La Data Retention operata dagli Operatori telefonici per fini di giustizia e repressione dei reati è un'attività fondamentale su cui si basa l'attività investigativa condotta dalla Polizia giudiziaria, a cui spetta poi l'analisi dei tabulati di traffico storico. L'analisi tradizionale di questo tipo di dati può realizzarsi con un approccio metodologico articolato in tre *step*: il primo rappresenta la mera lettura in sequenza cronologica delle celle agganciate, il secondo la georeferenziazione su mappa degli indirizzi dove sono ubicate le celle, infine il terzo prevede la rappresentazione, sempre su mappa geo-referenziata, delle aree di copertura teoriche delle celle. L'esperienza maturata dalla Polizia Scientifica in questa tipologia di accertamenti, oltre ad evidenziare i limiti delle tecniche tradizionali finora esposte, ha consento di ampliare le fasi di analisi rappresentazione dei dati di traffico. Le *Best Practices* che ne sono scaturite hanno condotto alla implementazione di un quarto *step* differenziato in base alla tipologia di quesito.

di Gianpaolo Zambonini e Claudio Fusco

GEO-TIMING NEI TABULATI DI TRAFFICO STORICO (I PARTE)

***Gianpaolo ZAMBONINI**, Primo Dirigente Ingegnere della Polizia di Stato, è Direttore della IV Divisione del Servizio Polizia Scientifica, nonchè Direttore della Sezione Indagini Elettroniche, presso il Dipartimento di Pubblica Sicurezza del Ministero dell'Interno. Nell'ambito della sua attività lavorativa è divenuto un esperto forense nel settore delle intercettazioni, dell'analisi della voce umana, delle localizzazioni, dell'analisi dei telefoni cellulari e dell'elaborazione delle immagini.*

***Claudio FUSCO**, Ingegnere Elettronico, matura un'esperienza ventennale nel settore delle telecomunicazioni prestando servizio in qualità di network engineer presso uno degli operatori nazionali dominanti, curandone l'ingegnerizzazione delle piattaforme di accesso ed autenticazione alle reti dati fisse e mobili. Attualmente in servizio presso la Sezione Indagini Elettroniche della IV Divisione del Servizio di Polizia Scientifica in qualità di funzionario addetto, è referente per le attività di intercettazione, analisi tabulati e radiolocalizzazione.*

1. Introduzione

Sono passati oltre vent'anni dalla nascita delle prime reti radiomobili, un intervallo temporale nel quale l'uso dei telefoni cellulari è entrato a far parte delle abitudini quotidiane di tutte le persone; tanto da generare una serie di effetti collaterali tra cui quello di trasformarli nel principale strumento investigativo nella disponibilità delle Forze di polizia. I cellulari, infatti, sono veri e propri contenitori di informazioni che, se correttamente elaborate, consentono di ottenere una serie di dati investigativi sui soggetti che li utilizzano, come la loro posizione. Per lo svolgimento di tali attività è necessario ottenere "a posteriori" i dati di interesse conservati dagli Operatori telefonici. Infatti, tutti i telefoni cellulari, quando sono accesi e con una SIM attiva al loro interno, colloquiano in modo regolare con la rete dell'operatore di appartenenza (in Italia ad es. TIM, Vodafone, Wind e H3G), segnalando ogni loro movimento e lasciandone traccia nei *server* della rete.

Questi dati non sono integralmente conservati dall'operatore e l'unico metodo che può essere utilizzato da un investigatore per individuare le informazioni di interesse, è quello di analizzare i tabulati telefonici, basati a loro volta sui cartellini di traffico generati dalle centrali telefoniche. Ciò significa che, in generale, gli eventi memorizzati dagli operatori e messi a disposizione dell'Autorità Giudiziaria, sono quelli riferiti ai momenti in cui il terminale è in comunicazione (eventi di chiamata, SMS, etc.) e di conseguenza viene applicata loro una tariffazione, ad eccezione di tipologie di eventi come i tentativi di chiamata che non vengono tariffati ma comunque tracciati[1].

