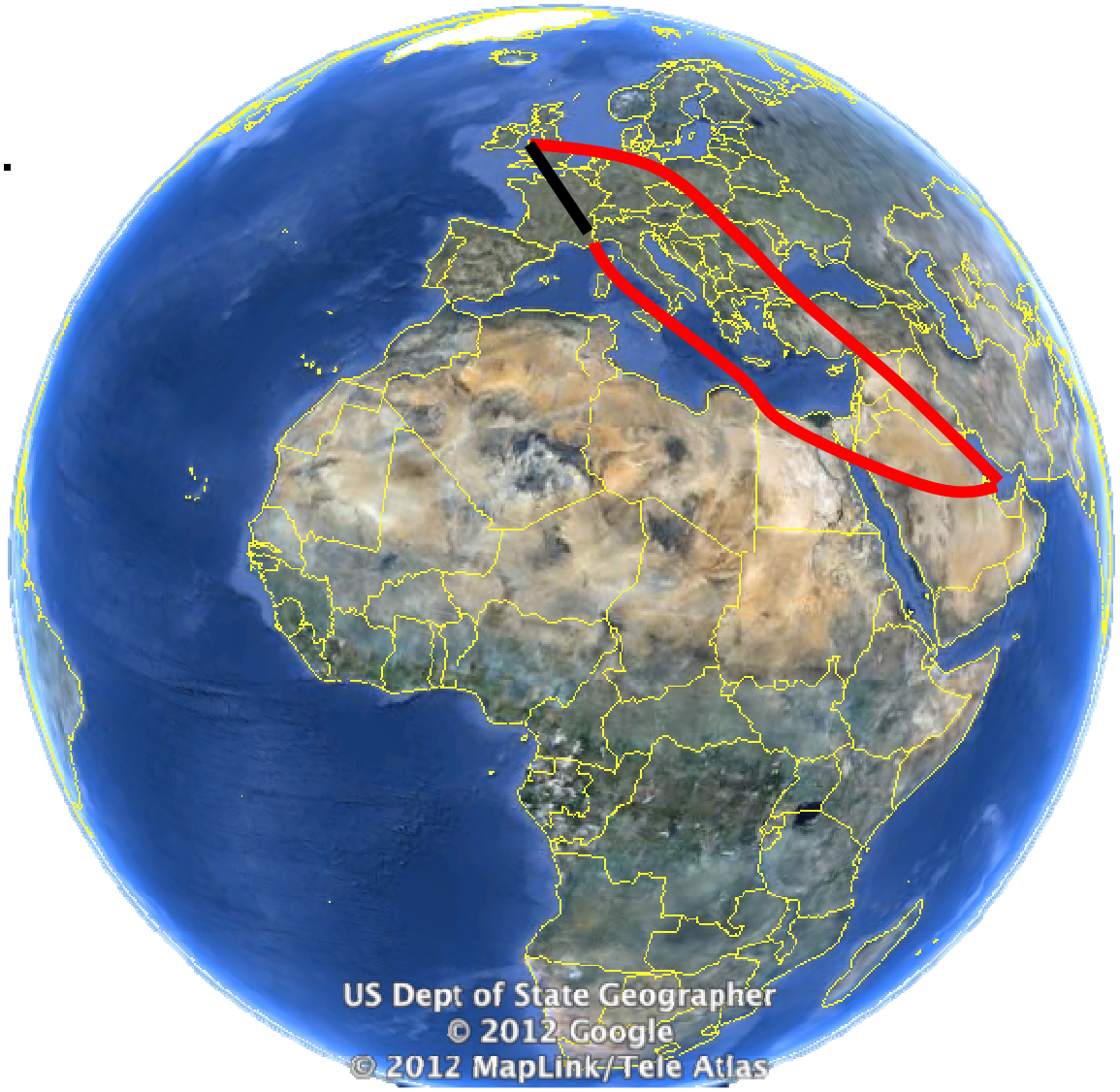
Un metodo efficace, a bassissimo costo, per il monitoraggio dell'esposizione a reti WLAN in ambienti ad alta complessità

Abel Rodríguez de la Concepción, Daniela Renga,
Riccardo Stefanelli, **Daniele Trinchero**

