



INTRODUZIONE AI SISTEMI WIRELESS DIGITALI

terza parte

IL BLUETOOTH

di Sandro Romagnoli

s.romagnoli@farelettronica.com

Il Bluetooth è una tecnologia a basso costo e molto flessibile, che permette di “tagliare i fili” ad un grande numero di apparecchiature elettroniche e di aprire nuove possibilità. Vediamo a cosa serve e come si pone in relazione con gli altri standard di comunicazione wireless più diffusi, come Wi-Fi e GSM/GPRS.

L'idea è sempre quella: eliminare l'intrico di cavi di collegamento che caratterizza l'utilizzo di più apparecchiature elettroniche insieme, siano essi i vecchi cavi RS232, che troviamo ancora nei modem per la linea telefonica analogica o le nuove connessioni seriali ad alta velocità come USB e FireWire che vengono impiegate in dispositivi caratterizzati da una più elevata multimedialità, come fotocamere, scanner e stampanti.

Alla diffusione sempre maggiore che accompagna il PC e quindi tutte le sue periferiche, si aggiunge la rivoluzione dettata dall'utilizzo del telefono cellulare, che è diventato in pochi anni un vero e proprio computer palmare e richiede un livello elevato di connettività per scambiare dati con il PC

stesso o con altri dispositivi cellulari.

Da questa premessa è nato lo sforzo delle più grandi aziende operanti nel settore della telefonia cellulare, fra cui Motorola, Nokia ed Ericsson, teso a definire una tecnologia di connessione wireless a basso costo che potesse risolvere tutte le nuove esigenze di connettività che si venivano a creare (la tecnologia IrDA a raggi infrarossi già usata da tempo ha

il limite di funzionare solamente in assenza di ostacoli). Il risultato degli studi effettuati è il Bluetooth (www.bluetooth.com).

Le specifiche iniziali erano molto ambiziose soprattutto riguardo l'obiettivo di costo sotto i 5 dollari per ogni radio, ma solo negli ultimi due anni l'industria microelettronica è

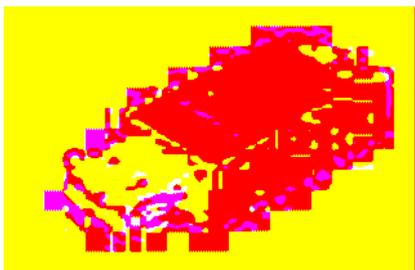


Figura 1: Adapter Bluetooth USB per PC

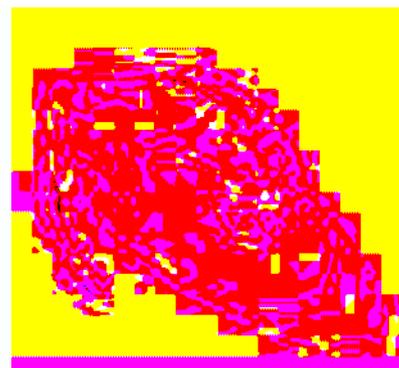


Figura 2: Auricolare Bluetooth per telefoni cellulari



avanzata al punto da riuscire a produrre dei singoli circuiti integrati CMOS in grado di ospitare al loro interno tutta la parte in banda base e quasi tutta la sezione RF (in genere rimane fuori solamente l'antenna) consentendo di abbassare drasticamente i costi e consentire così una grande diffusione. Oggi appaiono sul mercato continuamente nuovi dispositivi dotati di interfaccia Bluetooth, in primo luogo i telefoni cellulari, ma anche GPS, stampanti e modem: nasce così il concetto di PAN (Personal Area Network), una rete wireless a corto raggio formata da tanti dispositivi elettronici che si scambiano dati fra loro.

In figura 1 si vede un adattatore USB, mentre in figura 2 un auricolare.

PRINCIPI DI FUNZIONAMENTO

L'idea di progetto iniziale di realizzare un sistema che permettesse la trasmissione di voce e dati e che fosse semplicissima da usare per gli utenti finali, ha portato allo sviluppo di uno stack di protocollo veramente complesso. Uno dei fondamentali è che le radio Bluetooth devono essere in grado di riconoscersi e formare delle reti fra loro in modo autonomo senza praticamente l'intervento esterno, al contrario del Wi-Fi in cui è normalmente richiesta una seppur minima conoscenza di base delle reti di calcolatori.