I tabulati telefonici quindi nascono come strumenti di fatturazione e di documentazione del traffico. Quando il regime di concorrenza tra gestori non era così maturo e non venivano erogati contratti *flat* o a volume di traffico, alcune offerte prevedevano costi differenti delle comunicazioni a seconda dell'area geografica da cui veniva effettuata o dove veniva raggiunto il chiamato. In tale contesto ogni gestore ha un suo *format* per la presentazione dei tabulati, alcuni ad esempio riportano contestualmente soltanto l'indicativo della cella (Wind, TIM, 3), altri anche l'indirizzo (Vodafone), tanto che i formati con cui vengono consegnati alla Polizia Giudiziaria sono sempre differenti da un operatore all'altro.

Dal punto di vista normativo tutti i gestori di telecomunicazioni, sono chiamati - secondo quanto disposto dall'art. 96 D.Lgs. 259/03 "Codice delle comunicazioni elettroniche", nel rispetto del D.Lgs. 196/03 "Codice in materia di protezione dei dati personali" - ad assicurare all'Autorità Giudiziaria in forma riservata le cd. "prestazioni obbligatorie" che comprendono anche i tabulati di traffico telefonico pregresso, i quali contengono una serie di informazioni catalogabili in quattro categorie:

1 Tutti questi eventi vengono conservati dagli operatori telefonici fino al 31/12/2016 per effetto dell'entrata in vigore della Legge 17 aprile 2015, n. 43 di conversione, con modificazioni, del decreto-legge del 18 febbraio 2015, n. 7 "Misure urgenti per il contrasto del terrorismo, anche di matrice internazionale".

- *Luoghi* (CGI).
- *Eventi* (tipo di traffico, Generato/Terminato, non risposto, sms …)
- *Tempi* (*timestamp* dei dati traffico, durate …)
- *Identità di terminali ed utenze* (codici IMEI , IMSI ed MSISDN)

Sulla base di tali informazioni, e grazie alla correlazione delle tracce, possono essere condotte alcune attività tecniche forensi che aprono diversi scenari investigativi, come ad esempio: una volta individuata un'utenza telefonica è possibile verificarne 1) la presenza in un dato luogo e in un certo intervallo di tempo; 2) la dinamica degli spostamenti; 3) tutte le SIM ospitate al suo interno; 4) la rete delle relazioni; 5) la sostenibilità di ipotesi di incontro con altri soggetti noti e molto altro. Come in ogni indagine, anche questo elemento tecnico sarà tanto più solido quanto più risulti aggiuntivo o integrativo alle altre prove.

In questo caso, è fondamentale che tutti i dati investigativi a disposizione (dichiarazioni testimoniali, etc.) siano confrontati con le informazioni provenienti dall'analisi dei tabulati, in modo da costruire un quadro probatorio che possa essere complessivamente più preciso, per fornire una compatibilità tra una ricostruzione investigativa e i dati sui telefoni.

In relazione a quanto esposto, risulta evidente che **l'unica parte del procedimento di trasformazione delle tracce digitali contenute nei tabulati in fonti di prova, regolata dal punto di vista legislativo e dove le procedure sono ben definite, è la parte di acquisizione dagli Operatori telefonici, mentre quelle di ricerca, analisi e presentazione sono affidate alla capacità dell'esperto**. L'esperienza dimostra, infatti, come la mancanza di una adeguata professionalità da parte dell'analista, spesso, sia causa di ricadute nefaste sia sul fronte dello sviluppo investigativo sia su quello della formazione della prova in sede dibattimentale, con tutte le ovvie conseguenze in termini di risultato finale.

