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

Rodríguez de la Concepción A., Renga D., Stefanelli R., Trinchero D.

iXem Labs – Politecnico di Torino
corso Duca degli Abruzzi 24, 10129 Torino,
info@iXem.polito.it

ABSTRACT - *L'obiettivo di questo lavoro consiste nell'assemblaggio, configurazione e messa in opera di un semplice strumento per la valutazione del campo elettromagnetico a radiofrequenza generato da reti WiFi, di bassissimo costo realizzativo, semplice utilizzo ma anche ottime prestazioni funzionali ed eccellenti caratteristiche in termini di precisione e di sensibilità di lettura. Lo strumento prevede inoltre la possibilità di discriminare i valori di potenza associati a diversi segnali WiFi, offrendo addirittura la separazione dei contributi irradiati dai punti di accesso rispetto a quelli delle stazioni utente associate alla stessa rete. Lo strumento può essere assemblato da chiunque abbia adeguate, ma non specifiche, competenze radioelettriche. Il software di monitoraggio può essere autocostruito con semplici passaggi, ma ne esiste una versione già disponibile, in forma open source, pubblicata sul repository Wiki del laboratorio iXem del Politecnico di Torino*

INTRODUZIONE

I dispositivi WLAN (wireless local area network) sia fissi (punti di accesso) che mobili (personal computers e smartphones) sono sempre più continuativamente oggetto di monitoraggio dell'esposizione, in considerazione di esigenze non necessariamente motivate dal punto di vista tecnico (le emissioni sono molto contenute), ma comunque utili per fornire una corretta informazione ai cittadini. Il monitoraggio, e in particolar modo la misura del campo elettromagnetico, tuttavia, sono resi complicati dalle caratteristiche di modulazione, digitale e banda larga, nonché dagli scenari tipici, che prevedono la presenza simultanea di diverse fonti di rumore/interferenza. Molto spesso, infatti, la misura è effettuata in un contesto operativo all'interno del quale sono presenti diversi reti WLAN: quella "generata" dal punto di accesso oggetto della misura, quelle generate da punti di accesso "terzi", a cui si sommano segnali generati da utenze dell'uno o degli altri. A differenza di quanto avviene per il broadcasting , dove le utenze non sono presenti, o per la telefonia mobile, dove le utenze utilizzano una banda di uplink separata, in una rete WLAN i punti di accesso e le utenze condividono lo stesso canale. Quando le utenze sono agganciate alla stessa rete, la trasmissione avviene in una successione temporale stabilita dal punto di accesso. In presenza di utenze agganciate a reti diverse, la non contemporaneità non è garantita, e nel caso di utenze "libere", in cerca di una rete a cui agganciarsi, la situazione è ancora più complessa, in quanto il canale di trasmissione è cambiato in continuazione. Infine, tra le bande utilizzate dalle reti WLAN, quella a 2.4 GHz è particolarmente critica, in quanto i canali hanno banda di frequenza pari a 16.6 MHz, ma passo di canalizzazione paria 5 MHz, e quindi canali diversi sono pure parzialmente sovrapposti.
È evidente che in un contesto come quello descritto, solo uno strumento in grado di isolare contributi irradiati da soggetti diversi permetta di effettuare una misura corretta. In fase di misura, è necessario distinguere tra rete e rete, tra utenze e punti di accesso, al fine di isolare il contributo del punto di accesso oggetto di misura, e quantificarne il segnale irradiato. L'unica soluzione praticabile è offerta dall'utilizzo di strumenti sofisticati, i demodulatori vettoriali, di costo molto elevato e non sempre trasportabili sul campo.