Nella maggior parte degli adattatori Bluetooth per PC che si trovano in commercio, il proto-

collo è diviso in due parti (vedi figura 3, che ne riporta una versione semplificata): la parte di più basso livello (colore giallo) è ospitata sull'adattatore stesso, che può essere una chiavetta USB o una PC Card, mentre l'altra (colore azzurro) è implementata sul driver che gira sul PC, che è normalmente fornito dal costruttore dell'adattatore stesso. Per far parlare fra loro le due parti dello stack è definito un livello di interfaccia chiamato **HCI** (Host Control Interface). Chi è abituato a lavorare con interfacce semplici tipo la RS232, sa che lo standard definisce solamente la parte più vicina all'hardware, mentre non dice niente su come impacchettare o frammentare i dati che vogliamo inviare o ricevere su quell'interfaccia. Al contrario Bluetooth introduce il concetto di profilo che arriva quasi ad un livello applicativo e consente ad esempio di trasferire un file fra un nodo Bluetooth ed un'altro.

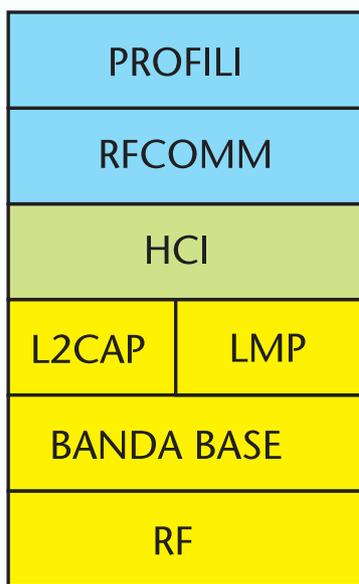


Figura 3: Stack Bluetooth

Livello RF

A questo livello sono definite le caratteristiche del segnale RF utilizzato dalle radio Bluetooth. La banda di lavoro è quella ISM posta a 2,4GHz (la stessa del Wi-Fi), che viene divisa in 79 canali, ognuno dei quali è ampio 1 MHz e, per far fronte alle interferenze, il sistema adotta un **FHSS** (Frequency Hopping Spread Spectrum) con 1600 hops/secondo, cioè 1600 volte in un secondo si "salta" su di un diverso canale fra i 79 disponibili. La modulazione utilizzata è la **GFSK** (Gaussian Frequency Shift Keying) che è una variante della modulazione di frequenza che invece di usare un'onda quadra per rappresentare i bit da trasmettere, adotta una forma d'onda che ricorda una campana di Gauss, ottenendo così una maggiore efficienza spettrale. Per quanto riguarda la potenza del segnale RF emesso, i dispositivi in commercio si riferiscono in genere alla portata in metri (ovviamente quello specificato è puramente indicativo) e se ne trovano da 10 metri (potenza dell'ordine di 1mW) o da 100 metri (potenza dell'ordine di 100mW).

Banda Base

Il funzionamento in Frequency Hopping, fa sì che la più piccola unità di informazione disponibile sia lo *Slot*, che consiste nella sequenza di bit trasmessa mentre la radio è posizionata su un canale. Poiché si lavora a 1600 hops/s, uno slot dura 625 microsecondi. La comunicazione avviene dividendo i messag-



gi in pacchetti ed un pacchetto può occupare uno o più slot (1, 3 o 5): mentre con l'utilizzo di un solo slot si può arrivare ad una velocità di trasferimento di 172 Kbit/s, l'utilizzo di più slot consente di aumentare la velocità, arrivando ad un massimo teorico di 721 Kbit/s utilizzando 5.

Livello L2CAP

L2CAP sta per Logical Link Control and Adaptation Protocol, qui vengono svolti il multiplexing dei dati provenienti dai protocolli di livello superiore (cioè, una unica radio Bluetooth può essere usata da diversi applicativi ad alto livello, ognuno dei quali usa un certo modo per trattare le informazioni), la frammentazione, il riassetto dei pacchetti ed il trasporto delle informazioni di "qualità del servizio" (QoS) che servono quando vengono impiegati dei flussi di dati in tempo reale, come ad esempio l'audio o il video che non tollerano ritardi di trasmissione superiori ad una certa soglia.

Livello LMP

LMP vuol dire *Link Manager Protocol* e si occupa della formazione e della gestione di reti fra i diversi nodi Bluetooth.

Livello HCI

Host Control Interface fornisce una interfaccia standard ai diversi hardware che implementano una radio Bluetooth, in modo che un medesimo driver scritto per funzionare su un PC possa funzionare con tutti gli adattatori presenti sul mercato,

indipendentemente dal costruttore dell'adattatore stesso.