L'utilizzo dibattimentale ed investigativo dell'evidenza elettronica è ormai sempre più ricorrente, con un *trend* in crescita esponenziale a cui non corrisponde un equivalente percorso evolutivo sia metodologico che delle strumentazioni utilizzate.
La rete telefonica, sempre più complessa e variegata in termini tecnologici, lo sviluppo di nuovi servizi e l'attuale regime "non strutturato" con cui le informazioni vengono prodotte dai diversi Operatori, richiedono un approccio metodologico sistematico e "robusto", in grado di garantire al risultato dell'analisi una tenuta dibattimentale dagli attacchi degli avvocati della parte e dei loro consulenti.

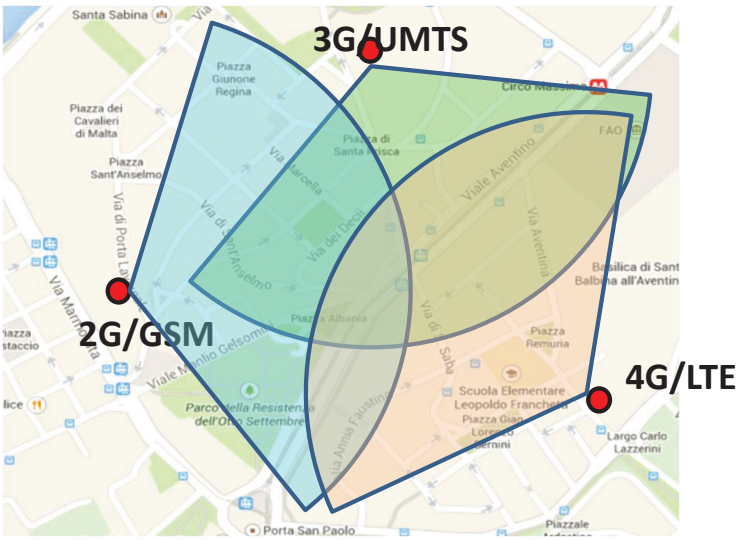
Obiettivo del presente intervento, dopo un sintetico cenno ad alcuni degli aspetti condizionanti degli agganci di cella, è quello di evidenziare i limiti delle tecniche tradizionali di localizzazione a posteriori basate sul traffico telefonico e fornire nuove soluzioni attraverso l'integrazione di strumenti utilizzati in differenti ambiti.
In tale ottica il Servizio "Polizia Scientifica" della Polizia di Stato ha sviluppato una nuova metodologia per l'analisi e soprattutto al visualizzazione a la presentazione in dibattimento dei dati presenti in un tabulato.

2. Alcuni richiami utili

L'evoluzione della telefonia mobile ha causato la disseminazione sul territorio nazionale di impianti appartenenti alle quattro generazioni tecnologiche che hanno seguito lo sviluppo delle reti mobili. In uno stesso luogo geografico possono essere co-presenti il segnale GSM 900 e 1800, l'UMTS 2100, l'LTE 800 1900 e 2600 (le cifre sono indicative della banda impegnata e sono espresse in MHz). La ripetibilità dell'aggancio di una cella ad una data ora, in una certa posizione geografica è quanto mai un evento statistico il cui studio va ricondotto a modelli matematici con innumerevoli variabili.

L'evento di traffico documentato nel tabulato con il relativo impegno di cella, pur costituendo un elemento oggettivo, deve essere ponderato alla luce di alcune inevitabili considerazioni:

- Il territorio nazionale è suddiviso in celle che costituiscono l'area elementare di influenza con cui il gestore intende coprire una porzione di territorio con una data tecnologia ad una data frequenza. In relazione alla zona, al grado di urbanizzazione e al tipo di collegamento con cui la BTS è connessa alla centrale, ogni cella ha un determinato numero massimo di canali simultaneamente disponibili al traffico dell'utenza.
- Ciascun terminale, dopo l'accensione, ricerca la rete del gestore telefonico associata alla SIM inserita al suo interno, tentando di agganciare le celle tecnologicamente più evolute a cui è abilitato (tra 2G/3G/4G) e selezionando quella che garantisce la miglior qualità del servizio.
- Quanto sopra comporta che non sempre il cartellino di traffico di un evento documentato è associato alla cella servente, ossia quella che



per il gestore, tecnologia e banda, assicura in quell'area il miglior valore di parametri utili al *Cell Selection*[2]. Ostacoli temporaneamente presenti, interferenze, guasti di impianti o la loro saturazione (in termini di numero di canali disponibili), possono spingere il terminale e la rete, a condurre flussi di traffico su celle limitrofe e comunque remote alla effettiva area in cui il telefono si trova, presenti sul sito con segnali deboli e al limite della accettabilità.