MISURA DI UN SEGNALE WLAN

Il contesto descritto richiede l'utilizzo di un demodulatore vettoriale, dispositivo di grande precisione, ma costo molto elevato. Difficilmente trasportabile, e soprattutto caratterizzato da complessità di utilizzo. Dal punto di vista misuristico, il demodulatore vettoriale rappresenta la "Soluzione", dove la "S" maiuscola caratterizza l'assoluta correttezza della soluzione, confrontata

con qualsiasi altro strumento: dai misuratori a banda larga, agli analizzatori di spettro, magari con front-end digitale, ma non vettoriali [1]-[3]. Recentemente sono stati pubblicati lavori che forniscono metodologie di misura per ovviare all'utilizzo di demodulatori vettoriali [4], [5]. Queste procedure sono efficaci in assenza di interferenze, però non è possibile prescindere dalla demodulazione, quando più segnali, totalmente o parzialmente sovrapposti in frequenza, siano presenti durante la misura.

IL DISPOSITIVO

L'idea realizzativa nasce da una considerazione "quasi" banale. La demodulazione di una segnale WLAN è effettuata continuativamente da qualsiasi chipset wireless montato su qualsiasi piattaforma (PC, gateway, smartphone) connessa ad una rete WLAN, ogni qual volta quella piattaforma voglia scegliere un punto di accesso, collegarsi ad esso, e con esso scambiare dati ed informazione. La piattaforma è normalmente attrezzata con un chipset che effettua le seguenti operazioni:

- filtraggio a radiofrequenza della sola banda WLAN prima del mixer, quindi grande precisione di misura e bassa componente di rumore; normalmente un chipset wireless presenta uan sensibilità in banda tra -102 dBm e -110 dBm, assolutamente confrontabile con il demodulatore più avanzato presente sul mercato
- demodulazione di tutti i segnali WLAN presenti nel luogo di connessione, individuazione degli identificativi di rete ed associazione ad ognuno del corrispondente contributo di potenza ricevuta; questa operazione, necessaria ai fini di stabilire il collegamento di rete, è svolta in modo "nascosto" rispetto all'utente della piattaforma, ma è indispensabile per stabilire un corretto collegamento in rete
- aggiornamento continuativo dello stato delle reti presenti nel luogo di connessione, con ricezione di tutti i segnali presenti, siano essi punti di accesso o stazioni utente.

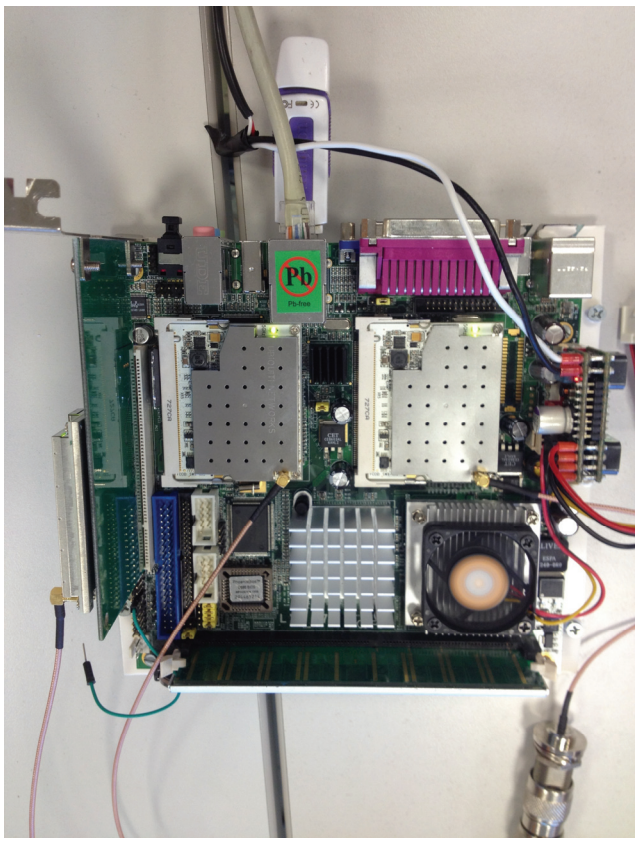
Da non trascurare il fatto che un chipset WLAN costa qualche decina di Dollari.

