Introduzione

Il mondo dell'Information Technologies (IT) e delle telecomunicazioni ha una capacità infinita di produrre nuovi termini e acronimi. Alcuni individuano tecnologie ben note, altri si riferiscono a nuove. Lo scopo di queste righe è di spiegare cosa c'è dietro a questi termini cercando di focalizzare alcuni concetti inerenti il mondo della radio.
WIRELESS, parola quasi abusata, può significare di tutto. Semplicemente significa senza filo: nulla di nuovo nel mondo della radio.
Il wireless è generalmente un collegamento dati senza la connessione fisica di un cavo in rame, restano disponibili come mezzo di connessione la radiofrequenza, la luce e l'infrarosso (in ogni caso si tratta di onde elettromagnetiche).
L'uso di radiofrequenza per la trasmissione digitale è noto da tempo, fra le applicazioni più comuni in campo radiantistico ci sono l'RTTY e il packet radio, ma il termine wireless si applica generalmente a tecnologie differenti fra le quali il Bluetooth[1] e le connessioni basate sullo standard 802.11.
Aspetti importanti di un canale di comunicazione in genere sono la capacità del canale, la distanza massima fra i dispositivi e la possibilità per più dispositivi di utilizzare la stessa banda contemporaneamente.
La tecnologia bluetooth consente distanze che sono dell'ordine del metro, massimo alcune decine di metri con velocità massima di 1 Mb/S. Più dispositivi possono condividere la stessa banda.
La tecnologia basata sugli standard 802.11 consente distanze di decine di metri a decine di chilometri con velocità di trasmissione fino a 54 Mb/S.
Claud Shannon[2] più di 50 anni fa, quando ancora non si parlava di trasmissione digitali, ha brillantemente studiato la trasmissione dati. Il risultato, non l'unico, ma il più noto, è una semplice formula che racchiude le problematiche connesse alla trasmissione dati fornendo la massima capacità di un canale trasmissivo: $\mathbf{C=B*\log_2(1+S/N)}$ [3] dove con **C** si indica la massima capacità del canale in b/s[4], **B** è la banda in Hz, **S/N** è il rapporto segnale rumore (in potenza). La forza della formula citata è nella semplicità e nella generalità. La si può applicare sia a un canale radio che ad un canale in rame o a qualunque canale che trasporta informazioni[5].
Dalla formula si vede immediatamente che per aumentare la capacità di un canale di trasmissione ci sono due possibilità: la prima consiste nell'aumento della potenza di trasmissione (potenza e.r.p., quindi con più watt o migliori antenne), in modo da aumentare il rapporto segnale rumore, la seconda alternativa consiste nell'aumentare la banda[6]. In entrambi i casi ci sono i pro e i contro.

---

1 https://www.bluetooth.org/spec/
2 http://www-gap.dcs.st-and.ac.uk/~history/Mathematicians/Shannon.html http://cm.bell-labs.com/cm/ms/what/shannonday/paper.html
3 Con un rapporto segnale rumore di 30 db (il segnale 1000 volte superiore al rumore) e una banda telefonica di 3 KHz, il tipico collegamento telefonico, si ottiene una capacità del canale di circa 30 Kb/S
4 Bit al secondo
5 Informazioni di qualunque tipo, anche analogico, in quanto è sempre possibile pensare di trasformare un segnale analogico, limitato in banda, in un corrispondente digitale. Il teorema di Nyquist ne fornisce la formulazione.
6 http://www.aei.it/viterbi.pdf

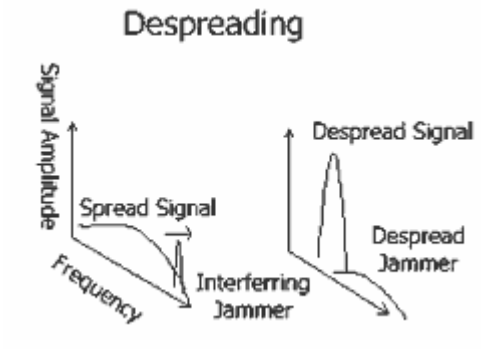
L'aumento della potenza non è facile, richiede molta energia, senza considerare la legislazione che ne limita il valore massimo; inoltre il termine S/N, legato alla potenza viene "ridimensionato" dal logaritmo: raddoppiando il termine (1+S/N) si ottiene un aumento di 1 in $\log_2(1+S/N)$. Molto meglio allora aumentare la banda, raddoppiando B si raddoppia la capacità del canale, ma anche la banda è una risorsa importante e inflazionata di cui non si può far uso a piacere. In ogni caso, è possibile notare come, anche con rapporti S/N molto bassi, facendo uso di una banda adeguata, si può ottenere la capacità di canale voluta.
Questo discorso, un poco teorico serve a introdurre il wireless. Questa tecnologia fa uso di bande molto ampie, diversi MHz. Il termine più corretto per le tecnologie bluetooth e 802.11 è Spread Spectrum[7] (SS).