- Nel caso di utilizzo in ambienti interni occorre considerare poi la diversa attitudine alla permeabilità delle strutture edilizie alle diverse bande di frequenza. Questo significa spesso che cambi di cella in eventi di traffico ravvicinati nel tempo, non sempre corrispondono a spostamenti sostanziali dell'utenza, ma possono essere ricondotti al diverso affaccio dei locali di cui un'unità immobiliare è composta e allo spostamento dell'utilizzatore da una stanza all'altra dell'edificio.
- Le celle per loro natura non sono invarianti e con un perimetro stabile e delimitato, infatti per sopperire alla diversa densità di utenze in una data area e fornire sempre il maggior numero di canali disponibili con la minore interferenza possibile, le reti tendono a variare il raggio operativo della cella[3]. Si ottengono in questo modo risparmi energetici nelle occasioni di minor densità di traffico e massimi profitti nell'ora di punta.

L'incidenza dei fattori sopra accennati rende talvolta di difficile interpretazione l'analisi delle sole sequenze di agganci di cella e può condurre a valutazioni errate se l'esperienza dell'operatore non è affiancata da un adeguato supporto metodologico e strumentale.

3. Limiti delle metodologie tradizionali

Molto spesso gli esperti del traffico telefonico, sia per le scarse risorse tecnologiche di cui dispongono che per le ridotte tempistiche imposte dalla magistratura, si limitano all'analisi cronologica di sequenze di indirizzi, corrispondenti alle celle riportate nei tabulati.

Tuttavia se nel caso più semplice relativo all'analisi del traffico effettuato da diversi soggetti che utilizzano lo stesso operatore telefonico, il ricorso ai soli indirizzi di sito, conduce a risultati difficilmente interpretabili da parte di soggetti non "addetti ai lavori", a maggior ragione nel caso di monitoraggi estesi su utenze di operatori diversi con celle fisicamente ubicate in siti differenti serventi le stesse aree di territorio, la lettura dei *report* degli eventi di traffico diventa proibitiva.

Per meglio comprendere i limiti delle metodologie di analisi e rappresentazione dei tabulati più diffuse, risulta utile considerare *due casi reali* che spesso ricorrono a livello investigativo e dibattimentale, ripercorrendo fase per fase lo svolgimento delle attività. In entrambi i casi di studio, inizialmente vengono svolte le analisi più semplici, che non necessitano di un esperto, mediante le tabelle di eventi, successivamente saranno introdotte elaborazioni mano mano più complesse che richiedono personale qualificato e sistemi di analisi sempre più evoluti.

Ne risulta un approccio metodologico articolato in tre *step*: il primo rappresenta la mera lettura in sequenza cronologica delle celle agganciate, il secondo la georeferenziazione su mappa degli indirizzi dove sono ubicate le celle, infine il terzo prevede la rappresentazione, sempre su mappa geo-referenziata, delle aree di copertura teoriche delle celle.

