Università degli Studi di Padova

Dipartimento di Ingegneria dell'Informazione
Corso di Laurea in Ingegneria dell'Informazione

Confronto tra Bluetooth Basic Rate e Bluetooth Low Energy

Relatore:
Prof. Stefano Tomasin

Laureanda:
Alessia Tiberto

Anno Accademico 2012/2013

Indice

Capitolo 1

Introduzione

Il Bluetooth è uno standard di trasmissione presente in moltissimi dispositivi di uso comune, come ad esempio cellulari, cuffie, auricolari, ecc.
Di questo standard esistono diverse versioni, l'ultima in ordine cronologico è il Bluetooth Low Energy, uscita nel giugno 2010. Questo standard ha introdotto molte novità tra cui la più significativa è il bassissimo consumo di energia se confrontato con lo standard classico Bluetooth Basic Rate.

Ciò che si farà nei prossimi capitoli è capire che differenze ci sono tra Bluetooth Low Energy e Bluetooth Basic Rate, seguendo la suddivisione del modello ISO/OSI, e determinare quali vantaggi hanno portato.
Nel primo capitolo verrà introdotto lo standard Bluetooth con i suoi aspetti e terminologie principali; nel secondo capitolo si confronteranno gli standard a livello fisico in termini di trasmettitore, ricevitore, modulazione e frequenze utilizzate.
Nel terzo capitolo si parlerà di modalità di accesso al mezzo e trasmissione dei pacchetti; verranno inoltre introdotti alcuni aspetti relativi alla sicurezza e alle modalità con cui è possibile testare il dispositivo. Nel quarto capitolo infine verranno trattati i profili Bluetooth e in che modo essi possono essere realizzati.
Nella pagina seguente una tabella riassume gli argomenti che verranno trattati, suddivisi nei livelli fisico, datalink e applicazione del modello ISO/OSI.

		Bluetooth Basic Rate	**Bluetooth Low Energy**
APPLICAZIONE	Profili	SDP (Service Device Discovery) →GAP (Generic Access Profile) + protocolli secondari	ATT (Attribute Protocol) → GATT (Generic Attribute Profile)
DATALINK	Modalità di test	Link e Non-Link Test Mode	Non-Link (Direct) Test Mode
	Sicurezza	Protocollo Link Manager	Protocollo Security Manager
	Formato dei pacchetti	pacchetti diversi per ciascun tipo di trasporto logico, lunghezza 68 – 2871 bits	unico formato di pacchetto, 2 PDU per canali data e advertising, lunghezza 80 – 376 bits
	Trasporto logico	Sincrono, asincrono	Solo asincrono
	Trasmissione pacchetti	Slots da 625 μs	Eventi di lunghezza variabile
	Stati del dispositivo	3 stati (standby, connection, park) e 7 sottostati Slave: 3 modalità (active, sniff, hold)	5 stati: standby, advertising, scanning, initiating, connection (master/slave)
FISICO	Canali fisici	79 canali da 1 MHz	40 canali da 2 MHz suddivisi in canali data e canali advertising
	Modulazione	GFSK (BR), π/4-DQPSK (EDR 2Mbs) e 8DPSK (EDR 3Mbs)	GFSK
	Ricevitore	Bit Error Rate 0.1% sensibilità -70 dBm	Bit Error Rate 0.1% sensibilità -70 dBm
	Trasmettitore	3 classi di potenza	Potenza minima e massima

