new trail of electronic evidence.

++
Roger L. Boyell, Electronics Analyst
416 Parry Drive, Moorestown NJ 08057-2877
Phone 856-234-5800 * Fax 856-234-9539
E-mail boyell@ieee.org * Web site www.boyell.com