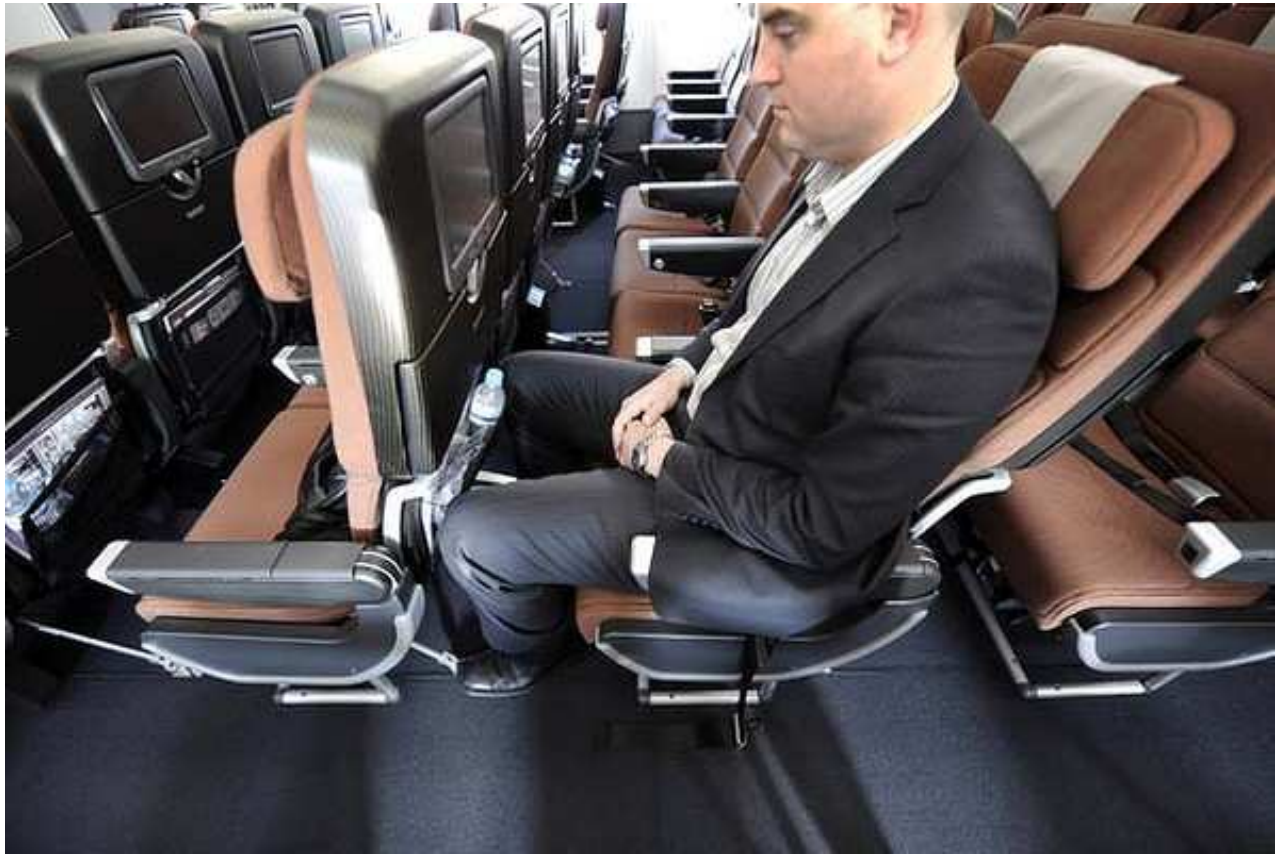
POLITECNICO DI TORINO

Antitesi Filosofica

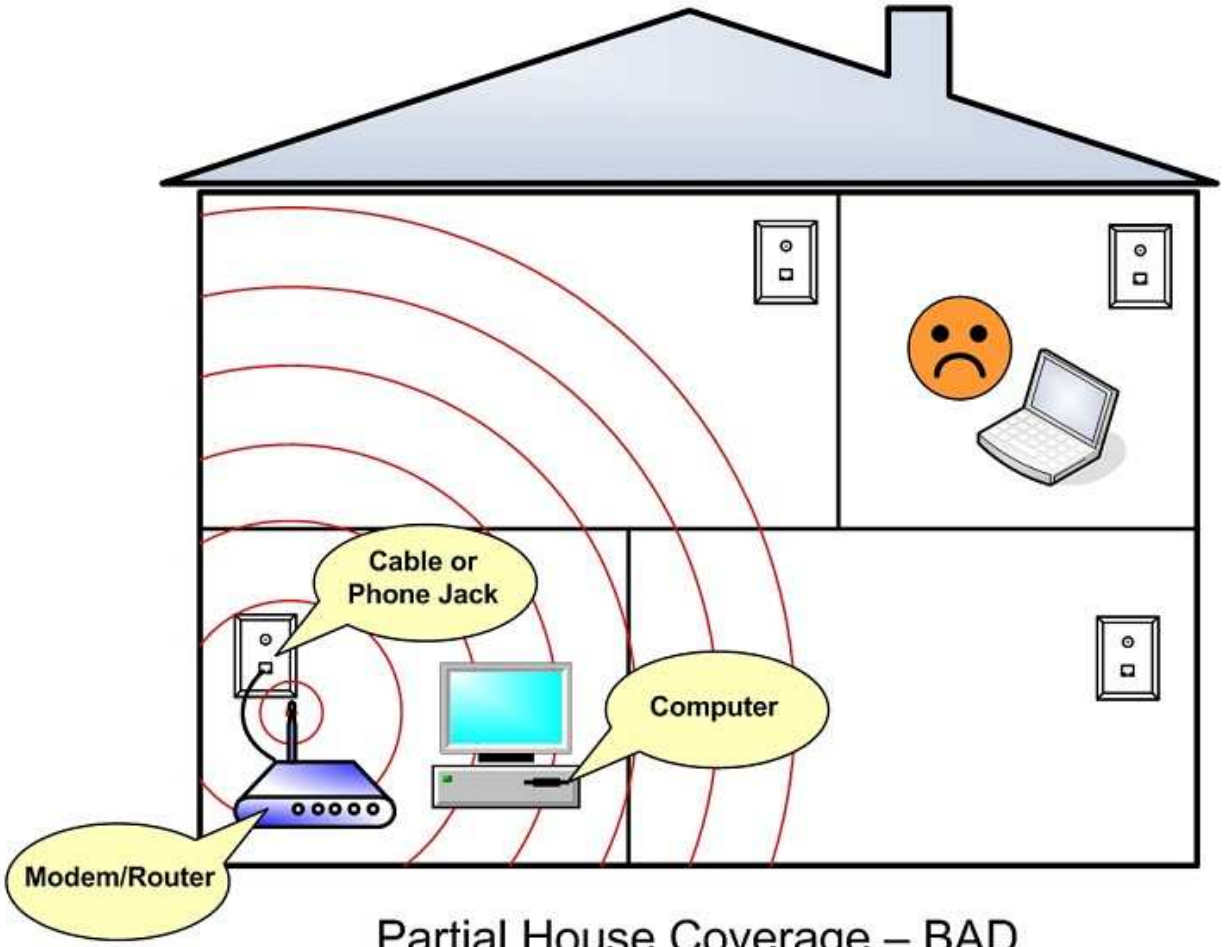


Antitesi Filosofica

Antitesi Filosofica

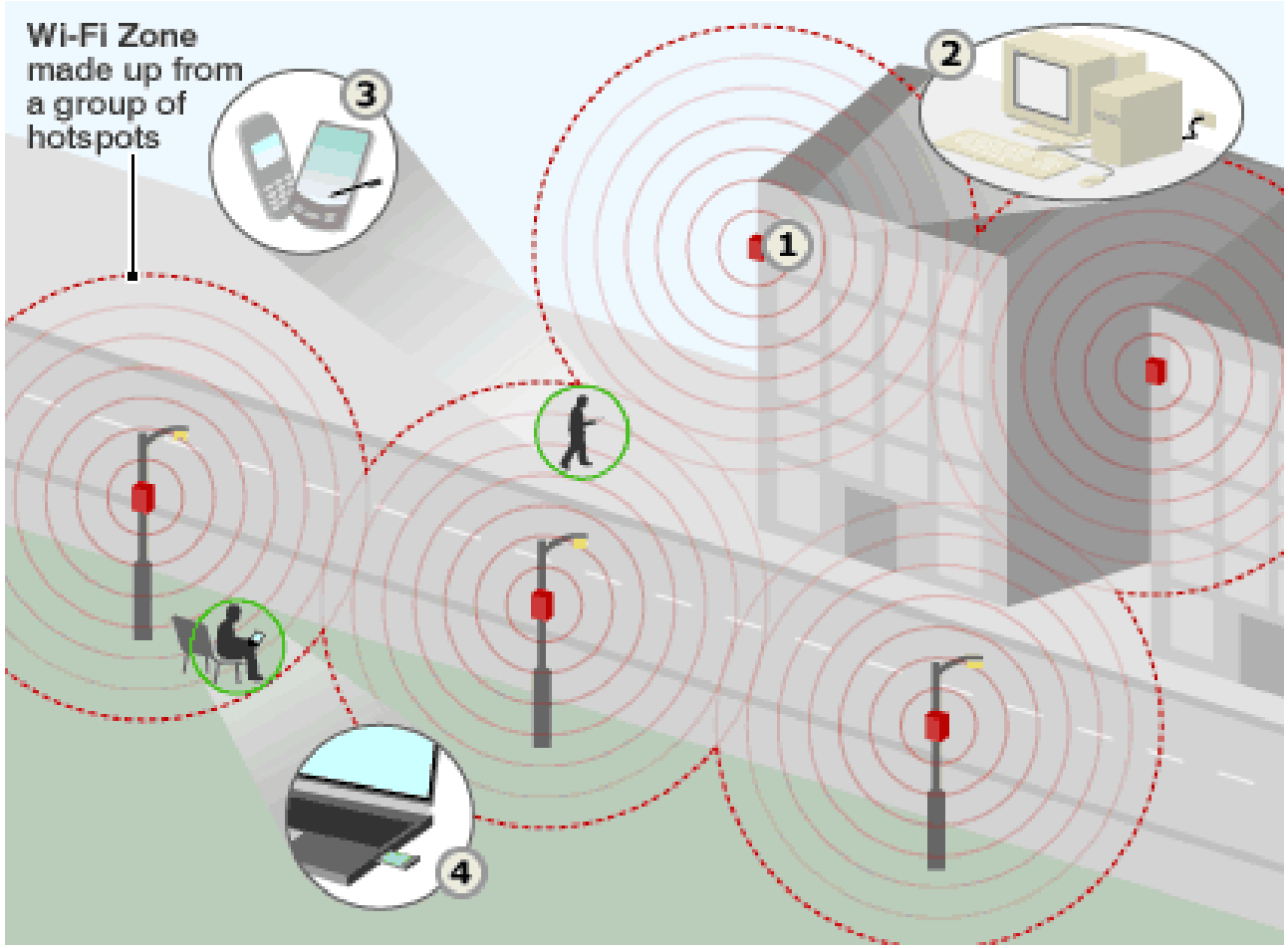


Wireless-Fidelity (Wi-Fi)

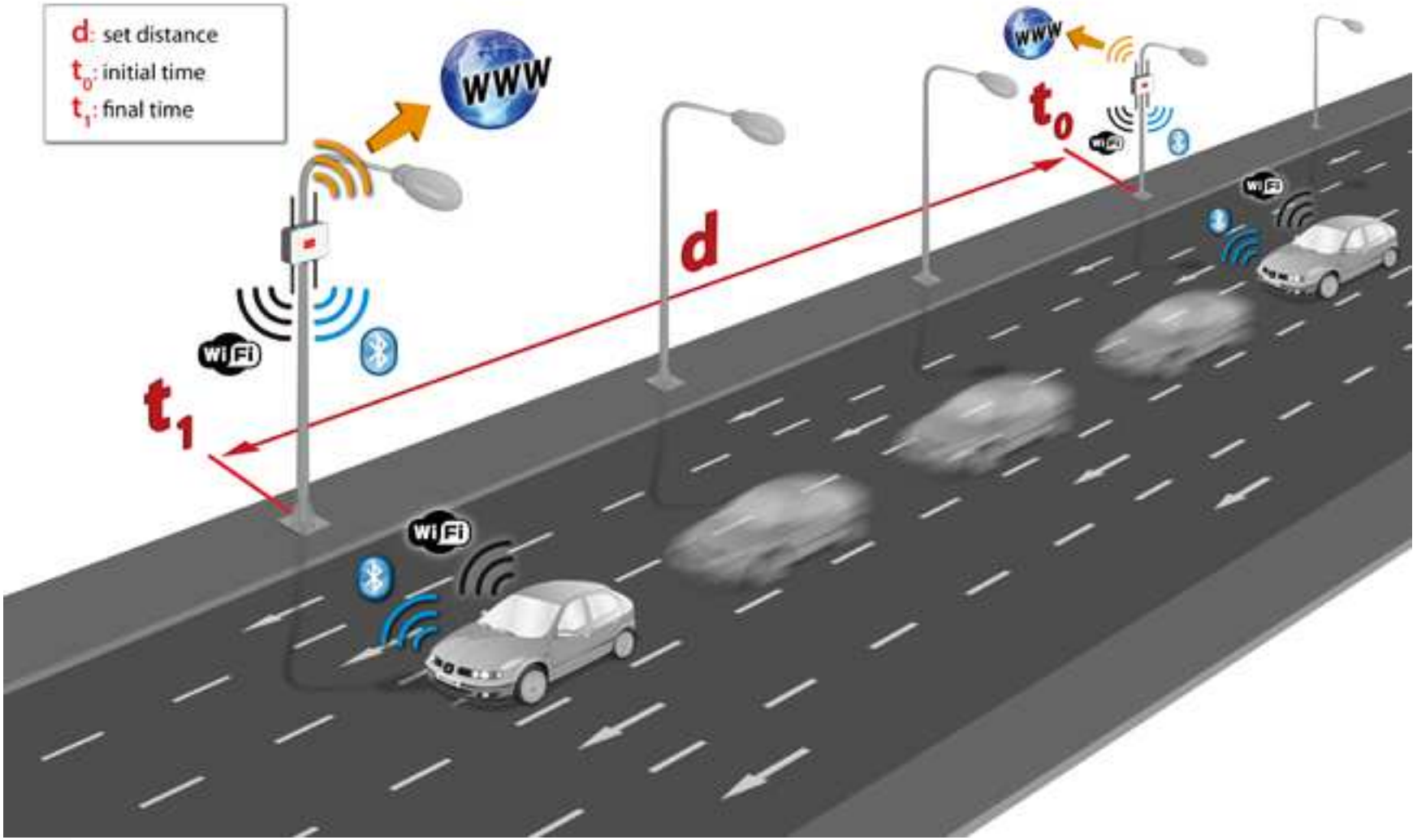


Partial House Coverage – BAD

Wireless-Fidelity (Wi-Fi)



Wireless-Fidelity (Wi-Fi)