Capitolo 2

Lo standard Bluetooth

2.1 Cos'è Bluetooth?

Bluetooth è uno standard tecnologico per le trasmissioni wireless a corto raggio tra dispositivi che possiedono chip compatibili.
Esso fu inizialmente sviluppato dalla compagnia Ericsson nel 1994, ma il suo successo e la sua diffusione sono dovuti all'organizzazione Bluetooth Special Interest Group (SIG), un gruppo di aziende fondato nel 1998 che si è occupato della ricerca e sviluppo di questo standard.
Bluetooth è stato progettato per offrire un'alternativa a basso costo e basso consumo al Wi-Fi a discapito del raggio di trasmissione, che è notevolmente più corto (al massimo 100 metri), e della velocità di trasmissione, che non supera i 721.2 kbps nella versione classica detta Bluetooth Basic Rate e può raggiungere i 3 Mbit/s con la funzione opzionale Enhanced Data Rate.
Un motivo del successo del Bluetooth è quello di poter personalizzare i chip a seconda del tipo di dispositivo su cui deve essere impiantato, creando i cosiddetti profili. Un *profilo* è un insieme di protocolli specifici che, assieme a quelli standard, permettono l'aggiunta di nuove funzioni, come ad esempio la ricezione di dati da strumentazione mediche (Health Device Profile) oppure collegare il cellulare all'auto per ascoltare della musica (Hands-Free Profile). Tutto questo però comporta dei vincoli nell'utilizzo dei vari dispositivi, poiché la comunicazione può essere stabilita solo tra profili compatibili.
La ricerca del SIG nel corso dell'ultimo decennio ha cercato di migliorare le prestazioni del Bluetooth in termini di consumo energetico, arrivando a presentare nel 2010 lo standard Bluetooth Low Energy che, grazie ad alcuni cambiamenti riguardanti tutti i livelli dello stack protocollare, ha ridotto i

consumi di potenza fino a 0.01 mW. Un consumo così basso rende il Bluetooth Low Energy ideale per quelle applicazioni che non richiedono un flusso di dati continuo ma accessibilità al dispositivo 24/24 h, come ad esempio le strumentazioni mediche.

2.2 Come funziona?

Lo standard è stato aggiornato nel corso degli anni, aggiungendo configurazioni specifiche per le diverse esigenze ma sempre basandosi sulle stesse linee guida della prima versione uscita nel 1998.
La comunicazione si basa sulla trasmissione di *pacchetti*, ovvero gruppi di bits che contengono non solo l'informazione vera e propria ma anche dati aggiuntivi per il riconoscimento e la sincronizzazione tra dispositivi.
I dispositivi trasmettono nella banda ISM (Industrial, Scientific and Medical) 2.4 GHz utilizzando la tecnologia FHSS (Frequency-Hopping Spread Spectrum), ovvero suddividendo la banda in frequenze intervallate tra di loro (dette *canali*) su cui i dispositivi si sincronizzano per la comunicazione. I dispositivi periodicamente cambiano canale, secondo una sequenza pseudo-random chiamata *hopping sequence*.
La configurazione base di trasmissione vede coinvolti due dispositivi, di cui uno assume il ruolo di *master* e l'altro di *slave*. Il master ha il compito di gestire la comunicazione (inizio, sincronizzazione, termine) mentre lo slave si limita a seguire le istruzioni del master.
Un master può collegarsi con più slaves, dando così origine ad una configurazione detta *piconet*. Le piconets possono essere collegate tra loro attraverso i loro master oppure stabilendo un collegamento tra un master e uno slave non appartenenti alla stessa piconet, per formare una rete chiamata *scatternet*.

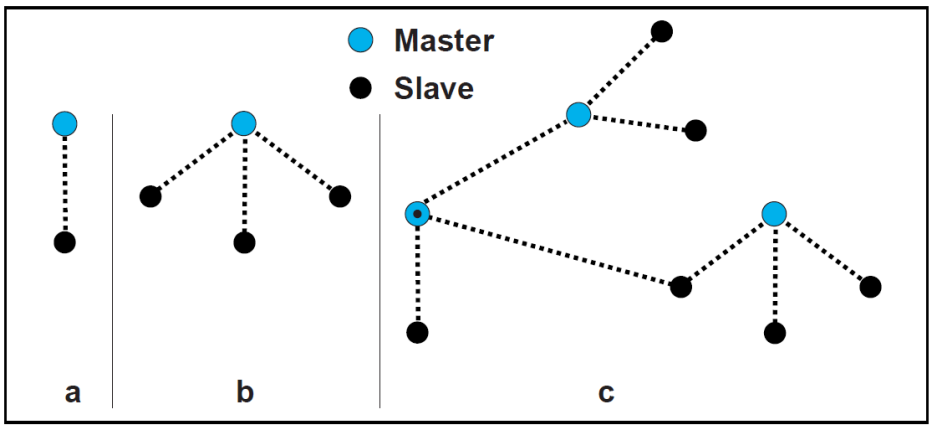

Figura 2.1: Piconet con un solo slave (a), piconet con più slaves (b), scatternet (c)

Capitolo 3

Confronto a livello fisico

La Figura 3.1 mostra uno schema delle principali componenti fisiche di un dispositivo Bluetooth. A sinistra è rappresentato il circuito digitale integrato su cui sono implementati i protocolli base per il funzionamento dello standard, mentre a destra sono schematizzati i circuiti per la trasmissione e ricezione del segnale fisico.
La selezione del circuito di trasmettitore o ricevitore è affidata ad uno switch posto dopo l'antenna.