Nel dettaglio i due casi sono:

1. **Caso dell'utilizzo indoor di un terminale mobile**
   L'impiego di un terminale all'interno di un edificio espone il processo dell'aggancio di cella all'effetto schermante delle infrastrutture edilizie. In queste circostanze, sebbene l'utilizzatore compia movimenti irrisori se riferiti alle distanze in gioco in termini di dislocazione delle celle, a seconda della posizione assunta dal terminale nel fabbricato gli ostacoli che il segnale radio deve attraversare per mettere in comunicazione il telefono con la BTS possono variare sensibilmente, sia in termini di quantità (numero di pareti nella direzione di una data cella) che di proprietà schermanti (cemento armato piuttosto che tramezzi in laterizio leggero).
   L'effetto che generalmente si riscontra sul tabulato in tali casistiche è una sequenza di agganci di cella spesso differenti e soprattutto dislocate su direzioni e distanze molto diverse tra loro rispetto alla fisica ubicazione del terminale.
2. **Caso del percorso comune**
   Altro contesto di studio ricorrente consiste nell'analisi del traffico rivolta alla localizzazione simultanea e reciproca di più utenze al fine di vagliare l'ipotesi di frequentazione o incontri tra i soggetti utilizzatori.
   In queste casistiche l'appartenenza delle utenze ad operatori differenti ed i fattori casuali nei processi di aggancio di cella accennati al paragrafo precedente introducono diversi elementi di criticità nelle metodologie comuni di analisi e rappresentazione dei dati.

2 Dalla normativa GSM ad esempio, in letteratura, sono ben noti i meccanismi che concorrono al calcolo dei famosi coefficienti C1 e C2, utili al ranking delle celle sulle quali il terminale è in ascolto e tenute in considerazione in caso di mutamento delle condizioni radio. Tra i valori che concorrono al calcolo ritroviamo la potenza ricevuta, il livello minimo di segnale in ricezione per cui il gestore autorizza l'aggancio, la massima potenza in trasmissione a cui il terminale è autorizzato a comunicare ed altro ancora.

3 Di seguito alcuni riferimenti di bibliografia:

- Marsan, M. Ajmone, et al. "Optimal energy savings in cellular access networks." Communications Workshops, 2009. ICC Workshops 2009. IEEE International Conference on. IEEE, 2009.
- Hanly, Stephen V. "An algorithm for combined cell-site selection and power control to maximize cellular spread spectrum capacity." Selected Areas in Communications, IEEE Journal on 13.7 (1995): 1332-1340.
- Micallef, Gilbert, Preben Mogensen, and Hans-Otto Scheck. "Cell size breathing and possibilities to introduce cell sleep mode." Wireless Conference (EW), 2010 European. IEEE, 2010.

Al solo scopo di esemplificare la tipologia di informazioni disponibili all'analista nei casi sopra accennati, si considerino le tabelle sotto riportate, che rappresentano i dati di partenza contenuti nei tabulati .

Utente	Ora	Ch.te/ Ch.to	Indirizzo
A	1	111111	Via Roma
A	2	222222	Via Bari
A	3	333333	Via Bologna
A	4	444444	Via Roma
A	5	555555	Via Bari

Tabella 1 – Uso indoor

Utente	Ora	Ch.te/ Ch.to	Indirizzo
A	1	111111	Via Ippocampo
B	2	222222	Via Primula
A	3	333333	Via Geranio
B	4	444444	Via Margherita
A	5	555555	Via Garofano

Tabella 2 – Percorsi comparati

In entrambe l'utente a cui l'evento di traffico è riferito è indicato con una lettera nella prima colonna. Data e ora dell'evento di traffico sono riportate in seconda colonna e per semplicità espositiva sono state sintetizzate in numeri progressivi secondo un criterio cronologico. La terminazione o la sorgente del traffico sono infine riportate in terza colonna, seguite dall'indirizzo di cella.

PRIMO CASO (utilizzo *indoor* di un terminale mobile)

Quesito: partendo dall'analisi delle celle verificare se il telefono indicato con A nel periodo temporale compreso tra 1 e 5 era in movimento lungo un percorso o è rimasto all'interno di un appartamento;
Soluzione: il telefono è rimasto all'interno di un appartamento.