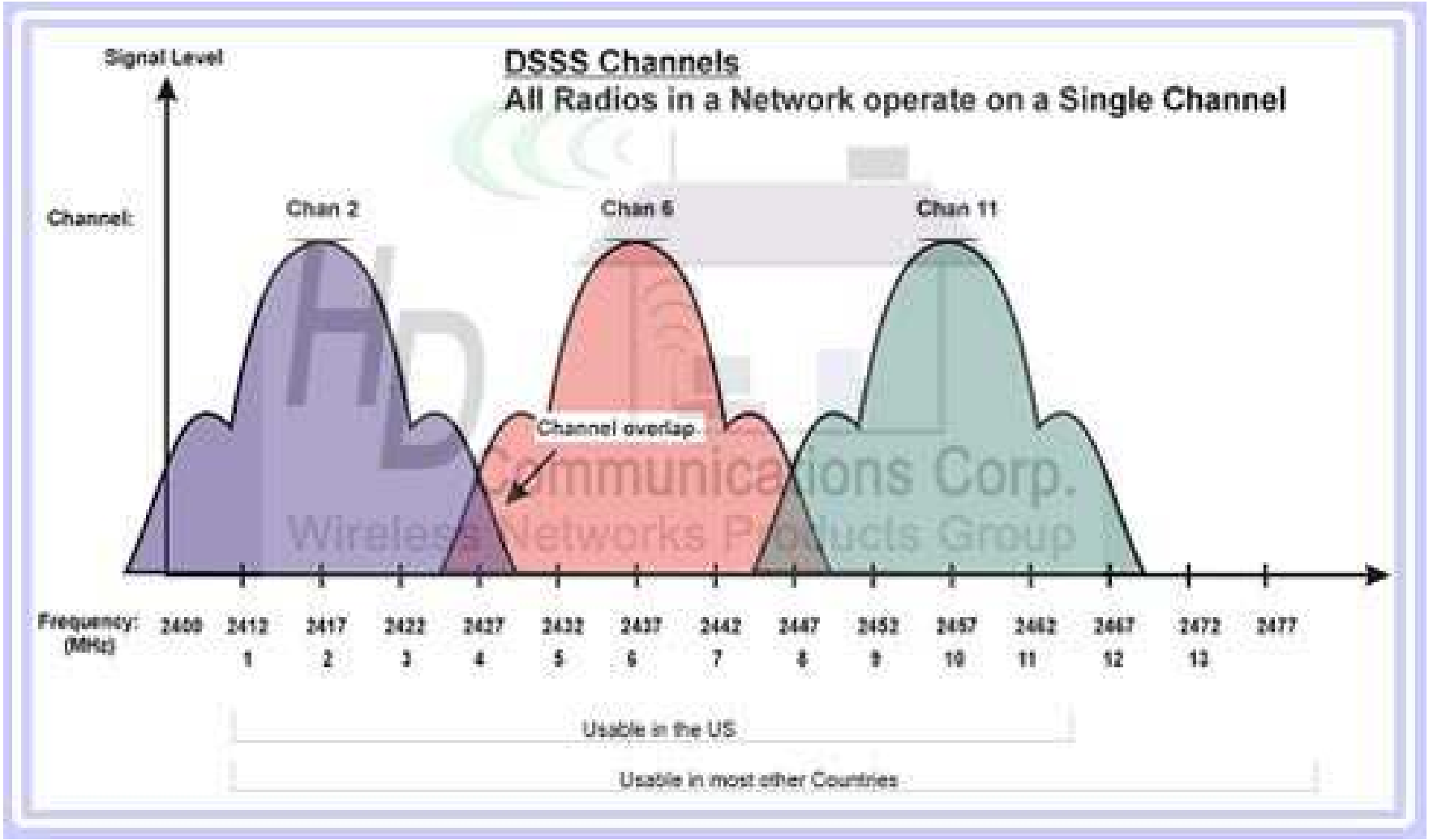
Wireless-Fidelity (Wi-Fi)

Wireless-Fidelity (Wi-Fi)

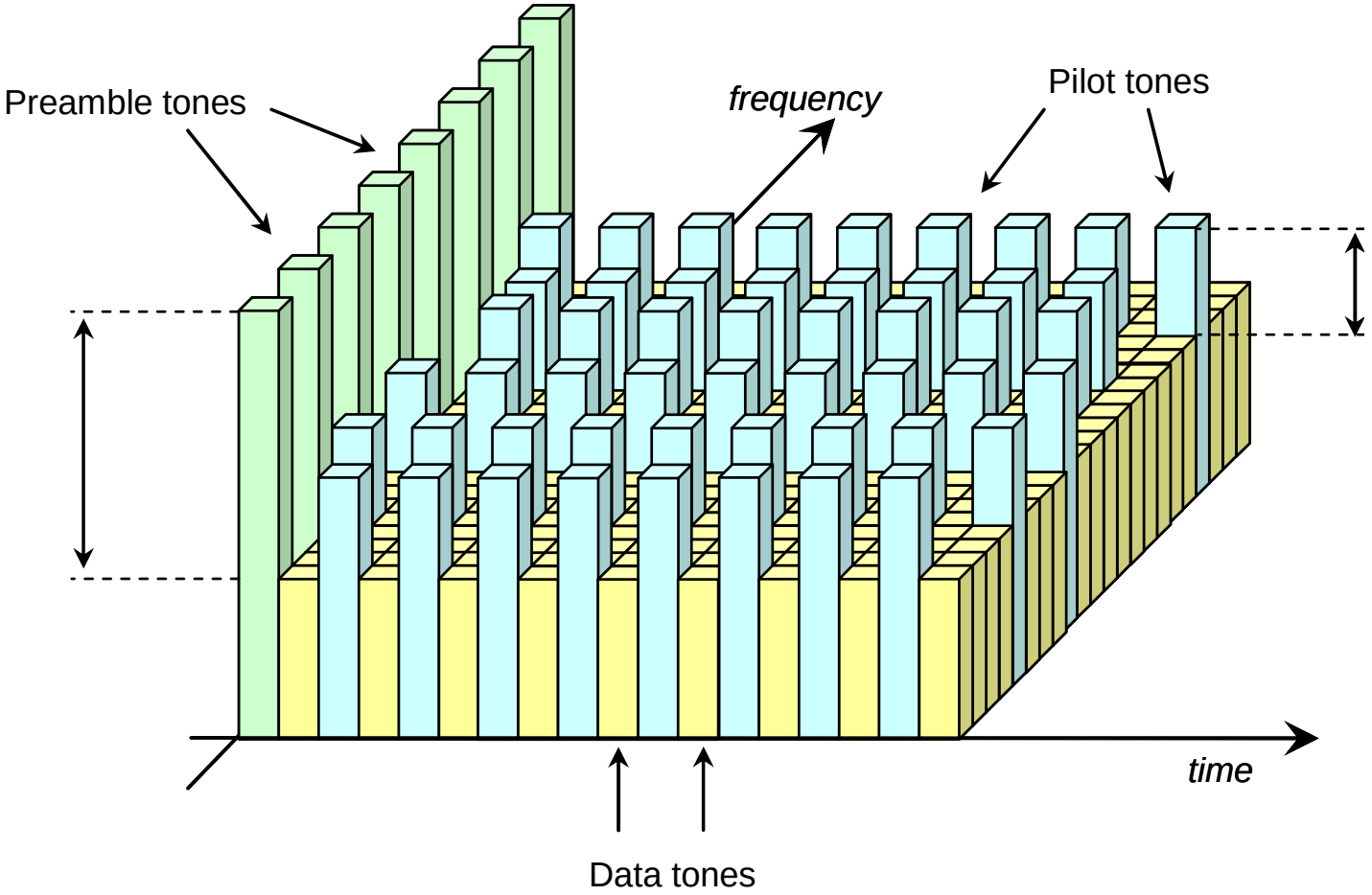
Evoluzione dello standard WLAN

Edizione	Data	Data rates [Mb/s]	Mod	Banda [MHz]	
802.11 1997	1997	1-2	HFSS	22	
802.11a	1999	6-12-18-24-36-48-54	OFDM	20	
802.11b	1999	5.5-11	DSSS	20	
802.11g	2003	6-12-18-24-36-48-54	OFDM	20	
802.11h		---		20	Hiperlan
802.11 2007	2007	---		20	= sum (a:j)
802.11n	2009	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	MIMO (4)	20, 40	
802.11 2012	2012	---			= sum(k:z)
802.11ac	?	Fino a 1GB/s	MIMO (8)	20,40, 80,160	

