LO STANDARD BLUETOOTH™

1.1 INTRODUZIONE

Nato originariamente come progetto interno di *Ericsson*, lo standard *Bluetooth™*, operante nella banda ISM (Industrial Scientific Medical) *"license free"* (libera da licenza) a 2,4 GHz, aveva come obiettivo iniziale quello di permettere una comunicazione radio tra il telefono cellulare ed i vari accessori ad esso abbinabili (quali ad esempio il tastierino, l'auricolare, ecc..) mediante una soluzione integrata, piccola (la lunghezza di un fiammifero, vedi fig. 1.1), economica e con un consumo energetico molto ridotto.

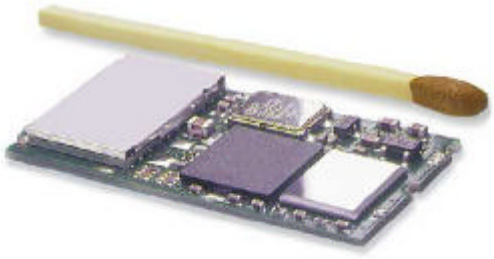

Fig. 1.1: Integrato Bluetooth™

Il progetto però ha avuto una risonanza maggiore del previsto presentandosi come una soluzione "unificatrice" per tutti i problemi di

interconnessione riguardanti quei dispositivi di uso quotidiano che, in qualche modo, hanno la capacità o la necessità di essere collegati tra loro, quali ad esempio il Notebook, stampante, telefonino, *PDA* (*Personal Digital Assistant*, agenda elettronica evoluta che scambia i dati con il pc desktop), autoradio, Navigatori Satellitari GPS, e altri ancora. Ciò ha spinto *Ericsson* ad allearsi con altre aziende, alcune delle quali in diretta concorrenza come la *Nokia*, per formare nel Maggio del 1998 il *Bluetooth Special Interest Group (SIG)*.

L'utilizzo delle onde radio per lo strato fisico della tecnologia *Bluetooth™* ha permesso i seguenti vantaggi:

- Aumentare la velocità di trasmissione dei dispositivi;
- Implementare sistemi di trasmissione *MULTICAST* (punto-multipunto);
- Interagire con le LAN (Local Area Network) preesistenti, in quanto lo standard Bluetooth, definendo un protocollo di trasmissione tra i vari dispositivi, consentirà di avere terminazioni wireless delle LAN aziendali, cosicché sarà possibile collegare terminali mobili alle LAN avvicinandoli ad una rice-trasmittente.

Ma perché il nome *Bluetooth* (che letteralmente significa "dente blu")? Questo era il soprannome di Harald II, re di Danimarca, che unificò quest'ultima e buona parte della Norvegia in un unico regno. Proprio per tale vocazione ad unire mondi diversi, la *Ericsson* decise il nome *Bluetooth™* per la tecnologia che si stava sviluppando.

1.2 GLI STANDARD PREESISTENTI E IL CONCETTO DI WPAN

Lo standard Bluetooth™ doveva però confrontarsi con le tecnologie wireless preesistenti quali:

- *DECT (Digital Enhacement Cordless Telecomunications)*, standard digitale criptato per telefonini cordless, utilizzante una modulazione GMSK, e avente un bit-rate massimo pari a 348 kbps. Presenta la caratteristica di permettere sia traffico dati, sia traffico voce;
- *IrDA (Infrared Device Application)*, tecnologia di interconnessione bidirezionale point-to-point, tramite infrarossi, tra dispositivi posizionati in visibilità reciproca ad una distanza massima di 1 m (e quindi poco versatile) e con un bit-rate massimo di 4Mbps. La sua poca versatilità ne ha effettivamente limitato lo sviluppo.
- *IEEE 802.11*, tecnologia per wireless LAN (Local Area Network), che a sua volta si articola in
  - *802.11a*, operante a 5,8 GHz e 40 GHz;
  - *802.11b*, operante nella banda ISM a 2,4 GHz, avente un bit-rate massimo di 11 Mbps;

Per dare maggiore enfasi al Bluetooth™ rispetto a tali tecnologie, il SIG introdusse allora un nuovo concetto di rete: la *WPAN (Wireless Personal Area Network)*. In pratica ogni individuo dispone di una rete che abbraccia tutti i suoi dispositivi di uso quotidiano, quali quelli precedentemente menzionati, come viene mostrato in fig. 1.2.