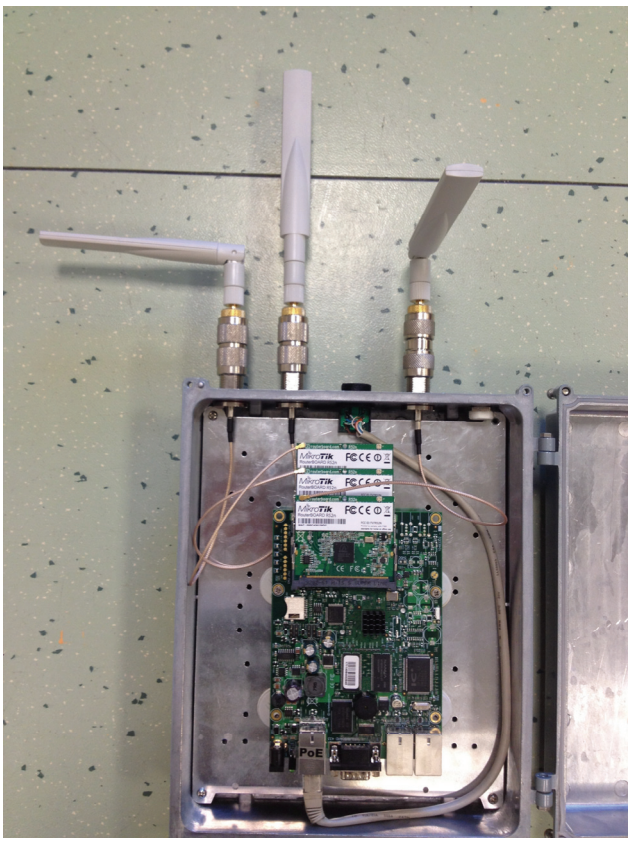
Sulla base di questa considerazione, abbiamo realizzato un PC attrezzato con un chipset WLAN, che accede direttamente alle funzionalità di scansione e monitoraggio implementate all'interno dello stesso chipset e normalmente non accessibili all'utente [6]. Il PC, in particolare, effettua una scansione di tutti i pacchetti presenti su ogni canale Wi-Fi per un tempo predefinito dall'utente, individua il nome della rete che li ha generati (E-SSID), e nel caso in cui il nome della rete sia nascosto, individua il MAC-ADDRESS (B-SSID) della stessa, che è sempre trasmesso in chiaro. Il PC, in pratica, funziona come un normale router Wi-Fi, offrendo all'utente la possibilità di accedere alle informazioni di rete che sono utilizzate da un router per il proprio funzionamento e che normalmente non sono accessibili all'utente dello stesso.

Il dispositivo è realizzato mediante un comunissimo chipset Wi-Fi, di tipo commerciale, del valore di poche decine di Euro, pre-montato sua una scheda di controllo standard, di tipo mini-PCI o PCI. Il meccanismo di controllo e gestione è affidato al PC, realizzato mediante una scheda che ospita una CPU e RAM adeguate. La scelta naturale è rappresentata da una soluzione integrata su SBC (single board computer), come quella rappresentata in Figura 1, a destra. Possono andare bene anche soluzioni che prevedano l'utilizzo di un computer di vecchia generazione, obsoleto per attività computazionali o di ufficio, ma utile per il controllo di hardware di misura, come mostrato in Figura 1, a sinistra. L'antenna può essere di tipo commerciale, ma può essere sufficiente un'antenna omnidirezionale a larga banda, che copra tutti i canali Wi-Fi, anch'essa autocostruita.

In particolare, il costo estremamente contenuto della realizzazione, permette di considerare la possibilità di montare sullo stesso PC non uno, ma più chipsets, in modo tale da effettuare la misura delle tre polarizzazioni (X,Y,Z) in contemporanea. Questo permette di ridurre i tempi di misura ad un terzo, permettendo l'esecuzione di monitoraggi in più punti. Alternativamente, è possibile utilizzare i tre chipsets per misurare il campo elettromagnetico in punti diversi dello spazio, effettuando la media spaziale sulla sezione trasversale del corpo umano richiesta dalla normativa tecnica in tempo reale.