Spettro del segnale WLAN

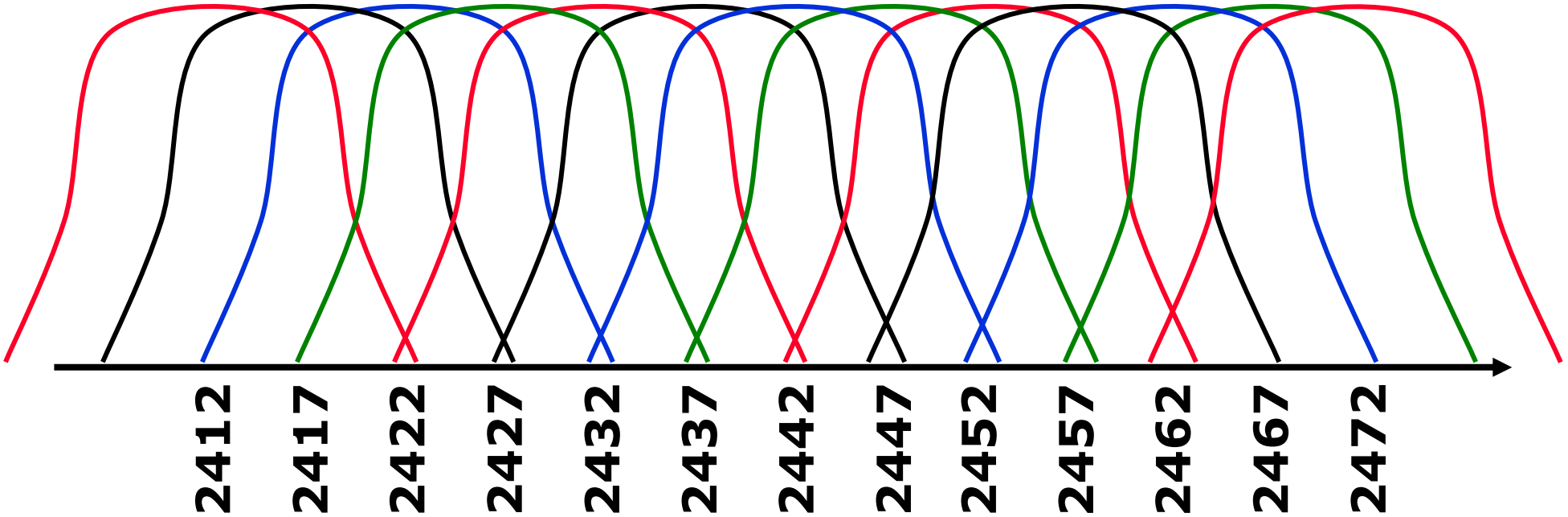


Spettro del segnale WLAN



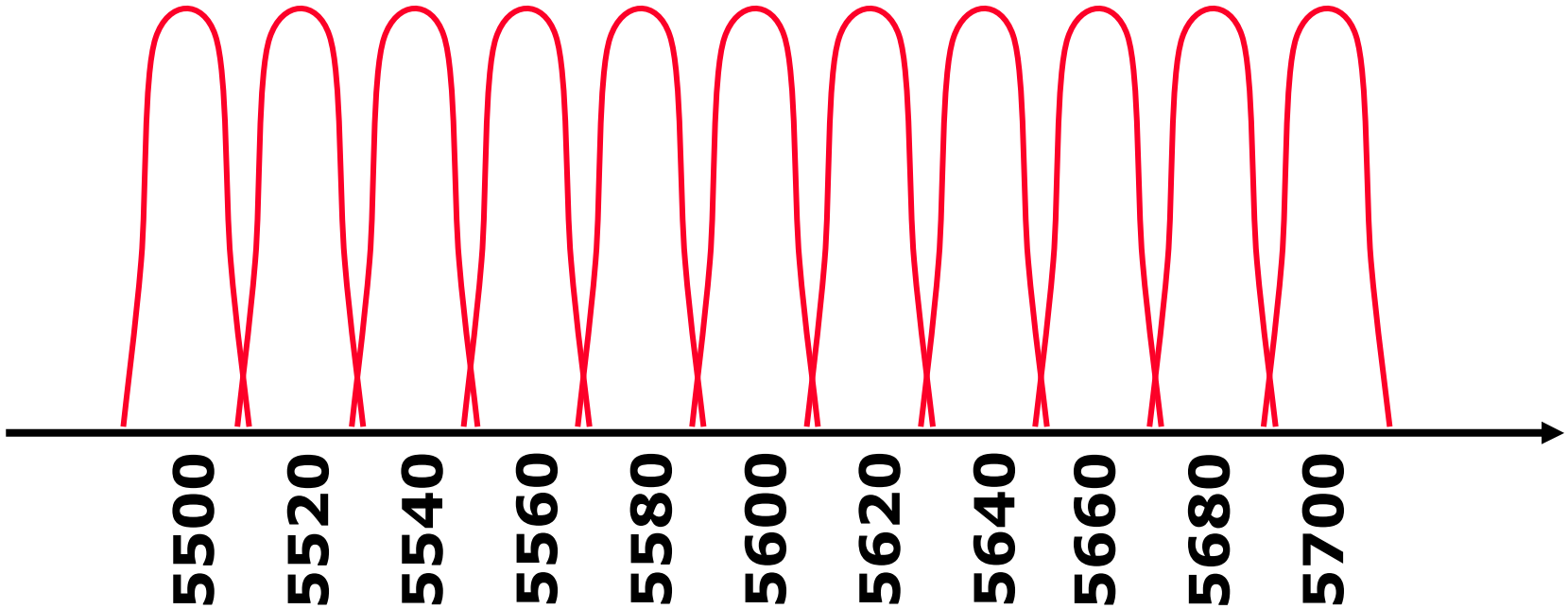
Separazione dei Canali

RadioLan Bandwidth

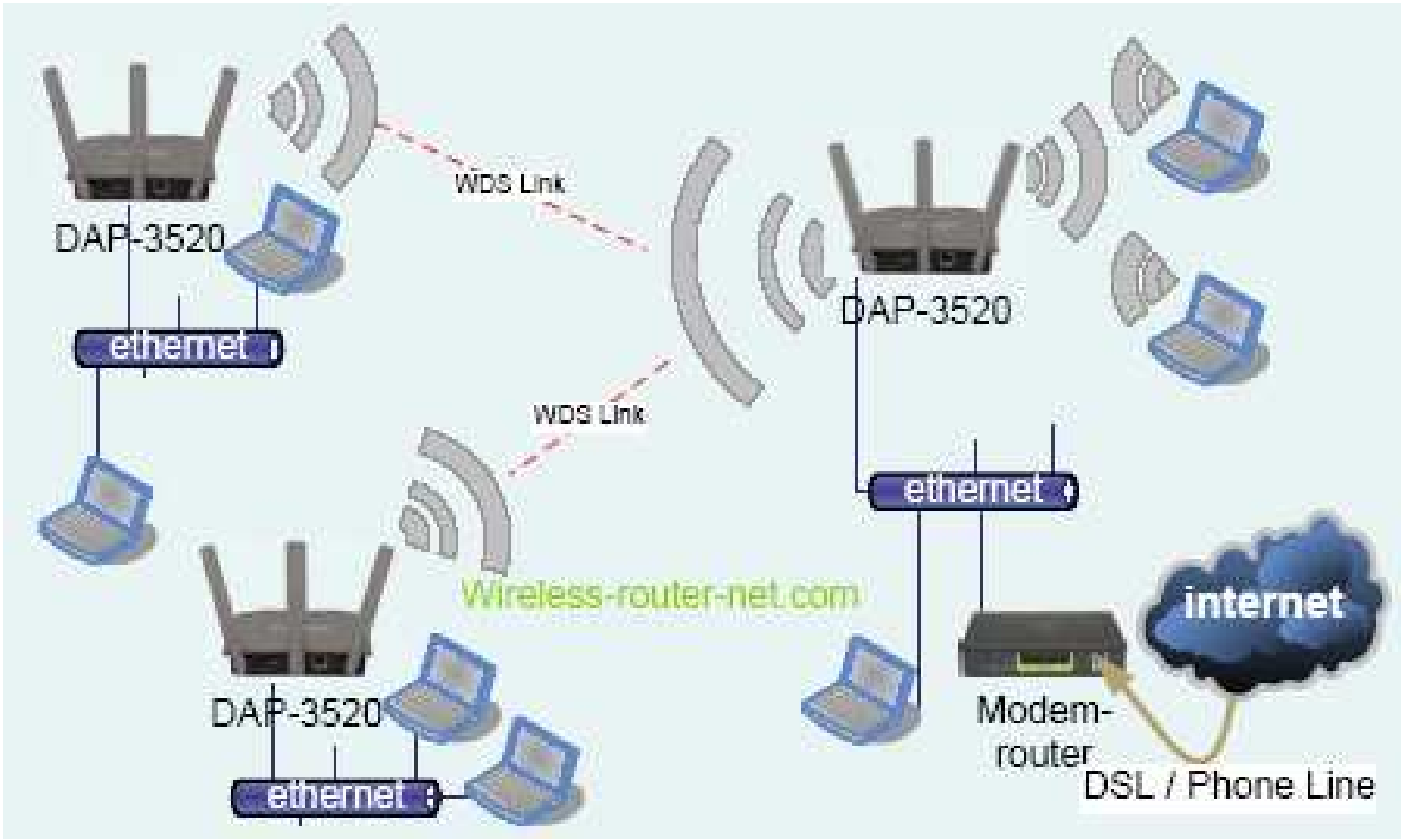


Separazione dei Canali

HiperLan Bandwidth



Interferenza diffusa



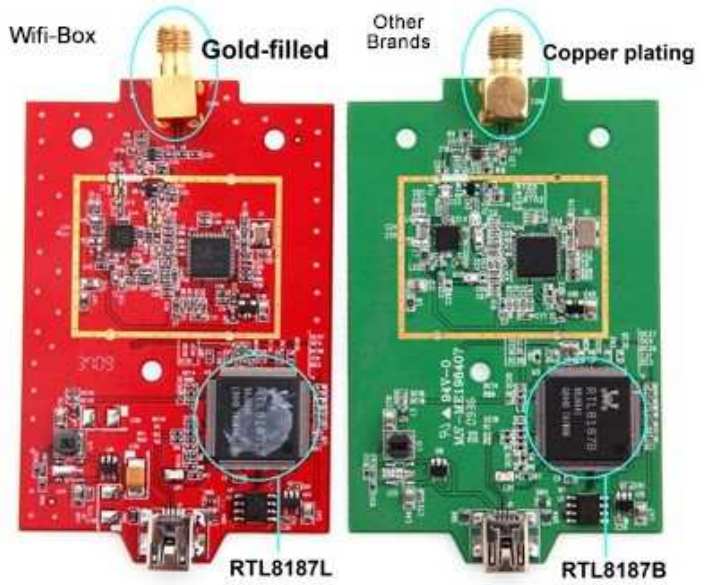
Interferenza diffusa

- **Access Points e Stations condividono lo stesso E-SSID, la stessa frequenza, la stessa banda di segnale**
- **Le Stations non sono governabili**
- **Le Stations non governate generano interferenza su TUTTA la banda Radiolan o Hiperlan: provano ad "ascoltare" tutti i canali**
- **Le Stations trasmettono a massima potenza in fase di "cerca"**
- **Gli Access Points che non hanno Stations agganciate non sono immediatamente rilevabili (trasmissione sporadica)**