Fig. 1.2: Wireless Personal Area Network (WPAN)

Ognuna di queste reti può collegare un certo numero di dispositivi, ognuno dei quali può entrare o uscire dalla rete dinamicamente a seconda che esso rientri o meno nel raggio d'azione della stessa.

1.3 ESEMPI DI UTILIZZO

Di seguito sono riportati alcune possibili applicazioni della tecnologia Bluetooth™:

- Un'automobilista seduto al posto di guida, otterrà un collegamento vivavoce senza fili perché il suo cellulare (che in quel momento si troverà nel taschino della giacca) comunicherà direttamente con l'autoradio, e se vorrà chiamare un suo cliente selezionerà il nominativo sull'agenda elettronica che a sua volta lo invierà automaticamente al cellulare.

- In aeroporto, Susanna e Tommaso utilizzano i loro computer portatili Bluetooth™ ed i servizi di imbarco della linea aerea, attraverso il più vicino punto d'accesso (access point) Bluetooth™, per scoprire così che il loro volo è in ritardo di due ore. Dopo l'autenticazione di sicurezza, essi possono confermare i posti assegnati e ricevere le proprie carte d'imbarco digitali. Mentre Tommaso informa, via e-mail, l'hotel e l'agenzia di noleggio auto relativamente al loro ritardo, Susanna rivede i propri documenti per un nuovo contratto di fornitura. Ma ahimè, manca un allegato. Susanna allora effettua una connessione remota alla LAN aziendale, utilizzando il suo cellulare Bluetooth™, e scarica l'appendice mancante.

- Utilizzare il proprio cellulare come dispositivo cordless DECT all'interno della propria casa.

- Collegamento di memorie di massa aggiuntive ai personal computer.

- Utilizzare il proprio cellulare per controllare i comuni elettrodomestici (accendere il forno e regolarne la temperatura, accendere il televisore e cambiarne i canali, programmare il videoregistratore, ecc..).

1.4 SPECIFICHE BLUETOOTH™

1.4.1 Generalità

La tecnologia Bluetooth™ [1] realizza un collegamento radio a corto raggio, che mira a sostituire completamente i cavi per la connessione tra dispositivi fissi e portatili e che si propone come una tecnologia robusta, non molto complessa, con basse potenze trasmesse e a basso costo. Essa presenta un bit-rate massimo pari ad 1 Mbps

Bluetooth™ opera su una gamma di frequenza centrata sui 2.45 GHz nella banda ISM (Industrial Scientific and Medical band) suddivisa in 79 canali di ampiezza di 1 MHz ciascuno. La ISM è formalmente utilizzata per alcuni scopi professionali e solo recentemente è stata aperta in tutto il mondo ad un uso commerciale anche se con modalità e frequenze non completamente omogenee (fig. 1.3). Ad esempio, negli USA e in Europa il range di funzionamento è tra i 2400 ed i 2483.5 MHz mentre in Giappone la banda tra i 2400 ed i 2500 MHz è stata concessa per usi commerciali. Quindi, tale banda non è utilizzata in egual modo in tutto il mondo ed in funzione di dove ci si trova bisogna rispettare diverse regolamentazioni che nascono dall'esigenza di prevenire un uso arbitrario delle frequenze.

Country	Frequency Range	RF Channels
Europe* & USA	2400 - 2483.5 MHz	f = 2402 + k MHz
Japan	2471 - 2497 MHz	f = 2473 + k MHz
Spain	2445 - 2475 MHz	f = 2449 + k MHz
France	2446.5 - 2483.5 MHz	f = 2454 + k MHz

Fig. 1.3: Allocazione della ISM nei vari paesi

Inoltre Bluetooth™ è stato appositamente progettato per funzionare all'interno di ambienti con un forte disturbo radio. Infatti, il sistema adotta la tecnica *FHSS (Frequency Hopping Spread Spectrum)* che divide la banda in un certo numero di canali di salto centrati in frequenze diverse. Durante una trasmissione radio, il trasmettitore e il ricevitore saltano in frequenza da un canale all'altro secondo una sequenza pseudocasuale. Questa tecnica permette di combattere in modo efficiente fenomeni di interferenza e fading.