Figura 1 – Esempi di realizzazione del dispositivo a tre radio, con PC (a sinistra) e SBC (a destra)





IL SOFTWARE

L'analisi in frequenza può essere facilmente realizzata dall'utente finale, mediante accesso alle funzioni di scansione e monitoraggio del chipset. Le procedure sono standard, e quindi è sufficiente la conoscenza dei codici di controllo del chipset stesso per avviare la scansione dei pacchetti e l'acquisizione del dai di monitoraggio. Operativamente, se non automatizzata, l'operazione può essere relativamente laboriosa, a causa del fatto che il chipset registra tutti i pacchetti generati da tutti i dispositivi wireless identificati. Occorre quindi una lavoro di scrematura e filtro dei pacchetti, per individuare quelli significativi, ai quali è associata l'effettiva potenza massima, irradiata sui sincronismi.

Per semplificare le operazioni di misura e fornire una lettura immediata, abbiamo realizzato un software di controllo, installato sul dispositivo (il PC) da noi progettato per effettuare la scansione di rete. Il software di controllo è attrezzato con interfaccia Web: a questo modo l'utilizzo del PC che effettua la scansione è garantito a tutti, mediante utilizzo di un qualsiasi browser, prescindendo dal sistema operativo o dal sistema di acquisizione utilizzato dall'utente finale.
Il software effettua le seguenti operazioni:

1. sceglie quali e quante chipsets utilizzare in fase di scansione
2. sceglie le frequenze (i canali) su cui effettuare al scansione
3. determina la durata della fase di ascolto per ogni canale
4. effettua la scansione
5. filtra i dati di monitoraggio
6. aggrega i risultati per B-SSID
7. stampa i risultati

La Figura 2 rappresenta la pagina Web utilizzata per impostare i parametri di scansione (punti da 1. a 3. dell'elenco precedente), mentre la Figura 3 mostra un esempio di risultati. Come si vede, la scansione è stata effettuata all'interno di un laboratorio del Politecnico di Torino.