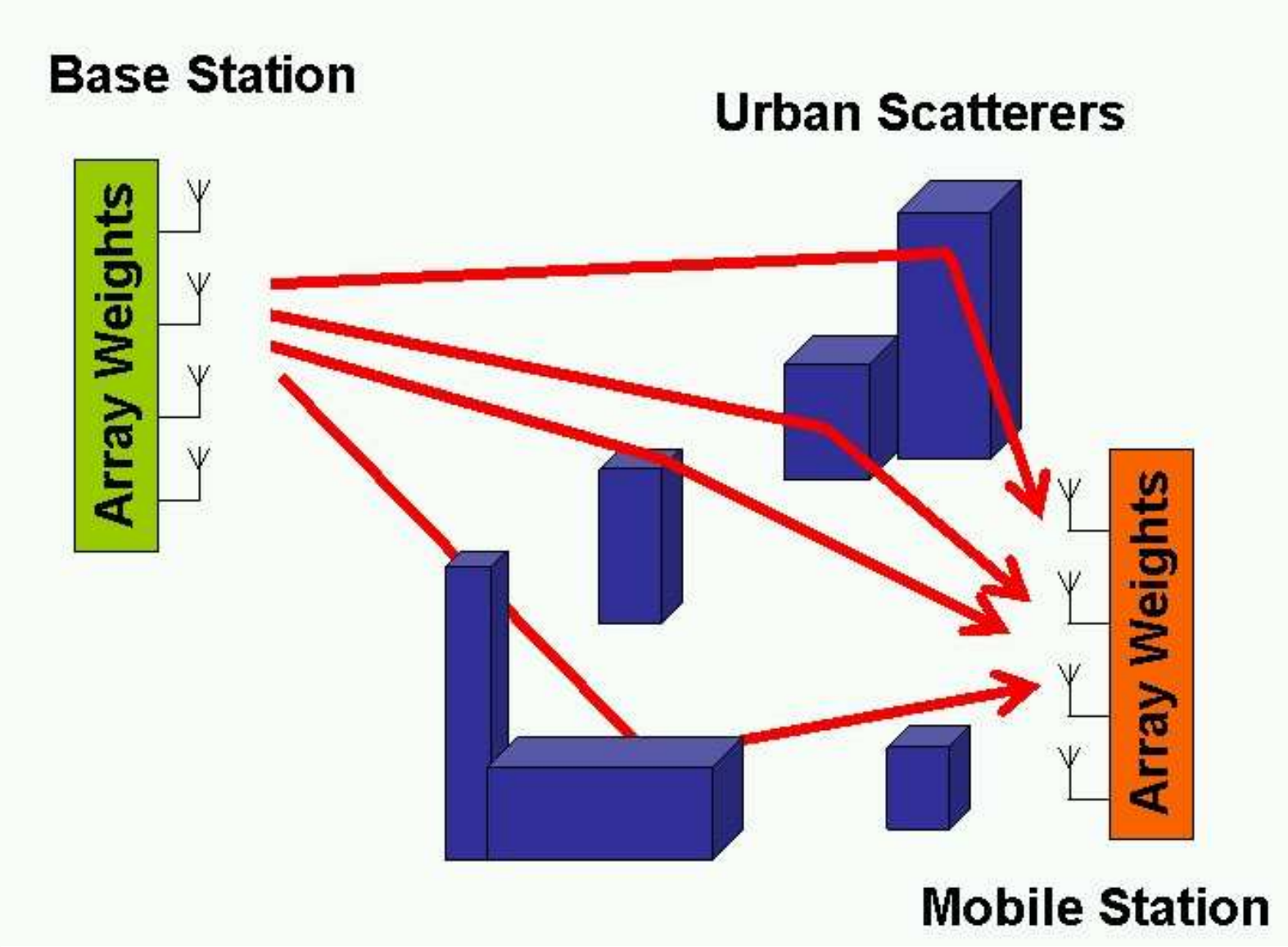
Interferenza diffusa

- **Stations e Access Points possono essere contemporanei**
- **Le Stations possono influire la misura in modo casuale e solo un'analisi attenta permette di rilevarle**
- **Gli E-SSID possono essere nascosti**
- **Access Points lontani possono trasmettere con potenza "superiore" al consentito**