La modulazione utilizzata è una GFSK (Gaussian Frequency Shift Keying) con basso indice di modulazione (0.28÷0.35) in cui un bit "1" è rappresentato da una deviazione di frequenza positiva, mentre un bit "0" è rappresentato da una deviazione di frequenza negativa.

Per quanto riguarda il tipo di dati che Bluetooth™ consente di trasmettere, esso permette di gestire sia traffico isocrono (voce) mediante un canale sincrono full-duplex, sia traffico dati mediante un canale dati asincrono. In particolare può supportare o un canale dati asincrono, oppure fino a tre canali voce sincroni, oppure ancora un canale che contemporaneamente supporti dati asincroni e voce sincrona. Il canale voce è un canale sincrono di 64 kbps, mentre quello dati può essere o 721 kbps in downstream e 57,6 kbps in upstream, oppure bilanciato con 432 kbps in entrambi i sensi.

Il sistema radio Bluetooth™ [1] consiste essenzialmente in una unità radio, una unità per il controllo del collegamento e una unità di supporto per la gestione del collegamento (*Bluetooth Link Manager*) e per l'interfaccia con l'esterno (come mostrato in fig. 1.4):

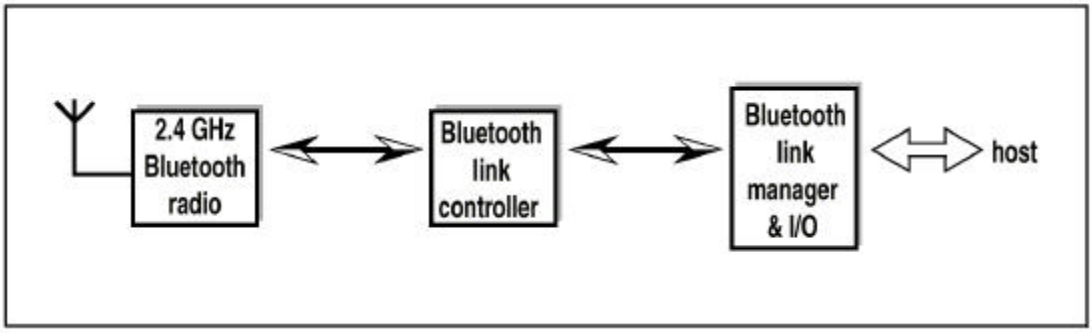

Fig. 1.4: Schema a blocchi di una generica unità Bluetooth™

Il Bluetooth™ prevede collegamenti punto-punto (nel qual caso sono coinvolti solo due dispositivi) e collegamenti punto-multipunto (nel qual caso invece il canale è opportunamente condiviso tra le varie unità collegate). Due o più unità che condividono lo stesso canale costituiscono una rete che prende il nome di *"piconet"*. In ogni piconet è possibile individuare un dispositivo detto "*Master"*, che gestisce il canale associato alla piconet stessa mentre gli altri sette dispositivi sono detti "*Slave"*. In pratica, la comunicazione tra le varie unità che partecipano alla piconet viene attivata in funzione dei servizi offerti da ognuna di esse e dalle esigenze delle altre. Inoltre uno slave può avere più master di altrettante piconet nel suo raggio di azione ed inoltre, un master di una piconet può essere a sua volta slave di un'altra piconet. Quindi, almeno in linea teorica, una rete Bluetooth™ può estendersi senza limiti. Nella pratica, però, le prestazioni, sono accettabili fino ad un massimo di 10 piconet interconnesse. Una siffatta rete prende il nome di *"Scatternet"*. In fig. 1.4 sono ripotati tutti le possibili configurazioni tra dispositivi Bluetooth™: possiamo vedere in a) una semplice rete piconet con un solo master ed un solo slave (collegamento punto-punto), in b) abbiamo una configurazione multi-slave (punto-multipunto) e infine in c) abbiamo una configurazione Scatternet.