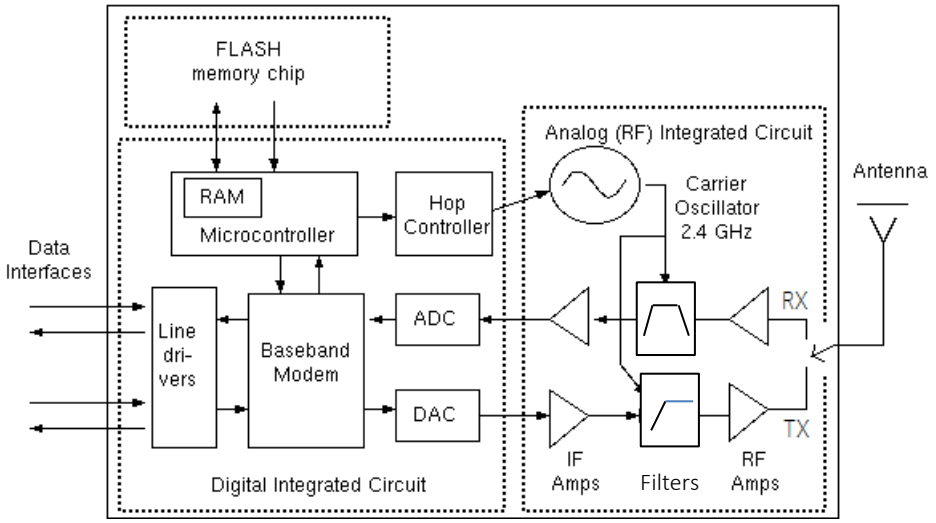

Figura 3.1: Schema a blocchi di un chip Bluetooth

3.1 Trasmettitore

Il modulo del trasmettitore è composto principalmente da:
- convertitore digitale-analogico (DAC)
- filtro gaussiano
- un mixer collegato ad un oscillatore
- un amplificatore di potenza.

Una volta convertito in analogico dal DAC, il segnale attraversa il filtro gaussiano, che smorza le transizioni tra valori alti e bassi di tensione; poi entra nel mixer che, assieme all'azione dell'oscillatore, modula il segnale generando una forma d'onda con frequenza nominale quella scelta nella fase di hopping della piconet a cui il dispositivo appartiene.
Infine il segnale viene amplificato e trasmesso dall'antenna.

Potenza del trasmettitore

I dispositivi Bluetooth Basic Rate sono suddivisi in tre classi a seconda della loro potenza in uscita. Ciascuna classe è caratterizzata da una potenza massima e una potenza minima all'output e, in base a questi valori, è definita la distanza entro la quale il dispositivo è in grado di comunicare. [1]

Classi di potenza	Potenza massima all'output	Potenza minima all'output	Distanza
1	100 mW (20 dBm)	1 mW (0 dBm)	~ 100 m
2	2.5 mW (4 dBm)	0.25 mW (-6 dBm)	~ 10 m
3	1 mW (0 dBm)	N/A	~ 1 m

Figura 3.2: Classi di potenza per trasmettitori Bluetooth Basic Rate

Nel Bluetooth Low Energy invece non ci sono suddivisioni in classi di potenza ma vengono forniti solo i valori di potenza massima e minima all'output del trasmettitore e un valore approssimativo della massima distanza raggiungibile.

Potenza massima all'output	Potenza minima all'output	Distanza
10 mW (10 dBm)	0.01 mW (-20 dBm)	~ 50 m

Figura 3.3: Valori di potenza all'output e distanza per trasmettitore Bluetooth Low Energy

La bassa potenza richiesta all'output è la caratteristica principale dello standard Bluetooth Low Energy e questo risultato è dovuto a varie modifiche fatte rispetto alla versione classica, tra cui la riduzione del numero di frequenze e l'uso di pacchetti più corti. Tutte queste modifiche verranno approfondite nei capitoli successivi.

3.2 Ricevitore

Il modulo del ricevitore è composto da:

- un amplificatore di potenza
- un mixer con oscillatore
- filtro IF (Intermediate Frequency)
- convertitore analogico-digitale (ADC).