I° *STEP* DI ANALISI

Partendo dai tabulati e dalla tabella degli eventi corredati con gli indirizzi di cella (il contenuto della colonna denominata indirizzo nella tabella), l'attività più semplice è la lettura da 1 a 5 degli indirizzi delle celle agganciate dall'utenza A.
Poiché l'indirizzo tende a cambiare è facile ipotizzare una dinamica di spostamento dell'utenza A, che non trova riscontro con quella reale. Infatti pur cambiando l'indirizzo il soggetto non ha mai abbandonato la propria abitazione.

II° *STEP* DI ANALISI

Nel secondo *step* viene implementata una rappresentazione cartografica dei soli indirizzi di cella ottenuti dai dati di traffico. La rappresentazione bidimensionale degli eventi di traffico comporterà la raffigurazione in punti coincidenti di eventi che nel tempo e nello spazio sono distinti. Nella figura, l'utenza A che si trova all'interno di un appartamento, è rappresentata nella sua posizione reale dal telefono giallo e, seppure sostanzialmente fermo, sembra disegnare un percorso in senso antiorario effettuando, sulle tre differenti celle evidenziate con pallini rossi, i cinque eventi di traffico contraddistinti dai progressivi di Tabella 1.
Anche in questo caso il risultato potrebbe essere forviante.

III° *STEP* DI ANALISI

Lo *step* successivo, oltre alla georeferenziazione degli indirizzi, prevede anche la rappresentazione della direzione di massimo irraggiamento della cella, l'apertura angolare del lobo principale e la considerazione della potenza irradiata. È ora intuibile come, anche all'occhio di un non addetto ai lavori, certe dinamiche assumano una maggiore comprensibilità.

L'intersezione delle aree lascia spazio all'ipotesi che il telefono sia rimasto all'interno dell'appartamento, sebbene tutte le informazioni utilizzate siano ricadute nell'ambito di stime puramente teoriche e semplificate, con nefaste implicazioni a livello dibattimentale.

SECONDO CASO (percorso comune)

Quesito: partendo dall'analisi delle celle verificare se due soggetti A e B, erano insieme mentre percorrevano un determinato percorso (o analogamente se due telefoni erano in uso alla stessa persona) o hanno effettuato due itinerari differenti;
Soluzione: i due telefoni erano insieme.

I° *STEP* DI ANALISI

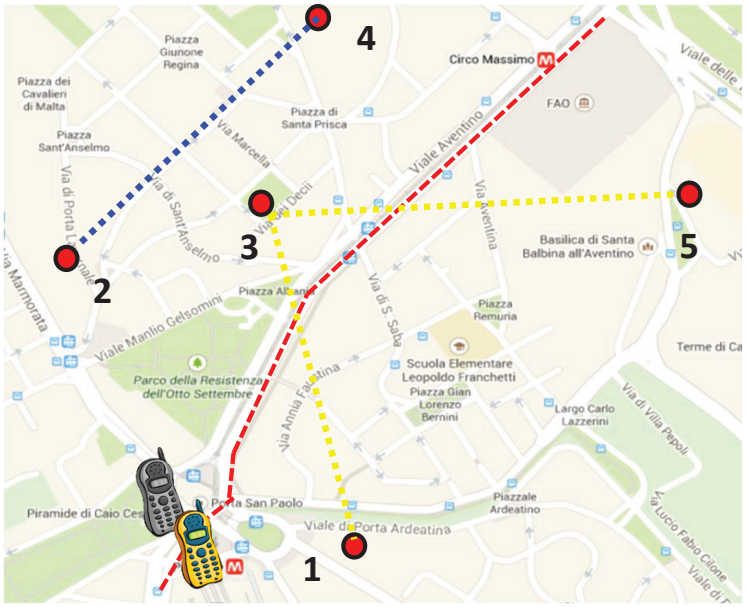
Anche in questo secondo caso il ricorso alla rappresentazione tabellare degli eventi di traffico, seppure corredati con gli indirizzi di cella, fornisce un risultato che potrebbe fuorviare la reale dinamica. Infatti A e B agganciano celle apparentemente differenti.