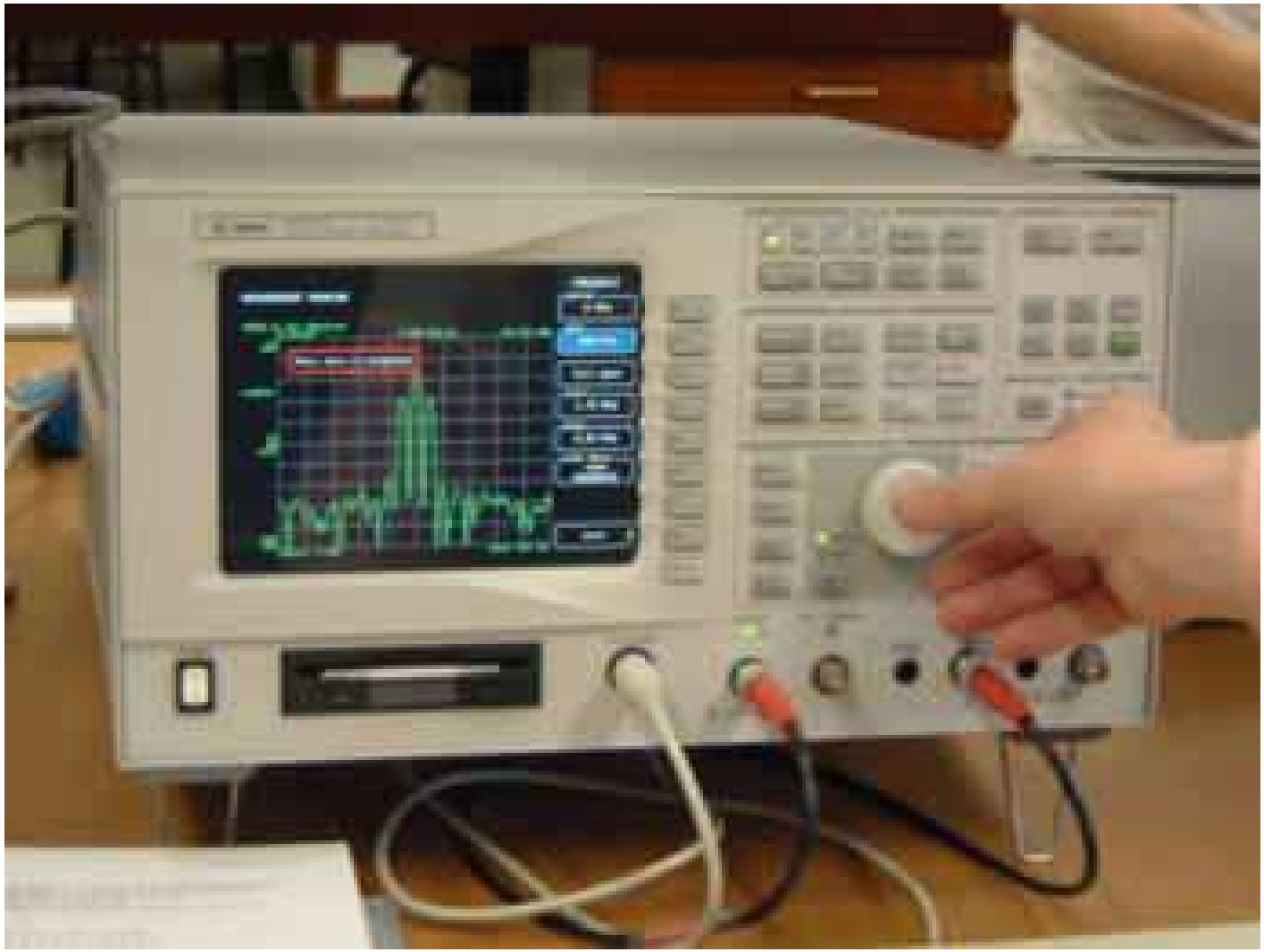
High Power Wi-Fi



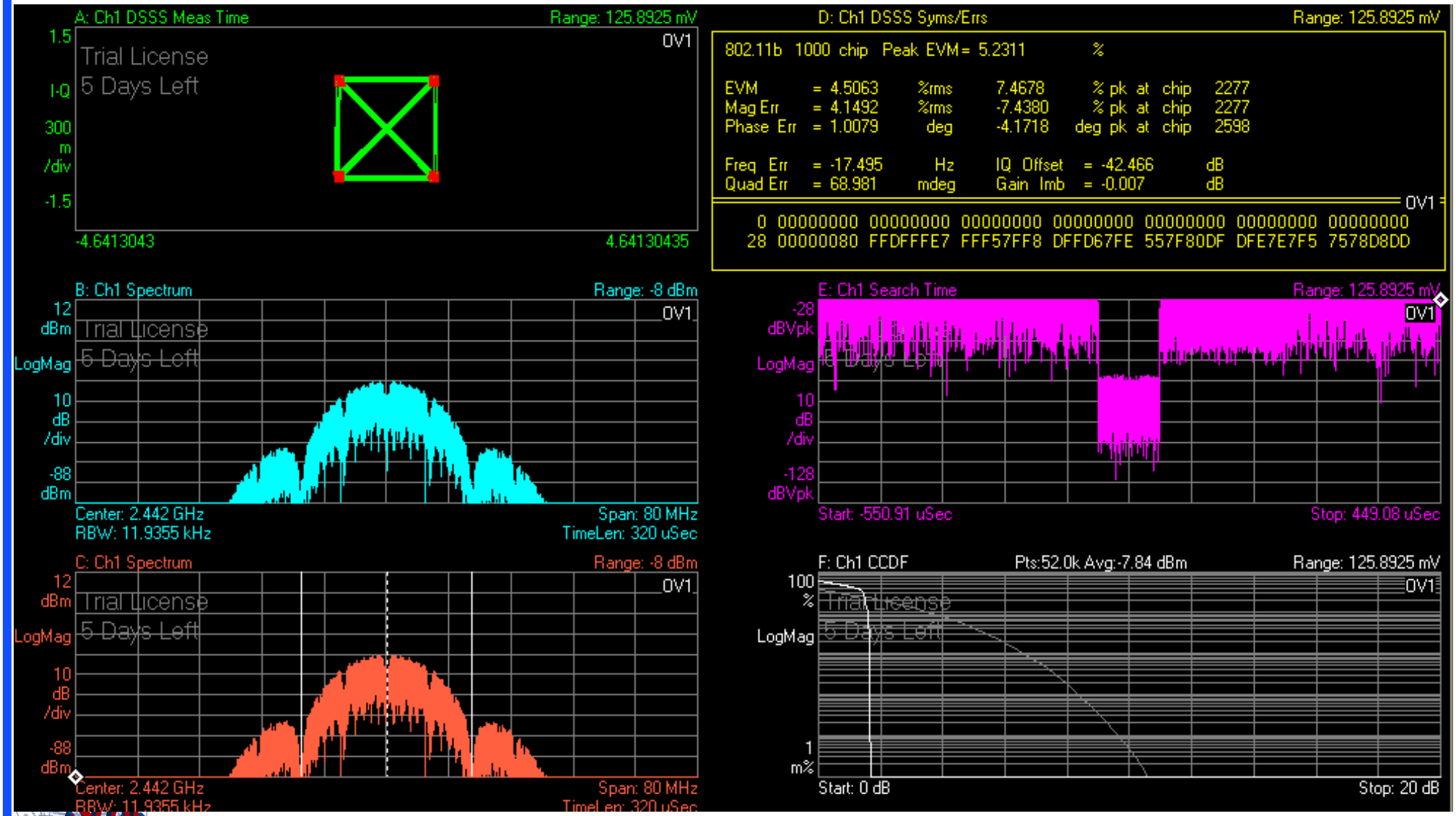
Diversità di spazio e di polarizzazione



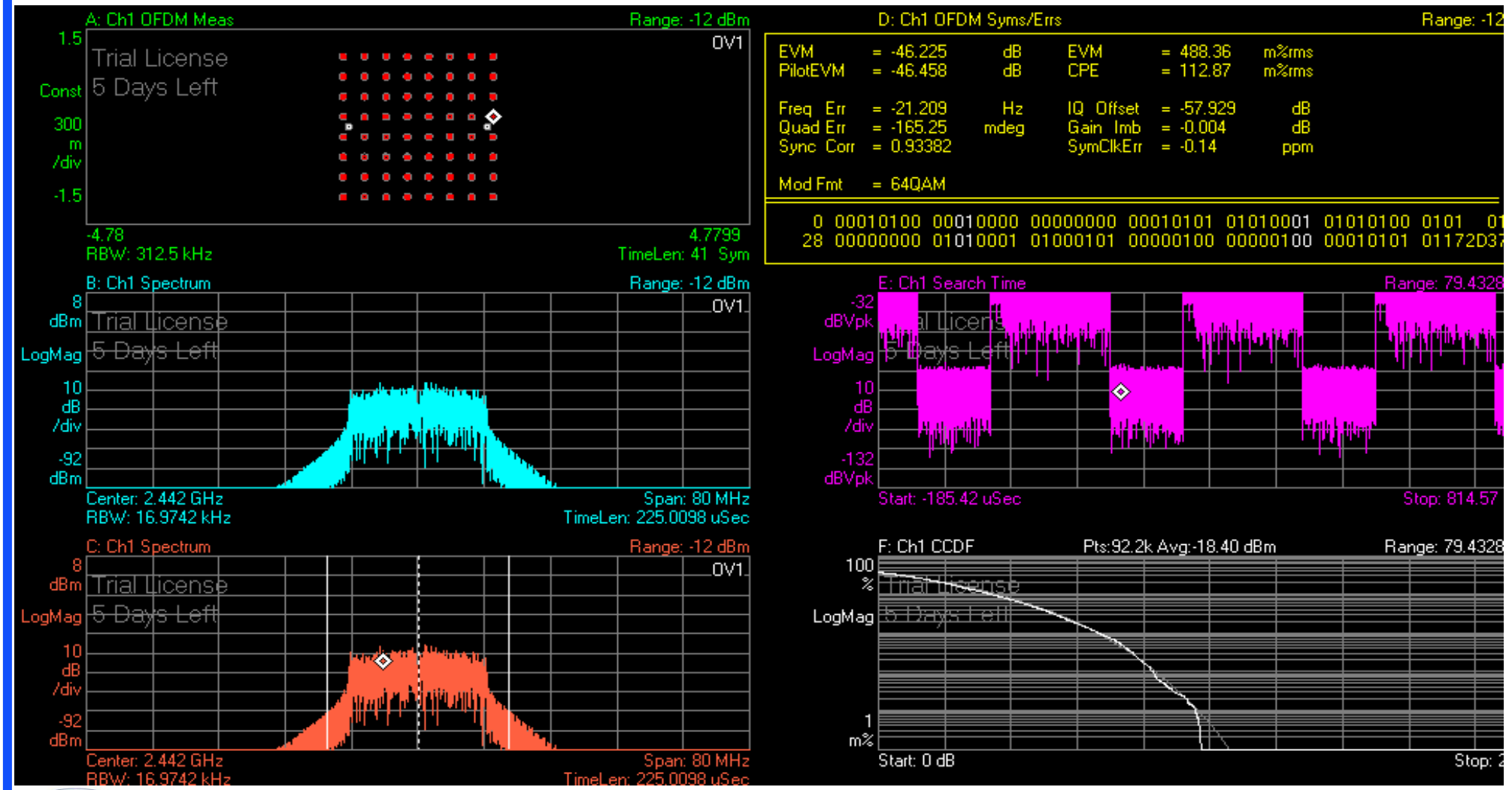
Analizzatore vettoriale di segnali



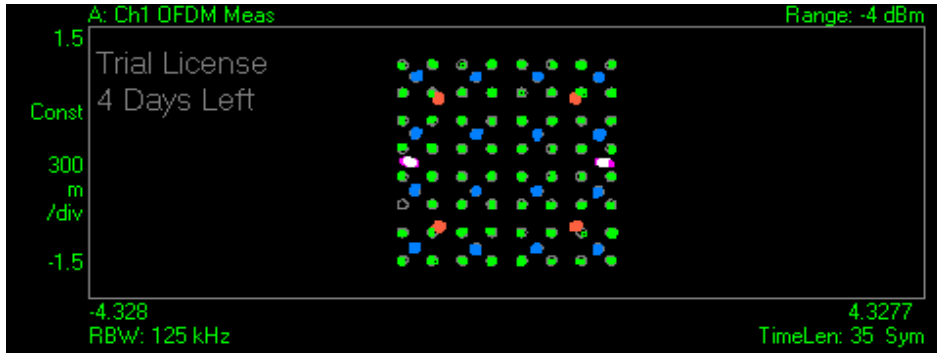
IEEE 802.11b measurements

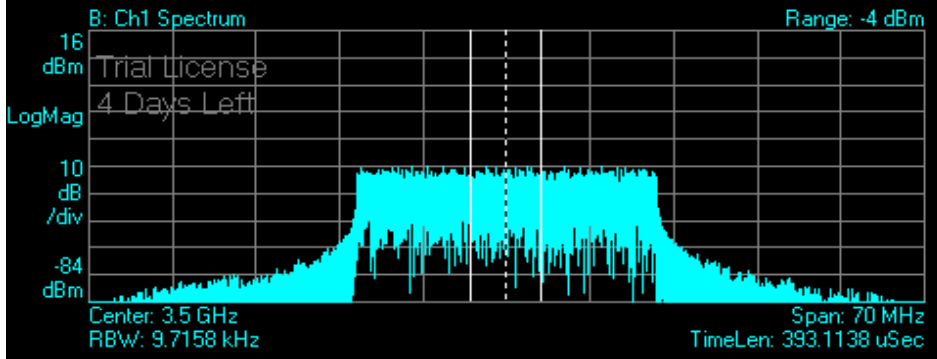


IEEE 802.11a measurements



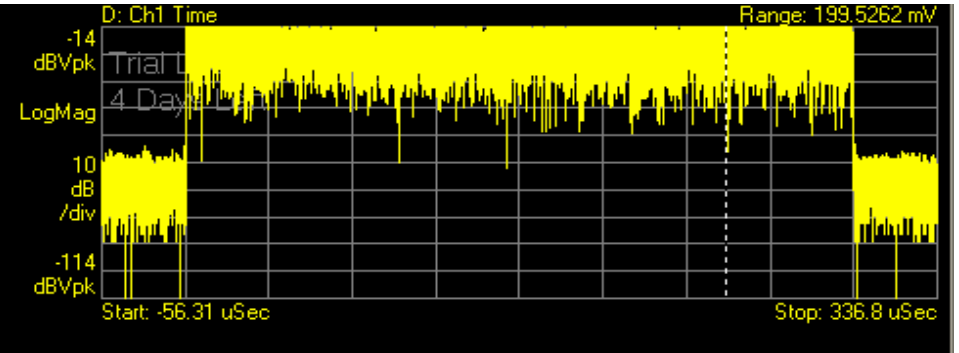
IEEE 802.11g measurements

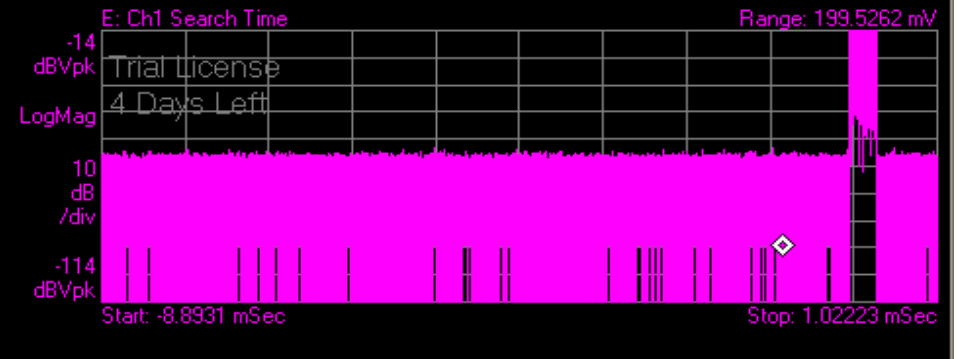


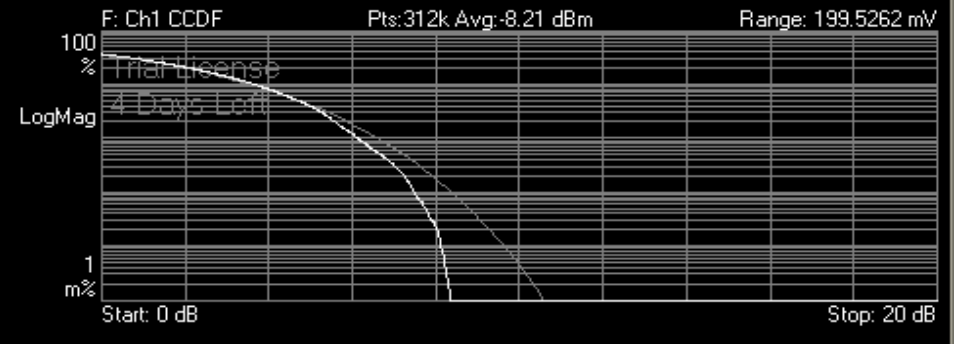


C: Ch1 OFDM Subframe Info — Range: 199.5262 mV

	ModFmt	Len(sym)	Pwr(dBm)	RCE(dB)
Pmbl	QPSK	2	-5.4931	***
	BPSK	1	-8.3653	-34.082
	BPSK	18	-8.3631	-33.456
	BPSK	1	-8.3875	-35.889
	BPSK	1	-8.3927	-36.468
	64QAM	1	-8.7081	-34.975
	64QAM	1	-8.5978	-34.554
	QPSK	5	-8.3449	-34.159
	16QAM	4	-8.3797	-32.534
	64QAM	3	-8.6424	-34.894
	***	37	-8.1849	-33.733