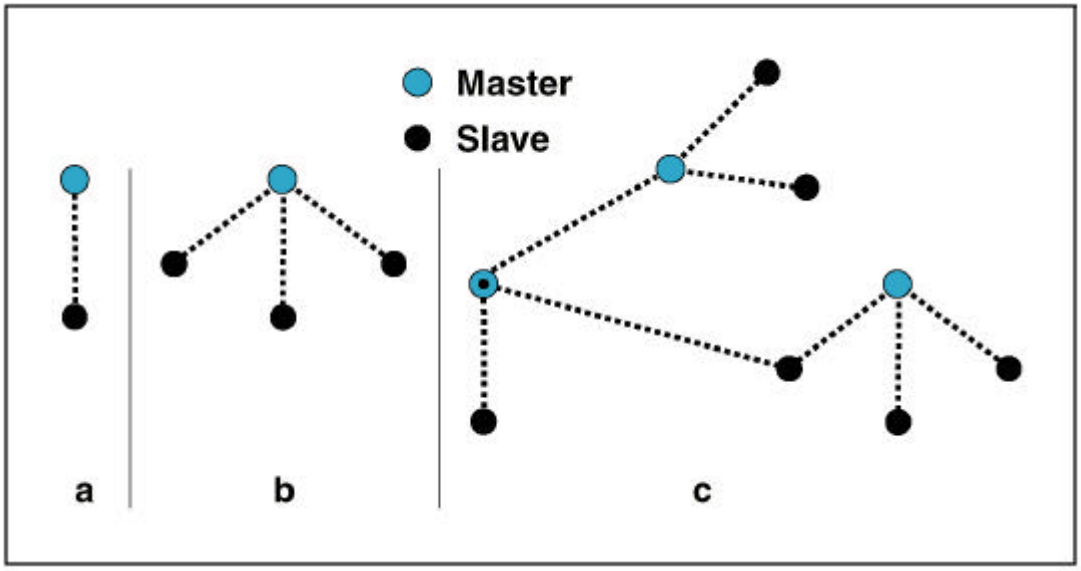

Fig. 1.4: Esempio di configurazioni tra dispositivi Bluetooth™.

Per quanto riguarda le potenze trasmesse, esse sono al massimo di 100mW, sufficienti per operare con tratte che vanno dai 10 centimetri ai 10 metri, distanze ritenute valide per gli scopi di connettività personale che il SIG si è prefisso.

1.4.2 Canale fisico

I canali Bluetooth usano lo schema *FH/TDD (Frequency Hopping Time Division Duplex)* [6], come mostra la fig. 1.5.

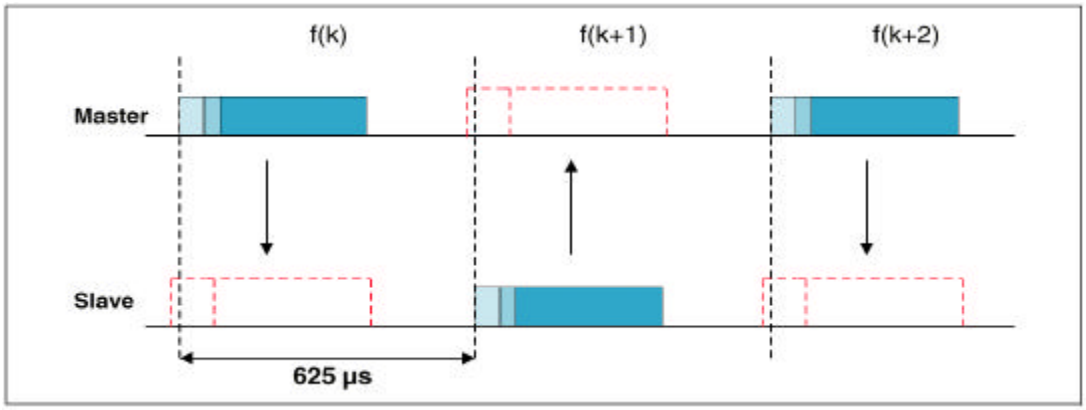

Fig. 1.5: Tecnica FH/TDD (Frequency Hopping Time Division Duplex)