Il segnale ricevuto dall'antenna, viene prima amplificato e poi introdotto nel mixer che, assieme all'oscillatore, ne effettua la demodulazione.
La frequenza dell'oscillatore, come nel caso del trasmettitore, è quella scelta in base alla sequenza di hopping della piconet della quale il dispositivo fa parte.
Il segnale così ottenuto quindi attraversa un filtro IF che lo amplifica alla frequenza intermedia, risultante dalla differenza tra le frequenze del segnale dell'oscillatore e il segnale all'ingresso del mixer, ed infine entra nel convertitore ADC che lo trasforma in segnale digitale.

Le specifiche fornite dallo standard per il ricevitore sono BER (Bit Error Ratio) di valore 0.1% e livello di sensibilità -70 dBm.

3.3 Modulazione del segnale

La modulazione del segnale è di tipo GFSK (Gaussian Frequency-Shift Keying) sia per la versione Bluetooth Basic Rate che per la versione Bluetooth Low Energy.
Se invece con lo standard Bluetooth Basic Rate viene utilizzata la funzione Enhanced Data Rate, la trasmissione di un singolo pacchetto utilizza due tipi diversi di modulazione: modulazione GFSK per la prima parte e modulazione PSK (Phase-Shift Keying) per la seconda parte.

Modulazione GFSK

La modulazione GFSK è un tipo di modulazione che agisce sulla frequenza del segnale d'ingresso. Per il valore logico "1" genera uno scostamento positivo fd dalla frequenza nominale Ft del segnale, mentre per il valore logico "0" genera uno scostamento negativo sempre di ampiezza fd, che è determinato dall'indice di modulazione utilizzato. Infatti indice di modulazione = 2*fd*T dove T rappresenta il periodo del segnale, che è 1μs. Questo indice assume valori diversi per i due standard.
Per Bluetooth Basic Rate l'indice di modulazione varia da 0.28 a 0.35 e perciò fd può assumere un valore da 140 a 175 KHz, mentre nel Bluetooth Low Energy l'indice di modulazione varia da 0.45 a 0.55 e fd assume valori da 225 a 275 KHz.
Un altro parametro definito nella modulazione GFSK è BT (larghezza di banda * periodo del segnale) di valore 0.5.

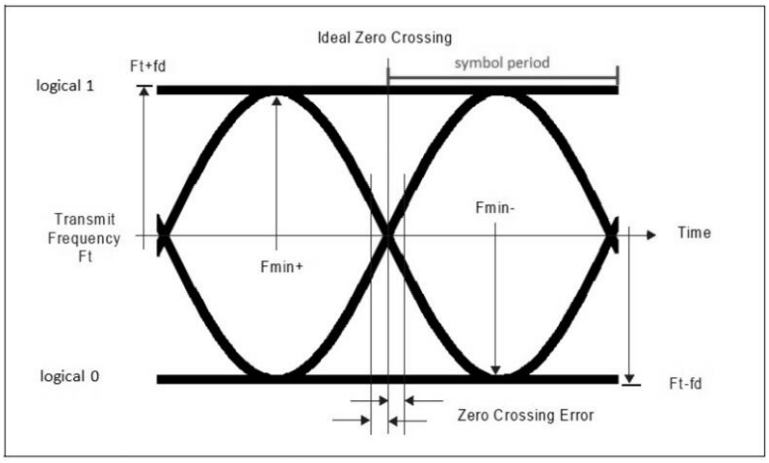

Figura 3.4: Definizione dei parametri della modulazione GFSK

Modulazione PSK

La modulazione PSK determina uno scostamento della fase del segnale di ampiezza φ a seconda dei valori dei bit in entrata.

Per una trasmissione da 2 Mbit/s viene utilizzata la modulazione π/4 DQPSK (π/4 rotated Differential encoded Quaternary Phase Shift Keying). Esistono due tipi di codifiche applicabili a questa particolare modulazione ma nel caso del Bluetooth Enhanced Data Rate si utilizza la codifica di Gray che mappa coppie di bit formate dal bit in ingresso e dall'ultimo bit ricevuto.

b_{k-1}	b_k	φ
0	0	π/4
0	1	3π/4
1	1	-3π/4
1	0	- π/4

Figura 3.5: Codifica di Gray

Per una trasmissione da 3 Mbit/s invece si utilizza la modulazione 8DPSK (8-ary Differential Phase Shift Keying), la cui codifica utilizza terne di bit formate dal bit in ingresso e dagli ultimi due bit ricevuti.