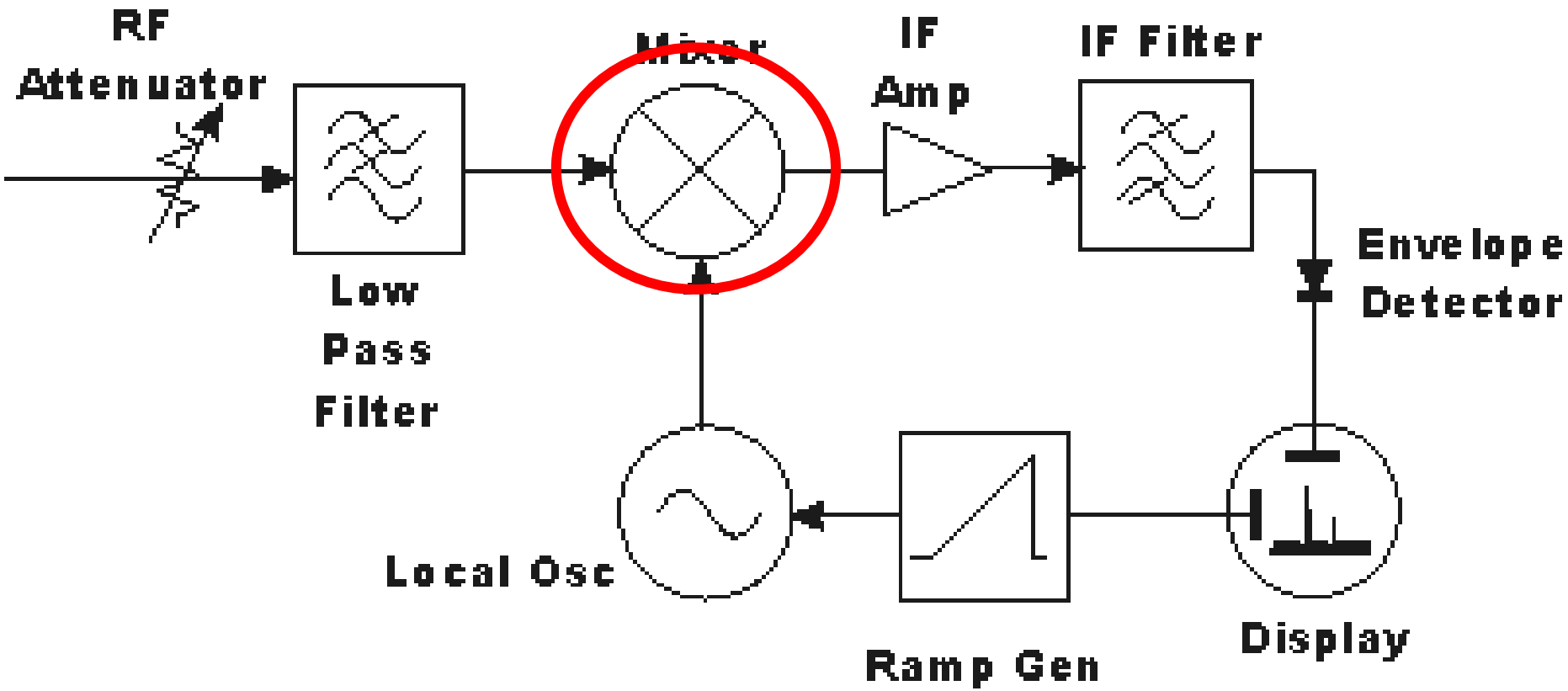




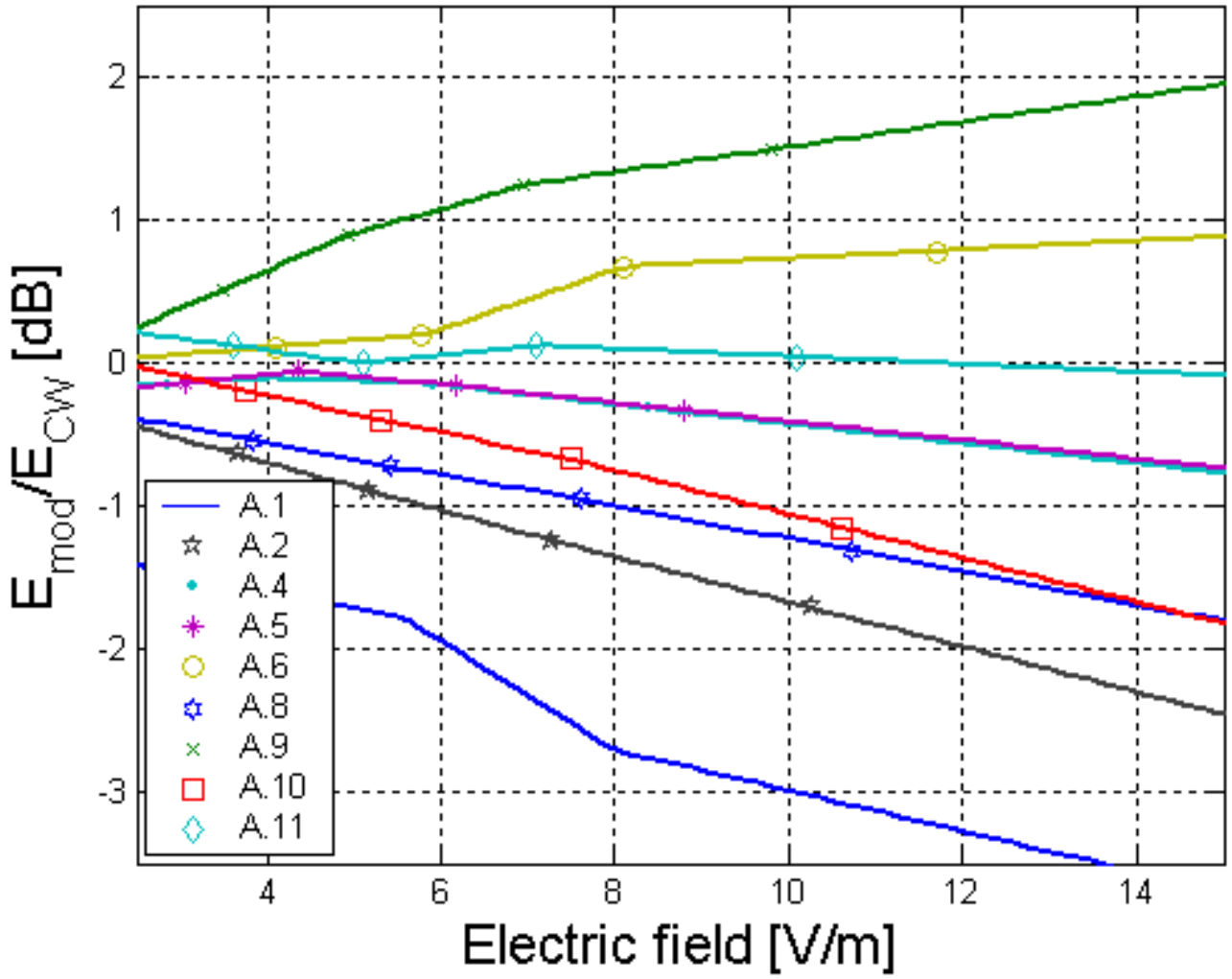
La demodulazione Vettoriale

- **Analisi dei Livelli Fisico e Mac con grande precisione**
- **Richiede una conoscenza approfondita dello strumento**
- **Strumenti costosi e di difficile trasporto**
- **Strumenti di non immediata applicazione**
- **Difficoltà ad implementare sweeps in frequenza meccanizzati**
- **Tempi di analisi normalmente lunghi**

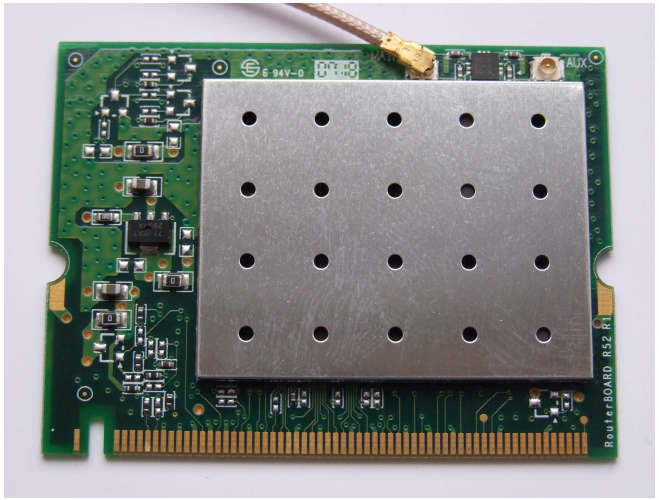
Filtraggio



Errore potenziale con misuratori a banda larga



Il chip-set Wi-Fi



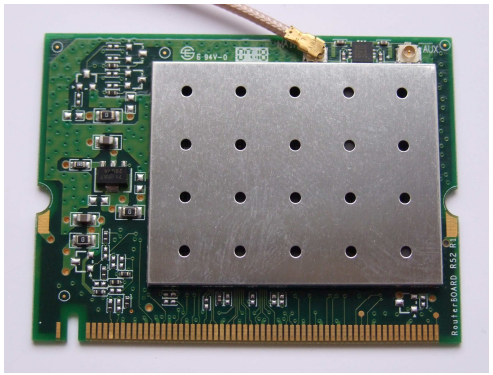
Il chip-set Wi-Fi

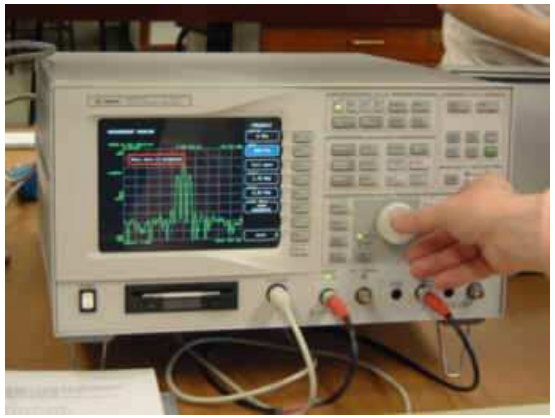
- **Riconosce gli identificativi di rete: E-SSID, B-SSID**
- **Esegue il monitoraggio delle reti presenti**
- **DEVE demodulare qualsiasi segnale WLAN, indipendentemente dallo standard**
- **Misura la potenza associata alle reti, verificando qualsiasi trasmissione di codice:**
  - **i beacon**
  - **il traffico dati**
  - **i segnali di controllo**
  - **i sincronismi**
- **Riconosce le Stations, associate e non associate**

Il chip-set Wi-Fi

- **Ha grande sensitività**
- **La massima banda in ingresso sul mixer è pari alla sola banda occupata dai segnali Wi-Fi**
- **Riconosce le interferenze e non le conteggia durante il calcolo della potenza associata al segnale principale**
- **Costa POCHISSIMO**
- **Lavora in tempo reale ed è naturalmente controllato da un PC (RISORSE LIMITATE)**
- **Tempi di analisi IMMEDIATI**

