

Controllo della configurazione di impianti di telefonia mobile tramite smartphone

Il controllo degli impianti di telefonia mobile è un'attività istituzionale delle ARPA. In Toscana, anche sulla base della normativa regionale, oltre ai livelli di campo elettromagnetico, viene **verificata la corrispondenza tra configurazione autorizzata ed esercita**

La verifica dei sistemi in aria viene normalmente effettuata mediante **analizzatore di spettro vettoriale** equipaggiato con i moduli software per la decodifica degli identificativi delle celle (CID, PCI)

L'uso di uno smartphone Android equipaggiato con chipset **Snapdragon** e con privilegi di root consente tramite la funzione **band lock** e **App** disponibili nello store ufficiale di identificare i sistemi e le bande attive nei settori delle Stazioni Radio Base per telefonia mobile.

OBIETTIVO DELLO STUDIO

valutare la possibilità di **utilizzare uno smartphone commerciale** come **strumento portatile e low-cost**

Per il sistema **LTE**, l'identificazione della cella principale a cui lo smartphone è connesso è possibile tramite il codice **ECI** (**E-Utran Cell Identifier**) formato dall'identificativo della Stazione (eNodeB) e da quello della cella (banda di trasmissione + settore della Stazione). Nell'App mostrata a fianco il codice ECI è indicato con **ECelld** nella forma **eNodeB/Banda+Settore**. Il codice ECI **identifica la cella univocamente nella rete** che viene invece individuata, nel livello fisico, dal codice **PCI** (**Physical Cell Identity**)

Nell'esempio, le **bande B20 (800MHz) e B01 (2100 MHz)** sono **presenti** nel settore indagato della Stazione. Nell'**ECelld**, infatti, l'**eNodeB** rimane **costante (56076)** come pure l'**ultima cifra del codice (3)** a dimostrazione dell'appartenenza al terzo settore. Varia al contrario la **banda utilizzata** (1 per la B20 e 4 per la B01 nella codifica del gestore). Al contrario, la banda **B28 (700 MHz) non è presente** nel settore indagato: l'**eNodeB (59221) risulta variato** rispetto a quello delle bande descritte in precedenza e i **valori del segnale ricevuto (RSRP, Reference Signal Resource Power) risultano decisamente inferiori** (<-110 dBm) rispetto a quelle delle celle presenti (compresi tra -65 e -80 dBm). I risultati ottenuti con l'App sono confermati da quelli forniti dall'analizzatore vettoriale (PCI individuati e relativi livelli di RSRP)

Il sistema **5G** è attualmente implementato in modalità **NSA (Non Stand Alone)** e necessita pertanto della rete **4G** per funzioni quali autenticazione, sicurezza ed handover. **Non è pertanto possibile effettuare il locking sul solo sistema 5G** ma occorre lasciare il sistema **4G** attivo. La presenza di una cella 5G nel medesimo settore della Stazione può essere dedotta dai **valori di RSRP dei beam** ricevuti. Nell'esempio (banda N78, 3700 MHz), tali valori risultano del tutto confrontabili, se non maggiori di quelli delle celle 4G presenti. La cella 5G con PCI 359 appartiene quindi allo stesso terzo settore della Stazione.

Scan Results (0 - 7)			
Cells (CC0)	Cell - 0	Cell - 0	Cell - 0
Frequency	3.649 GHz	3.649 GHz	3.649 GHz
PCI (C-S-G)	359-2-119	359-2-119	359-2-119
SSB Index	5	1	2
RSRP (dBm)	-78.453	-102.722	-106.444
RSRQ (dB)	-10.887	-14.506	-18.017
RSSI (dBm)	-54.555	-73.006	-75.416
SINR (dB)	18.696	-1.297	-6.413
PSS (dBm)	-78.434	-102.534	-107.610
SSS (dBm)	-78.451	-102.814	-107.798
DMRS (dBm)	-78.455	-102.672	-105.414
Freq Error (Hz)	21.582	21.582	21.582
Time Offset (us)	2445.573	2445.573	2445.573

Per il sistema **GSM** l'identificazione della cella si ottiene tramite il **Cellld** che comprende il **codice della Stazione e il relativo settore**. L'App consente di identificare anche BCCH e TCH utilizzate nella cella