Livello RFCOMM

Questo livello utilizza la radio Bluetooth per emulare un collegamento seriale standard (tipo RS232), viene utilizzato da molti profili di alto livello ad esempio per trasferire files.

Profili

I profili rappresentano l'interfaccia tramite la quale un utente interagisce con i dispositivi Bluetooth. I profili disponibili sono tanti e ne vengono continuamente introdotti dei nuovi per gestire al meglio le nuove periferiche che vengono immesse sul mercato.

Tipicamente, gli adattatori Bluetooth per PC supportano un ampio spettro di profili, mentre invece i dispositivi più semplici, come ad esempio i telefoni cellulari ne supportano un sottoinsieme. Alcuni esempi sono:

- **Serial Port Profile (SPP):** come si intuisce dal nome, questo profilo implementa una porta seriale virtuale. Consideriamo due PC dotati entrambi di radio Bluetooth: se il driver supporta questo profilo, avranno a disposizione delle porte COM virtuali che possono essere utilizzate mediante i normali programmi tipo HyperTerminal di Windows. Aprendo sui due PC due sessioni di terminali sulle rispettive porte virtuali potranno scambiarsi dati esattamente come se fossero collegati mediante un cavo null-modem RS232 attraverso

la radio Bluetooth.

- **Object Exchange (OBEX):** consente di trasferire files fra dispositivi dotati di radio Bluetooth, siano essi due PC, oppure un PC ed una fotocamera digitale.
 - **Dial Up Network (DUN):** questo profilo è in genere implementato sui modem Bluetooth e consente ad un PC con Bluetooth di utilizzarlo come se fosse collegato con un cavo. Questo profilo è in genere implementato nei telefoni cellulari, che possono funzionare da modem per il PC.
 - **Headset (Cuffia):** è usato anch'esso nei cellulari e consente l'utilizzo dell'auricolare wireless.
 - **Local Area Network (LAN):** tramite questo profilo è possibile accedere ad una rete locale TCP/IP in modo wireless. Consideriamo un PC collegato ad una rete Ethernet e dotato anche di una interfaccia Bluetooth: questo può diventare un punto di accesso wireless alla rete per tutti i dispositivi mobili Bluetooth che dispongono di questo profilo, ad esempio computer palmari.
 - **Personal Information Manager (PIM):** serve per scambiare fra dispositivi Bluetooth informazioni quali biglietti da visita elettronici, e-mail, note o appuntamenti.
 - **Human Interface Device (HID):** consente di connettere ad un PC periferiche come mouse e tastiera.
- Per poter utilizzare un profilo in



una connessione fra due nodi, il profilo stesso deve essere supportato esplicitamente da entrambi, altrimenti la connessione non può avere luogo. Esiste un protocollo apposito chiamato **SDP** (Service Discovery Protocol) che ha proprio la funzione di scoprire quali sono i profili supportati da un nodo Bluetooth remoto.

STRUTTURA DI UNA RETE

Come abbiamo detto in precedenza, le radio Bluetooth sono in grado autonomamente di formare una rete fra loro e per fare questo adottano una strategia di tipo *Master/Slave*. Il Master è il nodo della rete che

parte per primo e che coordina il funzionamento e la sincronizzazione degli altri elementi: gli

Slave. Normalmente le radio Bluetooth sono in grado di funzionare sia come Master che

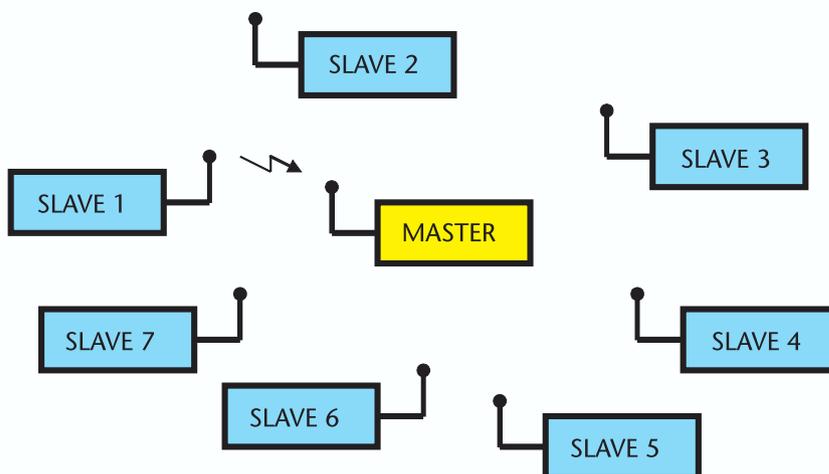


Figura 4: Piconet: la più semplice tipologia di rete Bluetooth

PIC® Microcontroller By Example

Un CD-ROM che non può mancare alla tua collezione!