Ogni canale è rappresentato da una sequenza di salti pseudocasuale tra le 79 possibili radio-frequenze in cui è stata suddivisa la banda ISM. La sequenza di salti è unica nell'ambito di una piconet ed è determinata dall'indirizzo del dispositivo master e la tempificazione dei salti è imposta dal clock dello stesso. Il canale è suddiviso a sua volta in time slot di durata pari a 625μs. Ogni slot, utilizzabile in entrambi i versi della trasmissione per trasmettere un pacchetto, corrisponde ad una particolare frequenza della sequenza di salto (vedi fig. 1.5). Il valore nominale dell'hop-rate è di 1600 hps/s. In un time slot, master e slave possono trasmettere pacchetti. Con la tecnica TDD (fig. 1.5) master e slave trasmettono alternativamente: il master trasmette negli slot pari, mentre lo slave negli slot dispari. Il pacchetto trasmesso da un dispositivo (master o slave che sia) non deve avere durata maggiore di cinque time slot. La frequenza di salto è costante per tutta la durata di un pacchetto. Quindi, nel caso in cui un pacchetto abbia un durata maggiore di uno slot, abbiamo la situazione di fig. 1.6.

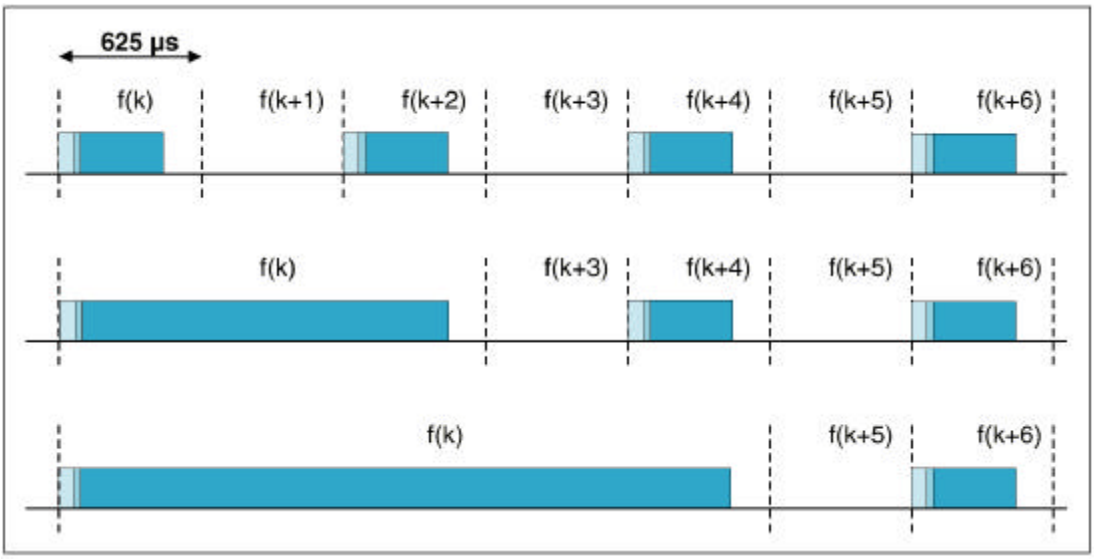

Fig. 1.6: Frequency-Hop per pacchetti di durata maggiore di uno slot.

1.4.3 Tipi di collegamento

Vi possono essere due tipi di collegameto tra il master e gli slave di una generica piconet, a seconda del tipo di traffico che si vuole trasmettere:

- *SCO Link (Synchronous Connection Oriented)*: collegamento punto-punto simmetrico tra il master e uno slave. Esso ha la caratteristica di riservare uno slot in un verso della trasmissione e lo slot consecutivo nel verso opposto. Per tale motivo esso può essere considerato come una connessione a commutazione di circuito. Il master può mantenere fino a tre SCO Link con lo stesso slave o con slave diversi mentre uno slave può mantenere fino a tre SCO Link con il master o, nel caso in cui sia master di una piconet e contemporaneamente slave in un'altra, può mantenere al massimo due SCO Link. I pacchetti persi non vengono ritramessi. Tale collegamento è pensato per il traffico voce.

- *ACL Link (Asynchronous Connectionless)*: non vi sono time slot riservati e quindi il master può scambiare pacchetti con ognuno degli slave. Quindi l'ACL Link realizza un collegamento a commutazione di pacchetto tra il master e tutti gli slave partecipanti alla piconet, permettendo cosi anche il multicast. Pacchetti errati vengono ritrasmessi per assicurare la correttezza dei dati.