Figura 2 – La schermata iniziale del Software di scansione

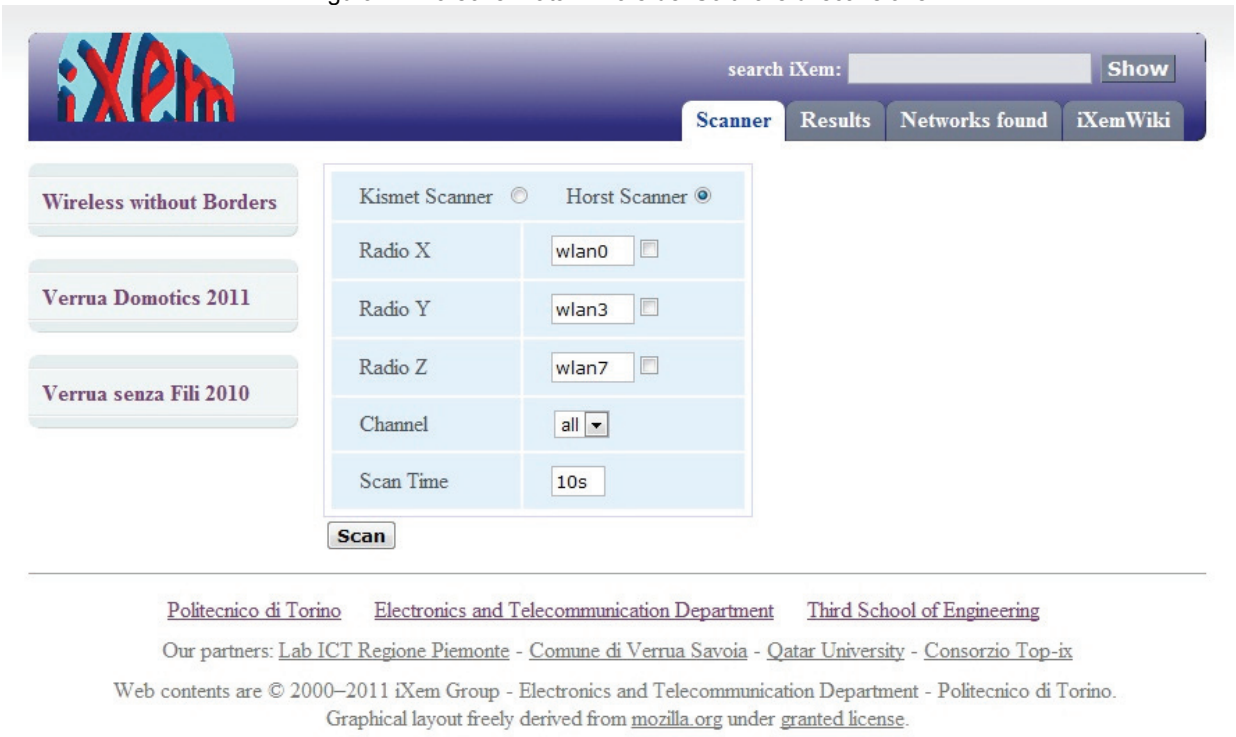
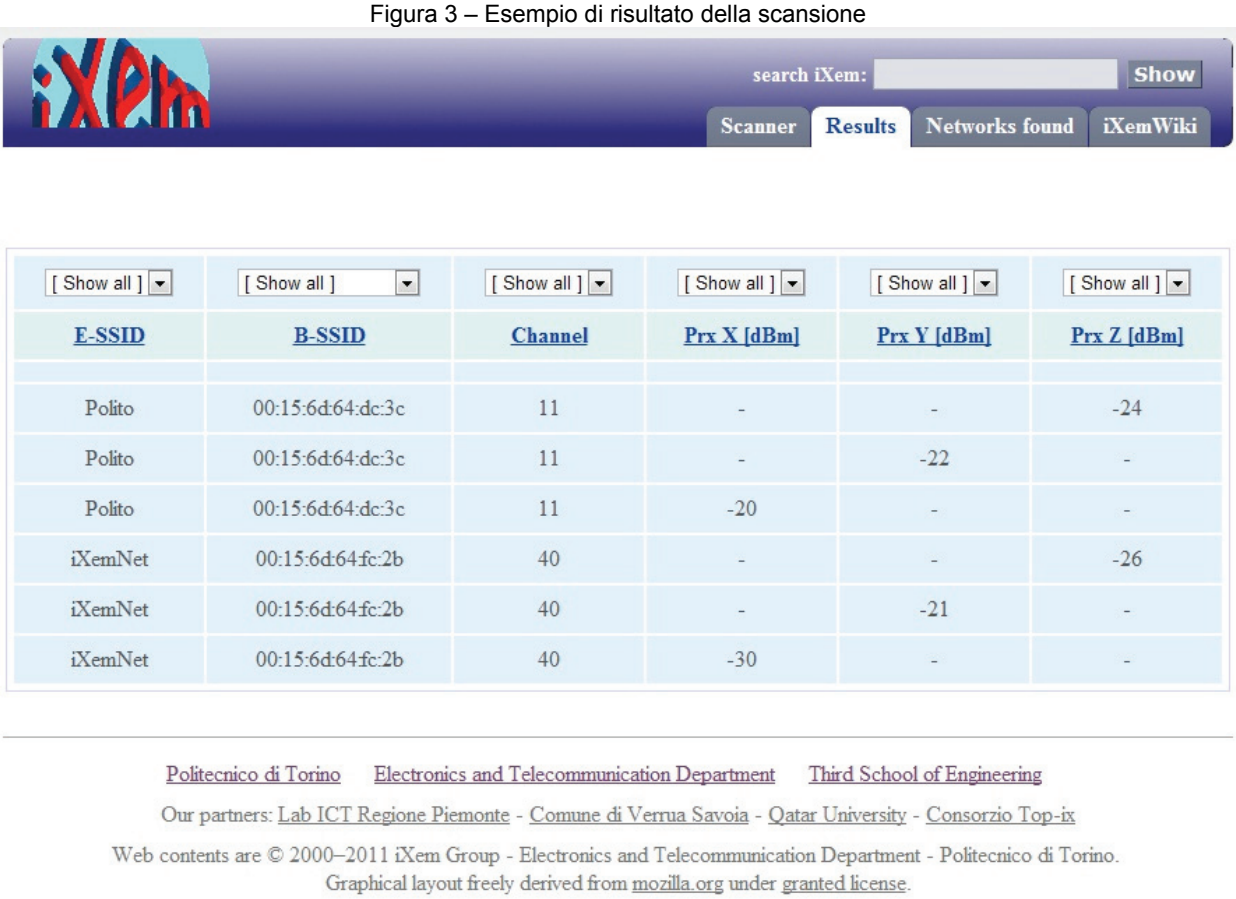