La soluzione





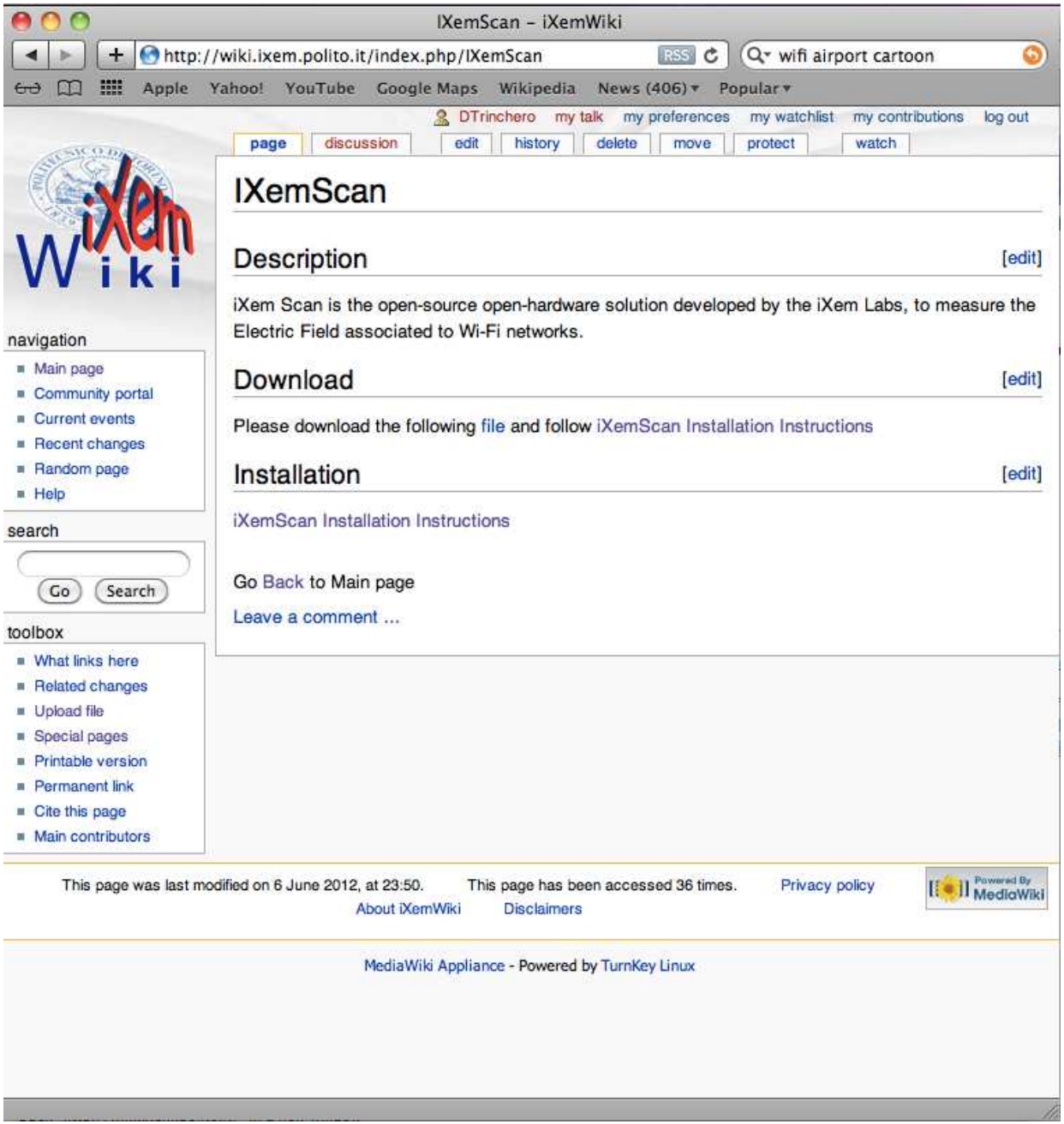
La soluzione

- **Costruiamo un router DEDICATO**
- **Utilizziamo un vecchio PC**
- **Oppure utilizziamo una scheda SBC**
- **Montiamo una radio Wi-Fi**
- **Installiamo un Sistema Operativo Open Source**
- **Costruiamo un'interfaccia grafica WEB per accedere alla macchina da QUALSIASI piattaforma senza alcuna LIMITAZIONE**

La soluzione

- **Costruiamo un firmware capace di impostare la radio in "monitoring mode"**
- **Definiamo i pacchetti "significativi" (beacons)**
- **Utilizziamo i pacchetti significativi come riferimento per la misura di potenza di segnale**
- **Programmiamo una scansione di canale**
- **Implementiamo i fattori di guadagno della catena di misura per trasformare la potenza in campo elettrico**

Troppa fatica???

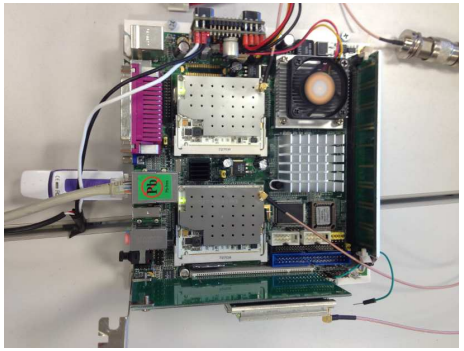


Valutazione di costo

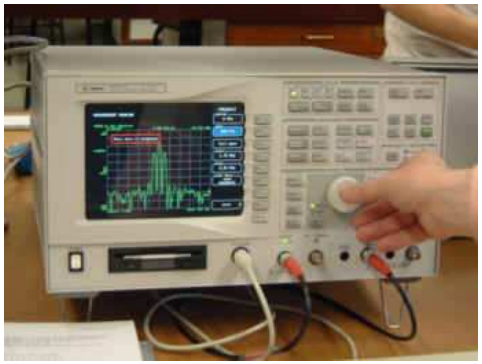
Wi-Fi Radio Card	**40,00 – 100,00 Euro**
SBC o PC	**80,00 – 200,00 Euro**
PigTail	**2,00 Euro**
Box (schermato)	**10,00 – 40,00 Euro**
Alimentazione PoE	**10,00 – 15,00 Euro**
Antenna	**COSTRUIAMOCELA**

Valutazione di costo

iXem Scan Single Pol — **140,00 – 300,00 Euro**



Analizzatore Vettoriale — **80.000,00 Euro**



Valutazione di costo

Aggiungo → **2 moduli radio**
2 pigtail

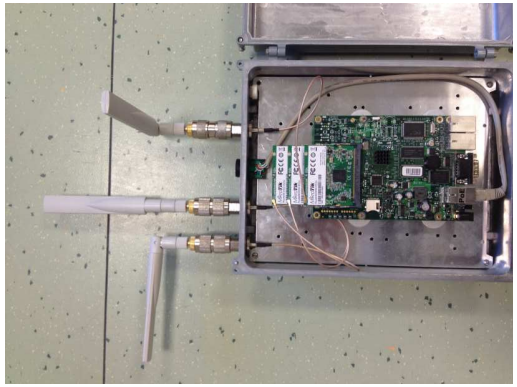
Costruisco uno strumento in grado di misurare le tre polarizzazioni del campo contemporaneamente

Ex, Ey, Ez

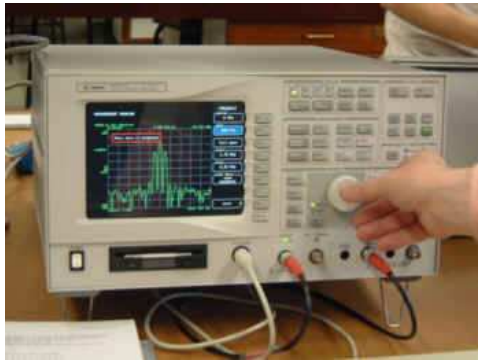
Valutazione di costo

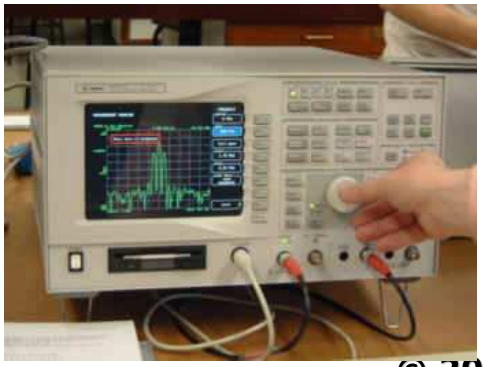
iXem Scan Triple Pol

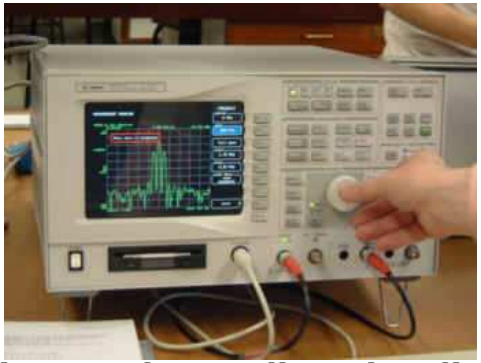
200,00 – 350,00 Euro



Analizzatore Vettoriale







Labs

Wireless anywhere, anyhow, anytime, for anybody

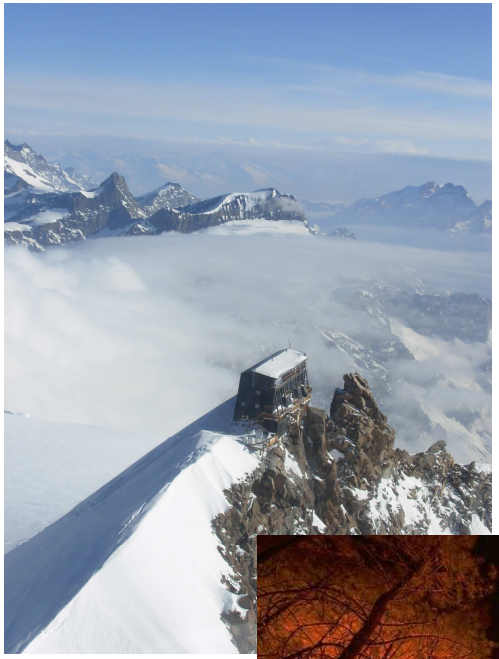
http://www.iXem.polito.it/

Labs

300 km at 30 MB/s spending something like 3 Euros

http://www.iXem.polito.it/

iXem Labs



Where you can't imagine to place an antenna, we (try to) DO

http://www.iXem.polito.it/