1.4.4 Correzione di errore e ritrasmissione

Per assicurare la correttezza dei dati ricevuti in un ACL Link, vengono utilizzati sia codici a correzione di errore quali:

- Codice **1/3** *Forward Error Correction* (**FEC**) che consiste nel trasmettere nel pacchetto stesso una copia dei dati utili;
- Codice **2/3FEC** che è un codice di Hamming;

sia la ritrasmissione dei pacchetti errati mediante un

- Protocollo *Automatic Repeat Request* (**ARQ**).

I codici FEC vengono utilizzati laddove si desidera ridurre il numero di ritrasmissioni di pacchetti errati. Quando però i codici FEC non sono sufficienti a garantire la correttezza dei dati, interviene il protocollo ARQ che realizza la ritrasmissione automatica dei pacchetti errati in caso di mancato riscontro (acnowldgement) della ricezione del pacchetto da parte del ricevitore.

1.4.5 Modalità di funzionamento delle unità Bluetooth

Una volta stabilita una connessione le unità Bluetooth possono essere in quattro stati diversi:

- **Active Mode**: l'apparecchio risulta attivo in una comunicazione o in trasmissione o in ricezione. Il master in questo caso invia agli slave in tale modalità il segnale di sincronismo ad ogni slot.
- **Sniff Mode**: viene ridotto il ciclo di attività di uno slave. In pratica, nel caso di un ACL link, il master può cominciare una trasmissione con lo slave in questione solo in un insieme ridotto e ben determinato di time slot. Tali slot sono chiamati *sniff slots*, e sono spaziati regolarmente con un intervallo di durata T_{sniff}, durante il quale lo slave può andare in una modalità *low-power* o partecipare ad altre piconet.
- **Hold Mode**: al fine di ottimizzare i consumi energetici, durante un intervallo di tempo predefinito dal master e dallo slave coinvolti, viene tolta la possibilità allo slave di effettuare comunicazioni asincrone o di crearne nuove sincrone.
- **Park mode**: si utilizza quando un dispositivo non deve partecipare ad una trasmissione, ma vuole rimanere sincronizzato per eventualmente farvi parte in un secondo momento. In questo modo deve semplicemente curare la sincronizzazione con i salti di frequenza della piconet.

Tutti gli apparecchi Bluetooth per default sono in **standby** (in attesa). Quando l'apparecchio è in attesa, ogni 11.25 ms completa un ciclo di scansione per sentire se ci sono comunicazioni da altri apparecchi.

La scansione effettuata può essere di due tipi:

- **Page Scan**, con la quale l'apparecchio stesso "cerca" un collegamento con un altro apparecchio Bluetooth;
- **Inquiry Scan**, molto simile alla precedente, ma con la differenza che l'apparecchio effettua una scansione qualitativa per "capire" quali apparecchi sono disponibili nell'area limitrofa ed approntare i necessari protocolli per il collegamento.

I risultati di una scansione, come abbiamo visto, possono essere molteplici: *active*, *hold*, *sniff*, e *park*. Naturalmente se non vi sono presenti apparecchi, oppure se gli utenti degli altri apparecchi non desiderano la comunicazione, la connessione non viene effettuata e l'apparecchio rimane in fase di scanning.

1.4.6 Sicurezza

La tecnologia Bluetooth garantisce tre differenti livelli di sicurezza:

- **“non-secure”**: non abilita l'apparecchiatura all'esecuzione di qualunque procedura che richieda sicurezza;
- **“service-level security”**: concede una maggior flessibilità all'apparecchiatura che sta processando una pluralità di applicazioni in parallelo, in pratica le permette di scegliere fra differenti livelli di sicurezza;
- **“link level security”**: nell’apparecchiatura le procedure di sicurezza sono completate prima che la macchina si colleghi, per

capire l'identità all'altra estremità del collegamento; la stessa fornisce l'autenticazione, l'autorizzazione ed i servizi di crittografia;

L'autenticazione è un passaggio chiave nella tecnologia Bluetooth, per consentire alle diverse apparecchiature di "conversare" con piena fiducia reciproca. I servizi di autenticazione permettono che due dispositivi possano decidere se un collegamento sia effettuato o meno. Una volta che un collegamento venga stato stabilito, un livello di sicurezza maggiore può essere applicato utilizzando la crittografia.

