Approccio all'Analisi Forense delle Celle Telefoniche (BTS)

L'enorme diffusione dei telefoni cellulari e le numerose possibilità di utilizzo degli stessi, non solo per la comunicazione di tipo voce ma anche per lo scambio di dati (messaggi brevi, navigazione Internet ed altre forme), hanno portato le indagini giudiziarie a fare largo uso dell'analisi forense sia degli stessi terminali sia delle tracce che questi lasciano nelle reti degli operatori telefonici.

Senza entrare nel merito del funzionamento di una rete di telefonia mobile, in tale contesto è sufficiente evidenziare che il terminale mobile, quando è acceso ed ha al suo interno una SIM attiva, colloquia con la rete dell'Operatore di appartenenza in modo regolare, aggiornandola costantemente ed in maniera puntuale relativamente alla localizzazione, anche quando non è utilizzato dall'utente per effettuare telefonate o altro.

Su queste informazioni, per inciso, si basano alcuni servizi di geolocalizzazione forniti dagli operatori stessi (informazioni turistiche, mappe, etc.).

Tali dettagli non sono conservati all'interno della rete dell'operatore se non all'interno della documentazione di traffico storico, che costringe l'investigatore ad un arduo lavoro di ricostruzione e di analisi della localizzazione sulla base di informazioni poco dettagliate.

L'unico metodo che può essere utilizzato, quindi, per individuare la posizione di un cellulare in un dato momento, "a posteriori", è quello di basarsi sui dati disponibili nei tabulati telefonici, basati a loro volta sui cartellini di traffico (Call Detail Record - CDR) generati dalle centrali telefoniche.

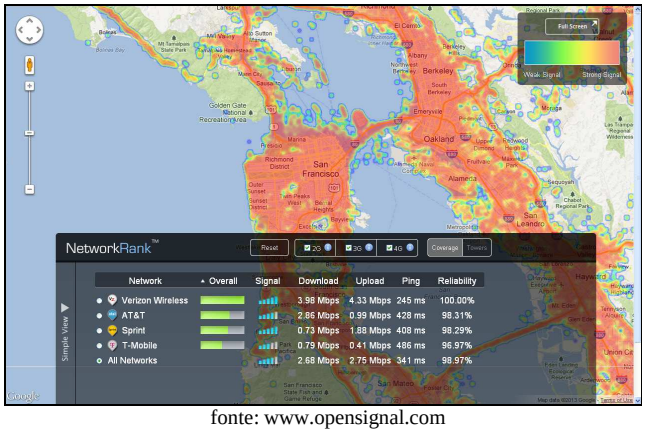
Premesso che ogni operatore telefonico fornisce questi dati in formati differenti, sono comunque sempre presenti informazioni quali: data, ora, durata della conversazione, numerazione chiamante, numerazione chiamata, identificativo del telefono (IMEI) chiamante e ricevente, cella agganciata (Cell ID) del terminale chiamante e ricevente.

Per l'analisi riveste grande importanza l'informazione sulla cella, identificata dal codice Cell ID, che consente di conoscere con certezza la stazione base cui il terminale era connesso mentre stava ricevendo/trasmettendo.

Ciò significa che nei momenti in cui il terminale è acceso, ma non sviluppa traffico, non è possibile conoscere (a posteriori) la cella (BTS) su cui era attestato.

Nota l'informazione sulla cella, bisogna disporre delle cosiddette "mappe di copertura" della rete.

Queste mappe vengono costruite dall'operatore telefonico sulla base dei parametri di configurazione della cella e del territorio e sono, sostanzialmente, una rappresentazione simulata del grado di copertura territoriale di ogni singola BTS e del relativo campo.



fonte: www.opensignal.com

Si tratta, quindi, di carte geografiche su cui viene indicato, per ogni singolo punto geografico, la predizione statistica della cella cosiddetta "miglior servente" (ovvero la BTS con il livello di segnale più alto), tramite l'uso di colorazioni differenti.

In questo modo è possibile verificare l'area geografica illuminata dalla stazione base, e da questa elaborare valutazioni statistiche sulla posizione geografica dell'apparato.

Da quanto precedentemente descritto, è evidente che l'analisi delle celle si fonda su una valutazione di tipo probabilistico, per cui è fondamentale comprendere quali siano i fattori da tenere in considerazione, per stimare l'affidabilità dei risultati.

Questi fattori possono essere sintetizzati in:

- la qualità delle mappe disponibili (accuratezza della modellizzazione del territorio, definizione della simulazione), che forniscono un'indicazione statistica della cosiddetta "cella miglior servente";
- lo stato effettivo della/e stazione/i base nel periodo di interesse, incluso il livello di traffico totale gestito: la rete prevede logiche di instradamento delle chiamate, e di aggancio delle celle, anche in funzione del carico servito;
- gli algoritmi utilizzati dalla rete e dai terminali in modo dinamico per stabilire l'aggancio e lo scambio con le altre celle;
- la peculiarità di alcune posizioni geografiche, che per varie ragioni (posizionamento degli edifici, riflessioni

di segnale etc.) possono far sì che, a dispetto di quanto rappresentato nella mappa, si possa avere una cella miglior servente diversa da quella prevista. Questo vale in particolare negli ambienti indoor;

- altri fattori specifici ambientali (es. meteorologici).