b_{k-2}	b_{k-1}	b_k	φ
0	0	0	0
0	0	1	π/4
0	1	1	π/2
0	1	0	3π/4
1	1	0	π
1	1	1	-3π/4
1	0	1	- π/2
1	0	0	- π/4

Figura 3.6: Codifica della modulazione 8DPSK

La differenza principale tra le tre diverse modulazioni utilizzate nello standard Bluetooth è il numero di bit utilizzati per identificare un unico simbolo: l'aumentare dei bit comporta l'aumento della velocità di trasmissione ma ciò avviene a discapito della potenza assorbita, che è maggiore rispetto alla modulazione GFSK.

La scelta di utilizzare la modulazione GFSK invece della modulazione PSK nello standard Bluetooth Low Energy è quindi giustificata dal volere un consumo di potenza il più basso possibile e, sempre per questo scopo, si è deciso di utilizzare un indice di modulazione diverso, il cui valore permette di risparmiare potenza. [2]

3.4 Determinazione dei canali fisici

A livello fisico vengono determinati i cosiddetti canali fisici, frequenze intervallate tra di loro alle quali possono lavorare i dispositivi.
Queste frequenze sono scelte nella banda ISM 2.4 GHz, la quale ha frequenza disponibili diverse a seconda del paese in cui ci si trova. Negli Stati Uniti, in Europa e nella maggior parte del mondo la banda ISM varia da 2.400 a 2.4835 GHz, ma in Spagna, Francia e Giappone la banda è più ristretta e ciò pone un limite la numero di canali che si possono individuare.

Dalla Figura 3.7 si può notare che ad inizio e fine banda sono tenuti liberi degli intervalli di frequenze di qualche MHz: ciò serve ad evitare interferenze con altre trasmissioni nelle bande attigue.

Luogo Geografico	**Range**	**Banda di guardia inferiore**	**Banda di guardia superiore**
USA, Europa e maggior parte del mondo	2.400-2.4835 GHz	2 MHz	3.5 MHz
Spagna	2.4450-2.4750 GHz	4 MHz	4 MHZ
Francia	2.4465-2.4835 GHz	7.5 MHz	7.5 MHz
Giappone	2.4710-2.4970 GHz	2 MHz	2MHz

Figura 3.7: Banda ISM nei vari paesi

Nel Bluetooth Basic Rate vengono individuati 79 canali (23 in Francia, Spagna e Giappone), con distanza 1 MHz l'uno dall'altro per ridurre eventuali interferenze con i canali adiacenti.
I canali sono determinati nel seguente modo:

Luogo Geografico	**Canali Radio**
USA, Europa e maggior parte del mondo	f=2402+k MHz, k=0,…,78
Spagna	f=2449+k MHz, k=0,…,22
Francia	f=2454+k MHz, k=0,…,22
Giappone	f=2473+k MHz, k=0,…,22

Figura 3.8: Determinazione dei canali fisici per Bluetooth Basic Rate

Nel Bluetooth Low Energy i canali definiti nella banda 2.400-2.4835 GHz sono 40, distanti tra di loro 2 MHz. Le frequenze sono determinate in questo modo:

$f=2402+k*2$ MHz, $k=0, \dots ,39$

Nell'ultimo decennio Spagna, Francia e Giappone si sono adeguati alle regolamentazioni standard per la banda ISM, rendendo non più necessario sviluppare un metodo alternativo per la determinazione dei canali.

Si vedrà nel capitolo successivo come la scelta di utilizzare un numero inferiore di frequenze rispetto allo standard classico influenzi molto i tempi di connessione tra dispositivi, abbassando così il consumo di potenza.

Capitolo 4

Confronto a livello datalink

4.1 Stati del dispositivo

Il funzionamento di un dispositivo Bluetooth si può sintetizzare con una macchina a stati, i quali definiscono le azioni che può compiere e il tipo di canale fisico utilizzato per comunicare.