Condivisione del Canale

La possibilità di condividere lo stesso canale di comunicazione con più dispositivi è spesso realizzata attraverso la contesa del canale, tipico è il meccanismo delle reti Ethernet (CSMA/CD) in parte simile a quanto utilizzato nel packet radio. La contesa consente ad un dispositivo di allocare in esclusiva il canale per un tempo sufficiente piccolo (ad esempio per il pacchetto che deve essere trasmesso) in modo che tutti i dispositivi possono accedere al canale dando l'illusione di un uso esclusivo, si parla di sovrapposizione nel dominio della frequenza ma non nel dominio del tempo, semplicemente la frequenza è la stessa per tutti i dispositivi, ma non impegnata contemporaneamente. È anche possibile la contemporaneità di più trasmissioni se il segnale di un dispositivo è distinguibile da un altro attraverso una codifica che permetta di elaborare solo il segnale desiderato. Il segnale degli altri dispositivi sarà visto come una sorta di rumore, tipico della codifica CDMA (Code Division Multiple Access)[8]: in questo caso si ha sovrapposizione contemporanea nel dominio della frequenza e nel dominino del tempo.

Spread spectrum

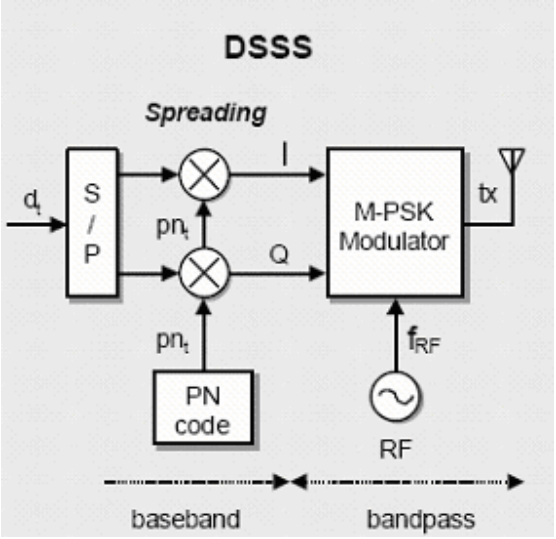
La tecnologia spread spectrum, non è nuova, ma poco conosciuta consiste nel distribuire il segnale elettromagnetico su un'ampia banda in modo da avere un canale di comunicazione adeguato con rapporti segnali rumore anche sfavorevoli.



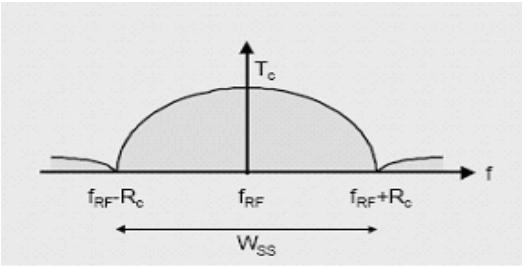
Tale metodo di trasmissione si contrappone con l'idea di un forte segnale su una banda ristretta. Concentrare un segnale su una banda stretta equivale ad urlare, cercare di portare la propria "voce" ad un livello tale da coprire le altre. Lo spread spectrum al contrario, distribuendo l'informazione su una ampia banda rende poco dannoso se non nullo la perdita di una parte di informazione dovuta ad un disturbo concentrato su una singola frequenza.
Per realizzare una trasmissione SS, viene usato

[7] http://www.sss-mag.com
[8] http://info.iet.unipi.it/~luise/HTML/AdT/Introd_CDMA.pdf