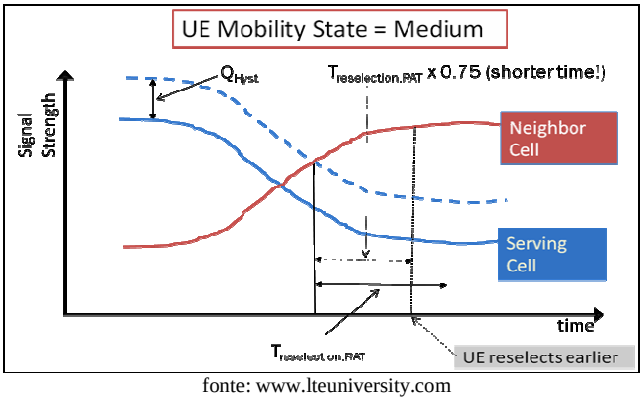
Tutti i fattori sopra descritti possono influire nel meccanismo di "aggancio" tra cella e terminale, facendo sì che in un dato punto geografico ed in un dato momento la cella che effettivamente sta servendo il cellulare possa essere differente da quella rappresentata dalla mappa di copertura analizzata.

Uno dei meccanismi che deve essere tenuto in grande considerazione nelle analisi è quello su cui si basa la mobilità stessa del servizio radio, ovvero la riselezione delle celle.

Un utente che si muove deve essere gestito dalla rete in modo che gli sia sempre, per quanto possibile, assicurato il servizio, in termini di raggiungibilità e qualità.

Il terminale mobile dovrà quindi, in modo dinamico, elaborare le informazioni relative alle celle disponibili (ovvero quelle con cui riesce a comunicare) agganciandosi coerentemente con le celle 'migliori'.

Tecnicamente questa elaborazione prende il nome di Cell Reselection: il terminale mobile, anche in fase di stand-by, continua a "leggere" il segnale che riceve dalle celle e, tra tutte queste, seleziona una cella servente sulla quale si attesta, ed una lista delle sei migliori candidate, dette celle non serventi.



fonte: www.lteuniversity.com

L'operazione di selezione della cella servente viene ripetuta ciclicamente ad intervalli temporali prefissati: detta scelta avviene tramite un algoritmo che si basa su alcuni parametri, calcolati per ogni singola cella con cui il terminale può dialogare.

Nel caso di un gestore che operi sia a 900 MHz che a 1800 MHz (bande di frequenza utilizzate in Europa, mentre negli Stati Uniti si usano le bande attorno a 850 e 1900 MHz), può essere utile assegnare alle celle di quest'ultima banda una priorità maggiore così che i terminali dual band si attestino preferibilmente su queste celle, lasciando libere quelle a 900 MHz ai terminali mono band, nel contempo rendendo fruibili ai terminali più evoluti i maggiori servizi disponibili nella banda a 1800 MHz (soprattutto lo scambio dati).

Ogni qualvolta il terminale seleziona una nuova cella come candidata per un cell reselection azzera un timer interno, applicando una "penalizzazione" alla cella abbandonata.

Questo algoritmo, che definisce una sorta di isteresi di connessione, serve a sfavorire temporaneamente le celle non serventi, rispetto alla servente nelle fasi di sgancio e riconnessione, al fine di evitare passaggi troppo frequenti tra due o più celle (c.d. effetto ping pong).

In altre parole, nel momento in cui viene selezionata una nuova cella quale miglior servente, la cella appena abbandonata potrebbe trovarsi ad essere nuovamente la miglior servente se il terminale non si è ulteriormente allontanato, o addirittura ha cambiato direzione: in questi casi, se non ci fosse la cosiddetta 'penalizzazione' nell'algoritmo, il terminale si connetterebbe nuovamente con la cella appena sganciata, magari in modo ripetuto.

Questo fa sì, quindi, che negli spostamenti tra una zona coperta da una cella e quella adiacente, ci sia un effetto di non contestualità nel comportamento di selezione della cella da parte del terminale mobile, effetto di cui l'investigatore deve tenere conto nelle sue valutazioni.

In base a quanto illustrato precedentemente, si può arrivare alla conclusione che la localizzazione "a posteriori" di un apparato radiomobile all'interno dell'area geografica illuminata dalla relativa antenna è un dato non certo, ma probabile.

E' possibile infatti che l'apparato si trovi geograficamente nel settore di una cella, pur essendo comunque servito da una cella adiacente non "prevista" nella mappa di copertura.

Più in generale, si può affermare che le conclusioni tratte dall'analisi delle celle non consentono (solitamente) di definire localizzazioni su aree geografiche ridotte, dell'ordine dell'area di copertura di una singola cella.

Anche volendo affrontare scientificamente tutti i possibili snodi, ovvero tramite un'analisi sperimentale e statistica, su aree ridotte è difficile conseguire risultati che abbiano una valenza dirimente.

Ciò non significa ovviamente che questa attività non abbia degli importanti risvolti, o che i suoi risultati debbano essere trascurati: esiste sempre la possibilità che in condizioni particolari l'analisi delle celle possa essere determinante, oppure, con maggiore probabilità, che questi risultati possano costituire elementi aggiuntivi o integrativi alle altre prove: in questo caso è fondamentale che gli elementi a disposizione (testimoniali, etc.) siano confrontati con le informazioni provenienti dall'analisi delle celle in modo da costruire un quadro probatorio che possa essere conclusivo, o almeno complessivamente più preciso.