Finalmente è disponibile il CD-ROM con il corso completo **PIC® Microcontroller By Example** in formato ACROBAT (PDF).

Tutte le lezioni pronte per la consultazione con i sorgenti dei progetti immediatamente utilizzabili nelle tue applicazioni.

Il modo migliore per avere sempre sottomano la soluzione per il tuo progetto con i PICmicro®.

Il CD-ROM PIC® Microcontroller By Example contiene una sezione "Contenuti Speciali" tutta da scoprire.

Ordinalo subito su www.farelettronica.com/pbc oppure telefonando allo 02.66504754.

Inware Edizioni
Via Cadorna, 27/31 - 20032 Corzano (MI)



come Slave. La più semplice topologia di rete Bluetooth è chiamata *Piconet* ed è formata da un Master e fino ad un massimo di sette Slave (figura 4).

Ogni radio Bluetooth è dotata di un indirizzo unico al mondo costituito da 48 bit (ad esempio 00:0B:0D:21:0C:84) ed il Master della Piconet parte da questo valore per determinare la sequenza di salti fra i 79 canali disponibili che viene adottata anche dagli Slave.

Perché si possa formare una Piconet, il Master comincia ad inviare dei pacchetti in cui interroga gli eventuali altri dispositivi Bluetooth presenti nell'area di copertura (questa fase è detta *Inquiry*), che intanto stanno in ascolto per un po' di tempo sui diversi canali in attesa di essere trovati. Una volta che uno Slave sente il pacchetto inviato dal Master gli risponde inviando il proprio indirizzo e così nel giro di pochi secondi il Master è a conoscenza di tutti i dispositivi Bluetooth presenti e con cui può creare una Piconet.

Una volta creata la Piconet, ad ogni nodo viene assegnato un indirizzo temporaneo da 1 a 7 (0 è il Master) tramite il quale i nodi possono parlare tra loro. Diverse Piconet possono convivere nella stessa area grazie al fatto che tutti i membri della stessa Piconet utilizzano una certa sequenza di salti fra i 79 canali disponibili (dettata dal nodo Master) che sarà diversa da Piconet a Piconet, certo, potrà succedere che occasionalmente più nodi si trovino a

trasmettere contemporaneamente sullo stesso canale e questo potrà portare alla ritrasmissione della informazione e quindi ad una diminuzione della velocità media di trasferimento.

Esiste anche un tipo più ampio di rete chiamato Scatternet in cui più Piconet sono messe in comunicazione tra loro attraverso alcuni nodi comuni a più Piconet che si occupano di trasferire i pacchetti da una Piconet all'altra.

Per i dispositivi Bluetooth a batteria, sono previste delle configurazioni di "riposo" ad assorbimento di corrente ridotto, che possono essere utilizzate nei momenti in cui non viene richiesto uno scambio dati (modalità *Park* e *Sniff*).

DIVERSI TIPI DI COLLEGAMENTO

Uno dei punti di forza del Bluetooth è la grande flessibilità che gli consente di trasportare sia voce che dati: questo è infatti stato richiesto fin dalle specifiche iniziali del progetto al contrario di quanto è avvenuto col Wi-Fi che è nato per gestire unicamente traffico dati e che richiede l'ulteriore introduzione di protocolli che gli consentano di supportare applicazioni multimediali in tempo reale. Infatti i requisiti richiesti dal traffico dati e da quello audio sono completamente diversi:

- **Dati:** quando si attua un trasferimento dati è di fondamentale importanza che il messaggio ricevuto sia uguale

a quello trasmesso fino all'ultimo bit (si pensi al trasferimento di un file contenente un programma eseguibile). Vengono quindi previsti meccanismi di *Forward Error Correction* (FEC) in cui vengono trasmessi dei bit di controllo aggiuntivi al messaggio vero e proprio che consentono al ricevitore di ripristinare eventuali bit sbagliati ed anche di ritrasmissione dei blocchi di dati non ricevuti correttamente.

Questo fa sì che possa essere variabile l'intervallo di tempo che intercorre fra la ricezione dei vari pacchetti dati che appartengono ad un medesimo messaggio.