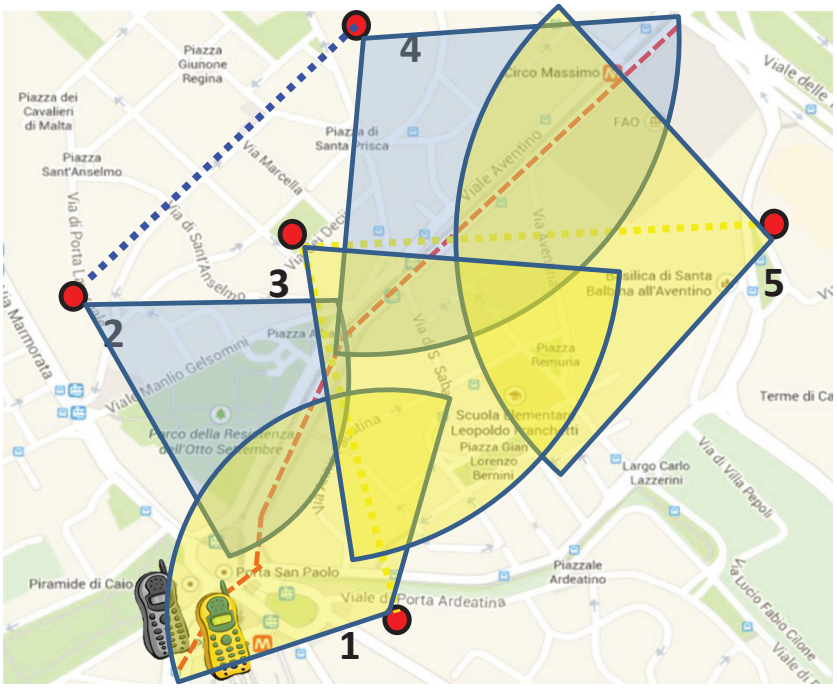
Di nuovo l'errore di ricorrere alla considerazione della cella come entità puntuale senza l'apporto di una rappresentazione immediata e fingibile dei suoi connotati di direttività e area di influenza, non contribuisce alle logiche deduttive.

II° *STEP* DI ANALISI

Nuovamente, nel secondo *step*, viene implementata una rappresentazione cartografica dei soli indirizzi di cella ottenuti dai dati di traffico.

Nella figura l'utente A e B, rispettivamente i telefoni giallo e grigio, seppure effettuino entrambi fisicamente il percorso disegnato in rosso, sembrano effettuare percorsi distinti, blu e giallo, in relazione al fatto che i due rispettivi gestori erogano i rispettivi eventi di traffico su celle distinte e condizionate dalla visibilità e da ostacoli contingenti di volta in volta presenti sul percorso dei due terminali al momento in cui viene generato l'evento di traffico.





III° *STEP* DI ANALISI

Con lo *step* successivo, ottenuto georeferenziando le aree teoriche delle coperture delle celle impegnate nei diversi eventi di traffico, si evince che le celle agganciate da A e B coprono di volta in volta le stesse aree di territorio.

L'estrema semplicità del caso rappresentato fa pensare ad una maggiore leggibilità degli eventi nella direzione del reale svolgimento delle dinamiche di movimento dei due terminali. La rappresentazione bidimensionale e statica delle aree coperte dalle celle però non consente di applicare considerazioni circa le sequenze e le effettive simultaneità o prossimità temporali dei singoli eventi di traffico, inducendo ulteriori margini di errori quando l'analisi richiede la considerazione fluida e simultanea delle posizioni reciproche di più terminali.

Giova sottolineare che, con riferimento allo *step* 3 di entrambe le casistiche analizzate, le rappresentazioni finora utilizzate sono delle semplificazioni teoriche di aree di copertura che non tengono in considerazione l'orografia del suolo, la presenza di fabbricati ed elementi interferenti fisici ed elettromagnetici tali da poter modificare, talvolta anche sensibilmente, l'effettiva possibilità di aggancio di una data cella. ©