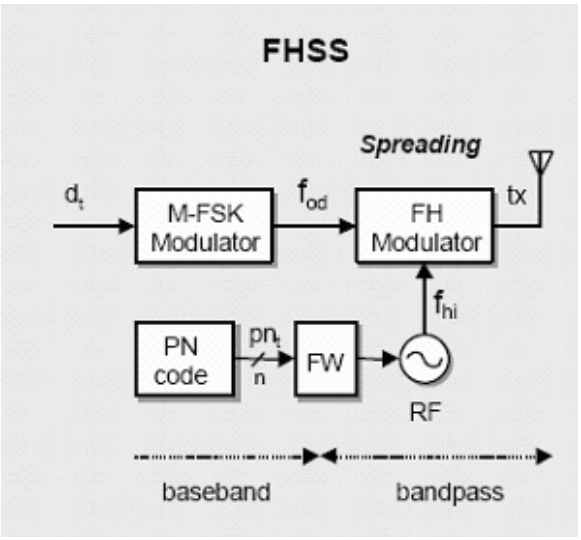
un codice pseudo-casuale (PN Pseudo Noise) per modulare il segnale contenente l'informazione da trasmettere. Il risultato è un segnale con una banda molto maggiore della banda occupata dal segnale da trasmettere[9]. In ricezione lo stesso codice pseudo-casuale viene utilizzato per ripristinare i dati originali. Va sottolineato un ulteriore aspetto della trasmissione SS: la conoscenza esclusiva del codice PN fornisce anche riservatezza per i dati trasmessi in quanto solo conoscendo il codice si può decodificare i dati.
Le tecniche SS possono essere di diversi tipi, ma i principali sono Direct Sequence Spread Spectrum (DS), Frequency Hopping Spread Spectrum (FH) o Wide Orthogonal Frequency Division Multiplexing (W-OFDM).

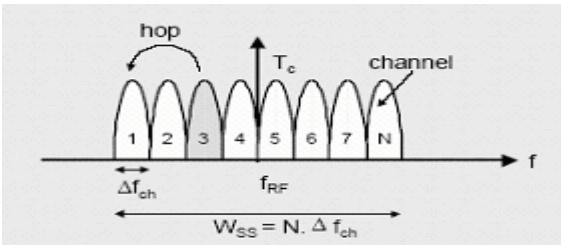


Nel primo caso (**DS**) il segnale da trasmettere viene miscelato con il codice pseudo-casuale (PN). La banda che si ottiene ha un andamento sen(x)/x. La scansione del codice PN avviene ad una velocità Rc multipla della velocità, in bit/Sec dei dati da trasmettere.



Con il modo **FH** l'allargamento di banda viene ottenuto allocando piccole parti di banda, in modo casuale (controllato dal codice pseudo-casuale) per tempi molto piccoli (mS). Ad esempio il bluetooth usa il metodo FH selezionando 79 frequenze differenti spaziate di 1MHz ed effettua 1600
hop (salti) al sec.





[9] Contrariamente alle tecniche di modulazione classiche, dove l'ampiezza di banda occupata dal segnale a RF è dello stesso ordine della banda dell'informazione trasmessa.

Il terzo metodo,W-OFDM, assomiglia al modo FH, ma le frequenze dei singoli canali sono scelte in modo opportuno consentendo una sovrapposizione dei singoli canali senza interferenza fra gli stessi. La difficoltà consiste nella generazione, molto precisa delle singole frequenze.

802.11x[10]

Le tecnologie basate su questo standard stanno prendendo velocemente piede nell'impiego in aziende, in parte per una effettiva necessità e in parte per un convincimento pubblicitario e sono usate per la realizzazione di reti dati.
Si tratta di trasmissione spread spectrum nella banda di frequenza dei 2,4 e 5 GHz. Queste bande sono ad uso libero, non sono richieste licenze o particolari autorizzazioni per utilizzarle. Le modalità sono definite dall'ente europeo E.T.S.I.[11], la principale restrizione è la potenza massima di 100 mW e.r.p.
I dispositivi wireless realizzati possono funzionare in modo autonomo o interfacciati con una rete ethernet preesistente.
Gli standard descritti con 802.11 sono diversi e con caratteristiche differenti che riassumo nella tabella seguente.