- **Audio:** un flusso audio è costituito a partire da una sorgente analogica (normalmente un microfono), che viene poi digitalizzata e compressa mediante un opportuno algoritmo. Il flusso di bit risultante dalla compressione viene poi suddiviso in pacchetti che vengono inviati via radio. Il ricevitore processa i pacchetti che gli arrivano, ricostruendo il flusso di bit non compresso, ed attraverso un convertitore digitale/analogico va a comandare un altoparlante. Perché un collegamento di questo tipo mantenga una buona qualità è necessario che i pacchetti in cui è suddiviso il messaggio non subiscano un ritardo troppo grande tra uno e l'altro che porterebbe a dei "buchi" nell'ascolto, ossia, bisogna introdurre il concetto di *Qualità del Servizio*.

Bluetooth ha introdotto due



diversi tipi di collegamento fra i nodi all'interno di una Piconet, normalmente questi collegamenti vengono attivati in modo trasparente all'utente:

- **Asynchronous Connection Less (ACL):** questo è il collegamento normalmente utilizzato per il trasferimento dei dati. Connection Less significa che non è necessario stabilire una connessione logica fra due nodi prima di cominciare un trasferimento, ma ogni nodo può trasmettere un pacchetto ad un altro della Piconet in qualsiasi momento e poi si aspetta un pacchetto che attesta l'effettiva ricezione (Acknowledge ACK). Se il pacchetto ACK non viene ricevuto entro un tempo pre-stabilito il pacchetto viene ritrasmesso.
- **Synchronous Connection Oriented (SCO):** al contrario del collegamento precedente, qui occorre stabilire una connessione logica fra i due nodi interessati e fatto questo viene garantita una certa "qualità di servizio" riservando alcuni slot solamente per questo tipo di traffico che viene usato per la comunicazione audio. In questo modo viene garantito che la distanza temporale fra due pacchetti non supererà mai una data soglia.

SICUREZZA DEL COLLEGAMENTO

Con il termine sicurezza si intende la protezione dei dati che vengono scambiati via radio nei confronti di malinten-

zionati che se ne vogliono appropriare. Abbiamo infatti detto che le radio Bluetooth sono in grado di riconoscersi e formare spontaneamente una rete, ma come impedire questo se non lo vogliamo?

Innanzitutto, per creare una Piconet, è necessario che gli Slave rispondano alle richieste di identificazione del Master e molti dispositivi commerciali consentono di stabilire se il dispositivo stesso è "scopribile" o meno dagli altri. Quindi è necessario assicurarsi che questa modalità sia normalmente disabilitata se non vogliamo che gli altri "ci vedano", per poi abilitarla esplicitamente solamente quando è necessario.

Il Pairing

Un altro concetto molto importante a riguardo della sicurezza del Bluetooth è il concetto di Pairing (in inglese "appaiamento"): quando il Master (supponiamo che sia un PC con radio Bluetooth) ha effettuato la scansione per individuare gli altri nodi Bluetooth sotto copertura, può decidere di stabilire il collegamento con uno di questi. A questo punto verrà richiesto all'utente del PC di inserire un PIN code, cioè una specie di password formata da quattro cifre. Per stabilire la connessione Piconet anche all'utente del nodo Slave (che potrebbe essere un telefono cellulare) dovrà inserire un PIN code, che dovrà essere uguale a quello inserito sul PC. Una volta effettuata questa procedura i due nodi Bluetooth, PC e cellu-

lare, si ricorderanno di essere stati appaiati e non chiederanno più esplicitamente l'inserimento del PIN code agli utenti.

Criptaggio dei dati

Oltre al Pairing, che consente di evitare la creazione di connessioni indesiderate, il Bluetooth prevede la possibilità di criptare i messaggi scambiati via radio utilizzando una chiave lunga fino a 128 bit. E' chiaro che le contromisure di sicurezza da adottare devono aumentare con l'importanza dei dati stessi che vogliamo scambiare.

BLUETOOTH E LE ALTRE TECNOLOGIE

Bluetooth va a definire un nuovo concetto di rete wireless (la Private Area Network) che si aggiunge a quelli già esistenti (la Wide Area network WAN e la Local Area network LAN) che consente di avere collegamenti senza fili fra un computer e le due periferiche, ma grazie alla sua flessibilità è in grado di fare da interfaccia fra le altre tecnologie radio disponibili.