1.4.7 Lo Stack dei protocolli Bluetooth

Facendo riferimento alla fig. 1.7, in cui i protocolli specifici dell'architettura Bluetooth sono riportati in blu, abbiamo:

- **Bluetooth Radio:** è il livello più basso dello standard in cui sono definite tutte le specifiche del canale radio (banda ISM, e sua divisione) e i requisiti cui devono soddisfare i ricetrasmettitori Bluetooth;
- **Bluetooth Baseband:** in questo livello viene gestito il canale fisico e fornendo servizi quali la correzione degli errori, la selezione dei salti di frequenza e la sicurezza. Il protocollo di questo livello è implementato mediante il Link Controller che cooperando con il Link Manager fornisce ai livelli superiori servizi quali le connessioni e il controllo della potenza trasmessa.

Esso gestisce inoltre i collegamenti sincroni e asincroni, realizza la procedure di *page scan* e *inquiry scan* prima menzionate. Infine, in esso è realizzata la tecnica del Time-Division Duplex (TDD);

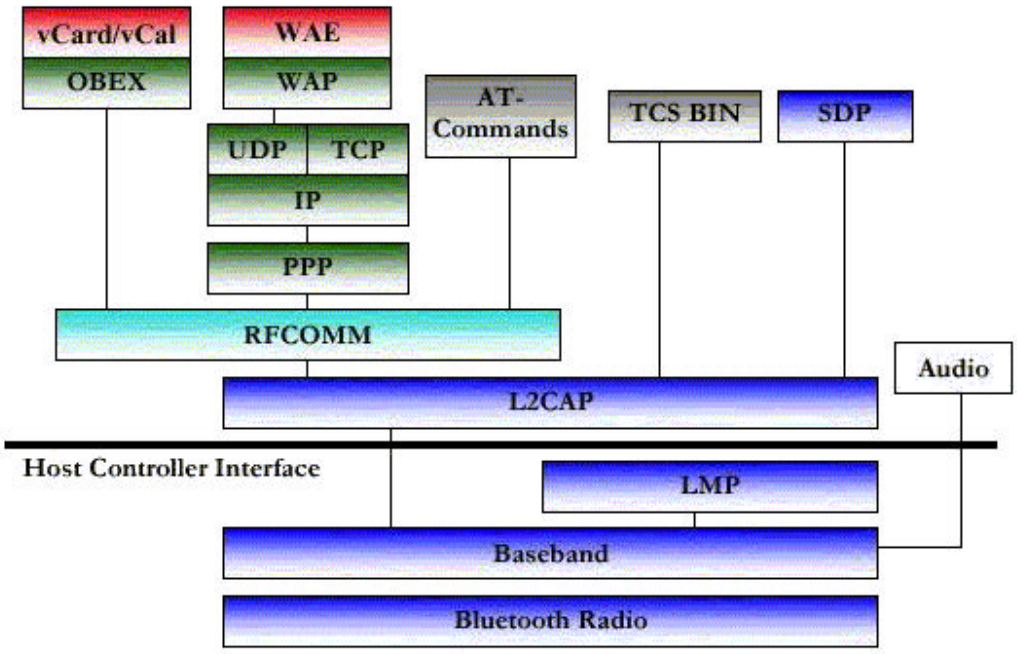

Fig. 1.7: Architettura a strati del Bluetooth

- **LM (Link Manager):** mediante questo livello fornisce servizi quali il set-up delle connessioni, l'autenticazione, la configurazione dei link. Esso coopera con i livelli LM degli altri dispositivi Bluetooth mediante il *Link Manager Protocol (LMP)*. Per svolgere tutte queste funzioni, tale livello utilizza i servizi fornitigli dal Link Control sottostante;
- **L2CAP (Logical Link Control and Adaptation Layer Protocol):** è posizionato al di sopra del livello Baseband e può essere visto come un livello Data Link. Esso frnisce ai livelli superiori sia servizi orientati alla connessione (traffico voce), sia

servizi connectionless (per traffico dati), realizzando inoltre il multiplexing dei pacchetti ed eventualmente, la loro segmentazione e riassemblaggio;

- **RFCOMM protocol:** è un semplice protocollo di trasporto che, usando i servizi forniti dal L2CAP, realizza l'emulazione della porta seriale RS232;
- **SDP (Service Discovery Protocol):** è il protocollo che consente di determinare le tipologie di servizi presenti e disponibili nella piconet sia in una modalità server (ossia che fornisce il servizio) sia client (che richiede il servizio). Nella modalità server consentirà ad un dispositivo di interrogarlo sui servizi e protocolli supportati, quindi renderli disponibili mentre, nella modalità client consentirà l'interrogazione dei dispositivi connessi alla piconet per avere informazioni.