Figura 3 – Esempio di risultato della scansione



iXemWIKI

La realizzazione proposta è descritta da un filmato pubblicato sul repository iXemWiki degli iXem Labs del Politecnico di Torino, insieme con una versione del software di scansione descritto nel paragrafo precedente. L'accesso al repository è garantito a titolo gratuito, ed è possibile registrandosi presso lo stesso sito e richiedendo le credenziali di accesso.
L'indirizzo Web del Repository è: wiki.iXem.polito.it

CONCLUSIONI

Il risultato è rappresentato da un dispositivo semplice, di costo bassissimo, molto più funzionale ed immediato di qualsiasi sistema di misura dotato di demodulatori vettoriali. La grande peculiarità è rappresentata dalla possibilità di utilizzare codici di hack che permettono l'individuazione della potenza associata a reti in chiaro, reti criptate, e e di separare con successo gli Access Point dalle station. Lo strumento ideale per una risposta chiara, veloce, precisa, affidabile, a costi molto contenuti.

Per il futuro abbiamo intenzione di sviluppare dispositivi analoghi da utilizzare per effettuare scansioni di altre tipologie di segnale digitale: telefonia mobile 2G, 2.5G, 3G, 3.5G, 4G, televisione digitale DVB-T e DVB-H, fonia digitale DAB, reti WPAN a standard 802.15

BIBLIOGRAFIA

[1] D. Trinchero "Valutazione teorica e sperimentale dell'esposizione in presenza di reti radio digitali di nuova generazione", *IV Convegno Nazionale Controllo ambientale degli agenti fisici: nuove prospettive e problematiche emergenti*, 24-27 Marzo 2009, Vercelli, Italy

[2] Agilent, Application Note 1380-1 "RF Testing of Wireless LAN Products"

[3] Rohde & Schwarz, Application Note 1MA69, "WLAN Tests According to Standard 802.11a/b/g"

[4] D. Trinchero et al., "Misura dell'esposizione a segnali radio digitali a banda larga mediante strumenti selettivi in frequenza", *IV Convegno Nazionale Controllo ambientale degli agenti fisici: nuove prospettive e problematiche emergenti*, 24-27 Marzo 2009, Vercelli, Italy

[5] D. Trinchero, A. Carta, L. Cisoni, R. Stefanelli, S. Trinchero, "Measurement of radio signals carrying wideband digital modulations by means of frequency selective instruments", XVIII Riunione Nazionale di Elettromagnetismo (RiNEM), 6-10 Settembre 2010, Benevento, Italy

[6] IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN, , IEEE Std. 802.11, 2007.