Reti GSM/GPRS

Tutti ormai siamo utenti della rete GSM per quanto riguarda il traffico voce e ne sfruttiamo anche le possibilità di trasferimento dati mediante gli SMS. L'evoluzione del GSM rivolto al trasporto dati è il GPRS, che pur utilizzando le infrastrutture radio preesistenti, supporta il protocollo TCP/IP e consente di trasferire dati con velocità che arrivano mediamente a 30Kbit/s (contro i 9,6Kbit/s del GSM). Lo step successivo che



porterà la velocità media di trasferimento a diverse centinaia di Kbit/s è la terza generazione di telefonia cellulare, l'UMTS. Quando la rete UMTS si sarà diffusa, darà la possibilità ai suoi utenti di accedere ad Internet o di scambiarsi contenuti multimediali ovunque si trovino.

Reti Wi-Fi

Questi sistemi si stanno diffondendo soprattutto in ambito indoor per fornire accesso wireless ad internet a banda larga, con velocità che oggi raggiungono anche i 100 megabit/s. La grossa differenza rispetto alle reti cellulari è che lavorano nella banda ISM e quindi non necessitano di licenze plurimiliardarie. Sono in corso progetti per ottimizzare questi sistemi in modo da poter trasportare la voce (c'è chi ha pensato alle cabine telefoniche wireless via Wi-Fi), rendendoli così preferibili in alcuni ambiti alla tecnologia UMTS, soprattutto perché contraddistinta da costi di gestione ed installazione notevolmente inferiori.

La connessione wireless globale

Lo scenario futuro più ottimistico è quello che prevede una integrazione delle diverse tecnologie in modo da permetterci di poter usare di momento in momento quella migliore. Supponiamo che esista un telefono cellulare che supporti contemporaneamente le tecnologie Bluetooth, Wi-Fi ed UMTS: quando siamo in ufficio il telefonino si aggancia automatica-

mente alla rete Wi-Fi aziendale, consentendoci di telefonare attraverso il Voice over IP (VoIP) che trasporta l'audio utilizzando una normale rete TCP/IP. Quando poi usciamo dall'ufficio, il telefono si aggancia automaticamente alla rete UMTS, dandoci la possibilità di trasferire audio e video ed anche di navigare in Internet mediante il nostro PC portatile al quale si collega via Bluetooth.

Affollamento dello spettro

Uno dei problemi più evidenti che sorge con il diffondersi dei dispositivi wireless è quello delle interferenze: infatti si ha un progressivo riempimento delle bande disponibili e con questo bisognerà fare i conti nel futuro prossimo. Basti pensare che Bluetooth e Wi-Fi attualmente condividono la medesima banda ISM a 2,4GHz. In pratica, quello che succede facendo operare contemporaneamente nella stessa area apparati Bluetooth e Wi-Fi, è una interferenza che finisce con abbassare le prestazioni in termini di velocità di trasferimento dei dispositivi. Sono, comunque, già stati pensati dei metodi che consentano di mitigare gli effetti delle interferenze, introducendo nei sistemi Bluetooth un Frequency Hopping intelligente, in cui prima di occupare un canale ci si accerta che sia effettivamente libero, cercando in questo modo di non sovrapporsi ad un eventuale canale Wi-Fi. Nel prossimo futuro verranno molto probabilmente rese disponibili nuove bande di fre-

quenza per queste applicazioni, che consentiranno un ulteriore sviluppo.

Nuove tecnologie

La ricerca segue anche altre direzioni ed una delle tecnologie più promettenti per i prossimi anni è l'**Ultra Wide Band** (UWB, www.uwb.org) che è rivoluzionaria rispetto ai sistemi di comunicazione che si basano sulla modulazione di onde sinusoidali. Infatti nell'UWB non si ha più un'onda continua, ma delle sequenze di impulsi di brevissima durata che hanno corrispondentemente un amplissimo spettro di frequenza che supera i 10GHz.

I promotori dell'UWB sostengono che una tecnica di trasmissione di questo tipo possa raggiungere agevolmente velocità di trasferimento di centinaia di megabit/s, ma il problema da risolvere è assicurarsi che questi impulsi ad ampio spettro non vadano a disturbare le comunicazioni tradizionali che lavorano nelle diverse zone dello spettro, si pensi in particolare alla strumentazione degli aerei, al sistema GPS ed ai radar.

CONCLUSIONE

Abbiamo visto quali sono le principali tecnologie wireless digitali e quali sono le loro principali applicazioni di oggi. Sicuramente questo è uno dei settori in cui i produttori di microelettronica sono più attivi e quindi le novità sono all'ordine del giorno con dispositivi sempre più piccoli e preformanti.