1.5 INTERFERENZE

La decisione da parte dei fondatori del Bluetooth di utilizzare la banda ISM a 2,4 GHz fu motivata principalmente dal fatto che si trattava di uno spettro di frequenze aperto, ove cioè è possibile la trasmissione in RF senza interventi da parte del governo. Ma, e qui sta il problema, la banda ISM non è stata originariamente riservata alle comunicazioni e questo comporta che una serie di elettrodomestici (forni a microonde, illuminazione industriale, sistemi informatici ed altri) che utilizzano proprio la frequenza 2,45 GHz producano non trascurabili interferenze a causa delle loro emissioni a bassa ed alta potenza. Inoltre, non vi è alcun

limite, se non quello oltre il quale le onde diventano nocive alla salute, che regoli le trasmissioni in RF operate in questa banda di frequenza. Il SIG ha infatti registrato molte interferenze in zone ad alta densità di popolazione, particolarmente durante l'ora di pranzo, proprio quando è maggiore l'utilizzo di apparecchi come i forni a microonde.

Va detto però che, sicuramente i principali prodotti Bluetooth non saranno utilizzati per periodi molto lunghi nell'arco della giornata, e non richiederanno un'affidabilità del 100% per il trasferimento dei dati.

Un altro aspetto da considerare è quello delle interferenze con gli standard preesistenti. Infatti, lo standard IEEE 802.11b per le Wireless LAN opera anch'esso a 2,4 GHz. Bisogna però ricordare che tale standard opera su distanze fino a 100m mentre Bluetooth opera fino a 10m, distanza sufficiente per realizzare le WPAN prima menzionate. Inoltre, i livelli di potenza trasmessi nei due standard sono diversi.

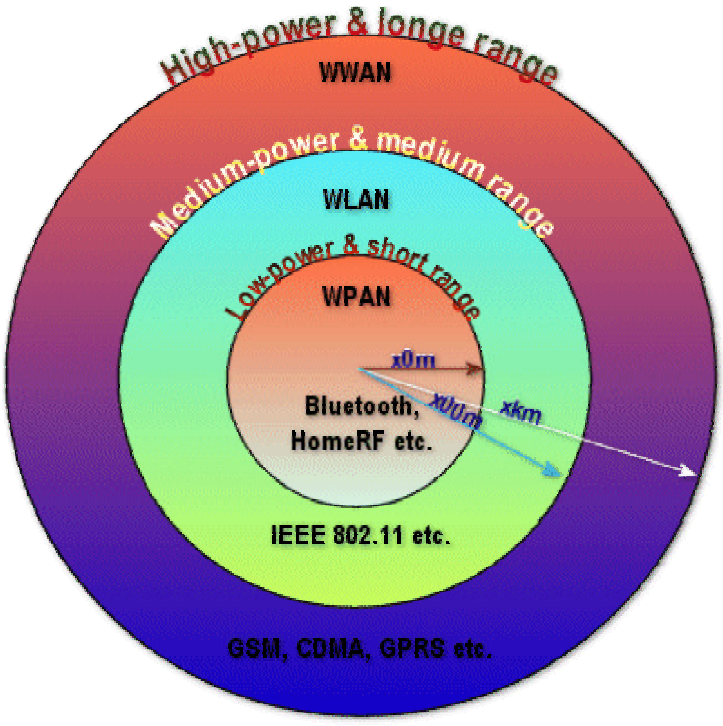

Fig. 1.8: Le attuali tecnologie wireless

Quindi, come mostrato in fig. 1.8, il panorama delle tecnologie wireless può essere suddiviso in termini di distanze e di potenze trasmesse, ove Bluetooth e 802.11b lavorano su range e distanze diverse. In pratica 802.11b si sta affermando come una valida alternativa alle attuali LAN cablate, mentre Bluetooth è pensato per realizzare una completa interconnettività tra i dispositivi di uso personale.