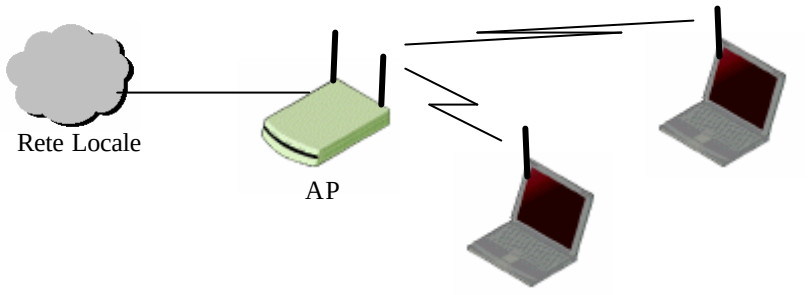
Standard	Modo	Frequenza (GHz)	Vel. Max (Mb/S)	Data di ratifica
802.11	FH[12] e DS	RF (2.4) e IFR	1-2	1997
802.11a	W-OFDM	5	54	1999
802.11b	DS	2.4	11	1999
802.11g	W-OFDM e DS	2.4	54	2003(?)
802.16	W-OFDM	10-66	54	
Bluetooth	FH	2.4	1	

L'***802.11*** è stato definito nella seconda metà degli anni 90 e prevede, oltre l'uso della radiofrequenza, anche i dispositivi a infrarosso, naturalmente non a 1 Mb/Sec. Lo standard ***802.11a*** apparentemente migliore per prestazioni non ha raggiunto una ampia diffusione per la difficoltà ad operare a 5GHz e per la coperture ridotta rispetto l'***802.11b***, a parità di potenza. L'802.11b[13] ha avuto un'ampia diffusione perché relativamente facile da implementare; la diffusione ha poi portato all'abbattimento dei prezzi, per questo motivo, salvo espliciti riferimenti, si parlerà dell'802.11b.

[10] In Europa il wireless è regolato da normative della E.T.S.I., mentre i termini 802.11 sono legati all'istituto IEEE americano. Le differenze sono poche, ma ci sono. Lo stato Italiano recepisce, in genere, le normative europee .
[11] http://www.etsi.org/
[12] 77 canali da 1 MHz
[13] Occorre anche tenere conto della normativa europea e italiana. In Italia solo dal maggio 2003 un decreto prevede l'uso del wireless a 5 GHz. Gazzetta Ufficiale n. 136 del 14 Giugno 2003

802.11g, unisce i vantaggi della banda a 2.4 GHz con la velocità a 54 Mb/S. Implementa sia la codifica DSSS che W-OFDM, consentendo la compatibilità con i sistemi 802.11b.
L'***802.16*** (802.16a è stata ratificata nel 2003) promette di riunire (sarà vero?) e superare i limiti delle precedenti tecnologie, ma al momento è meglio concentrarsi su quanto è maggiormente consolidato.

L'implementazione di una rete wireless vede l'uso di due tipi di dispositivi: l'**Access Point (AP)** e la scheda di rete sul PC.
L'access point altro non è che il ripetitore, che può funzionare autonomamente o connesso ad una rete ethernet esistente. La scheda di rete consente la connessione con l'access point e, tramite questo, con le altre stazioni.



802.11b, in Europa, prevede 11 possibili canali spaziati di 5 MHz, una connessione wireless necessita di una banda di 22 MHz, pertanto se si usano più AP contemporaneamente nella stessa area (ad esempio per funzioni di roaming) occorre scegliere attentamente i canali utilizzati ad esempio 1, 6 e 11, in modo da evitare sovrapposizioni. In molti casi, in applicazioni semplici, i dispositivi sono in grado di scegliere autonomamente un canale da utilizzare, è comunque evidente che i dispositivi devono funzionare tutti sullo stesso canale.

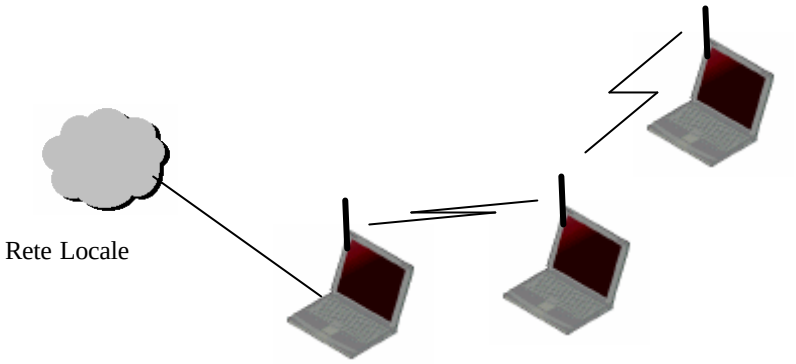
Canale	Frequenza GHz
1	2.412
2	2.417
3	2.422
4	2.427

Canale	Frequenza GHz
5	2.432
6	2.437
7	2.442
8	2.447

Canale	Frequenza GHz
9	2.452
10	2.457
11	2.462

E' da notare che non ho ancora utilizzato il termine *Wi-Fi (*Wireless Fidelity): non mi piace. L'uso del termine è commerciale e non è sufficiente a garantire l'interoperabilità di apparti e reti. Basta pensare che Wi-Fi si riferisce sia a tecnologia 802.11a che 802.11b che evidentemente non possono interoperare. Ci sono poi altre incongruenze.

802.11b definisce due possibili modalità radio che sono mutuamente esclusive: BSS e IBSS.
La prima sta per **Basic Service Set**. In questa modalità esiste una stazione master (AP) che fa da interfaccia (bridge) verso la rete cablata. Il PC deve connettere l'AP prima di accedere alla rete cablata o ad altri PC in wireless.



La modalità **Indipendente Basic Service Set** (IBSS) consente una comunicazione peer-to-peer senza l'uso di access point. Un PC che è opportunamente collegato alla rete fissa può fornire l'accesso alla stessa anche per gli altri PC

Sicurezza.

E' al momento un punto di debolezza del wireless. Basta un PC e una scheda wireless che si entra in rete. La situazione è molto comoda in alcuni casi, magari in una wireless area pubblica, ma certamente improponibile per una azienda. Sono poi disponibili software e hardware ad hoc realizzati per 'sniffare l'aria' e cercare accessi a reti.[14]
In primo approccio a protezione dei dati è fornita dalla crittografia WEP (Wired Equivalent Privacy) prevista dalle specifiche 802.11b. L'algoritmo impiega una chiave segreta, ma non molto, in quanto tutti i PC in rete wireless condividono la stessa chiave. Da un qualunque PC è possibile vedere il traffico di tutti gli altri. Inoltre è stato dimostrato che la crittografia adottata, vuoi per la chiave di soli 40 bit, vuoi per l'algoritmo, non è sicura e in poco tempo e con mezzi semplici è forzabile. Esistono anche apparati che implementano crittografia più efficace anche a 128 bit, ma non essendo prevista dallo standard 802.11b, non è garantita l'interoperatività fra varie marche.
Altro approccio alla sicurezza è possibile con la specifica **802.1x**. Questo standard, sempre emesso all'IEEE, non è rivolto solo al wireless, ma anche alle reti cablate, si pensi ad una università con migliaia di punti di accesso, diventa praticamente impossibile controllare gli accessi anche alla rete cablata. 802.1x consente il controllo dell'accesso basato alle porte (Port Based Access Control). Prima di stabilire una connessione alle rete, cablata o wireless, occorre superare un meccanismo di autenticazione che assicura l'identità dell'apparto collegato.
Una volta autenticato l'accesso, possono venir distribuite chiavi di crittografia, ad esempio chiavi WEP, ma ancora non sono ben definiti i vari tipi di crittografia, ma solo linee giuda. Anche con 802.1x rimangono diverse lacune. Non è ben definito il servizio di autenticazione, che può essere implementato in vari modi.

Un ulteriore opzione, per aumentare la sicurezza, è utilizzare tecniche di tunneling e criptare il traffico dal dispositivo fino al servizio che viene utilizzato, si parla di SSL e SSH, VPN, PPTP, IPSec, ma sono altre sigle che vanno oltre lo scopo di queste note.

[14] Il rischio per le reti cablate è minore, ma non certamente nullo.

Conclusioni

Lo scopo di queste righe non è certamente l'approfondimento degli argomenti trattati, ma fornire una panoramica alle problematiche che si devono affrontare indagando nel mondo del wireless.
Installare una rete in banda 2.4 GHz non è difficile, specie se non si affrontano strutture complesse e problemi legati alla sicurezza e alla riservatezza.
Per i radioamatori ci sono diversi punti di interesse che vanno dalle antenne all'interfacciamento con altri sistemi. In particolare la tecnologia Spread Spectrum per quanto non nuova non è certamente diffusa e merita ulteriori approfondimenti.

Fabrizio Restori I4NKF

f.restori@rsadvnet.it