Bluetooth Basic Rate

I tre stati principali in cui un dispositivo Bluetooth Basic Rate può trovarsi sono: *standby*, *connection* e *park*. Esistono poi sette sottostati che sono utilizzati nella fase di ricerca di dispositivi e nella fase di connessione e sono i seguenti: *page*, *page scan*, *inquiry*, *inquiry scan*, *master response*, *slave response*, e *inquiry response*.
Lo stato standby è lo stato di default del dispositivo, che in questo caso non può né ricevere né inviare pacchetti.
La fase di ricerca prevede che dispositivo in modalità inquiry invii un pacchetto specifico a diverse frequenze richiedendo una risposta ai dispositivi in stato inquiry scan che lo ricevono.
Se il dispositivo inquiry decide di stabilire una connessione , si sposta nello stato page e il dispositivo che verrà scansionato da quest'ultimo dovrà trovarsi nello stato page scan. La scansione avviene tramite l'invio di un pacchetto specifico nei diversi canali fino a che non raggiunge il dispositivo desiderato. A questo punto entrambi i dispositivi cambiano stato: il dispositivo in stato page passa allo stato master response e l'altro dispositivo passa allo stato slave response e, tramite l'invio di altri pacchetti, si sincronizzano.

Una volta stabilita la connessione, i dispositivi in stato master response e slave response passano allo stato connection, assumendo rispettivamente i ruoli di master e slave della piconet appena formata.
Il modo in cui il dispositivo può passare da uno stato all'altro è riassunto nella Figura 4.1.

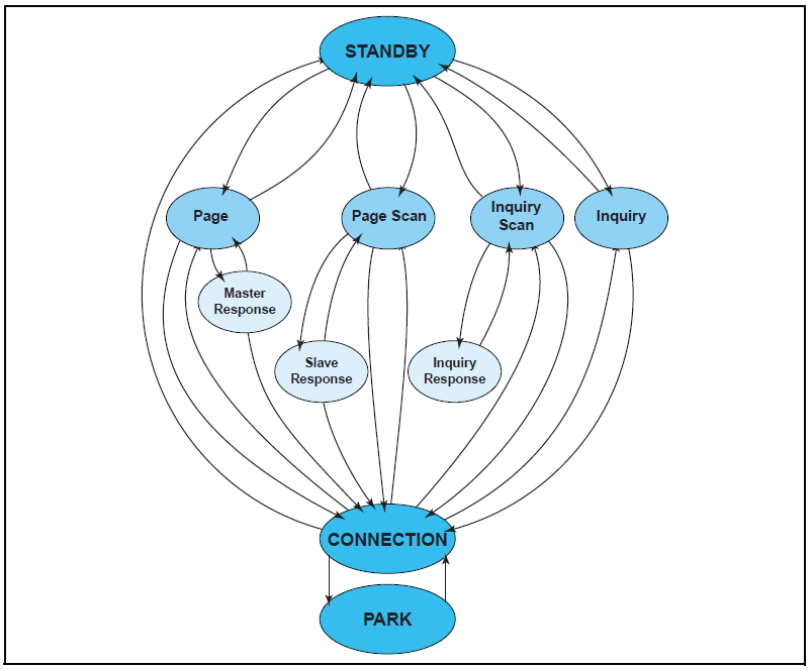

Figura 4.1: Diagramma degli stati di un dispositivo Bluetooth Basic Rate

Per ciascuna di queste fasi viene utilizzata un tipo di canale fisico diverso in termini di frequenze: nella fase di ricerca si utilizza il canale *inquiry scan*, nella fase di connessione il canale *page scan* e nella fase di trasmissione il canale *basic piconet* o *adapted piconet*.
I canali inquiry scan e page scan sono 32 e distribuiti in modo omogeneo nella banda disponibile mentre il canale basic piconet è scelto tra le 79 frequenze disponibili. Il canale adapted piconet è una variante del basic piconet che può utilizzare un numero inferiore di frequenze (minimo 20).

Esistono degli ulteriori sottostati che un dispositivo slave può assumere per facilitare la conservazione di energia:

- *Active*: un dispositivo in questo stato è sempre acceso e disponibile
- *Sniff*: il dispositivo slave passa allo stato active periodicamente
- *Hold*: lo slave passa allo stato active dopo un periodo di tempo concordato prima con il master
- *Park*: uno slave in questo stato non è più considerato parte della piconet ma si sincronizza periodicamente con il master.

Le modalità sniff e hold garantiscono in particolar modo un consumo di potenza inferiore mantenendo comunque bassi i tempi di reazione ad eventuali richieste da parte del master ma il tempo massimo che lo slave può passare in questi stati è di 40 secondi.

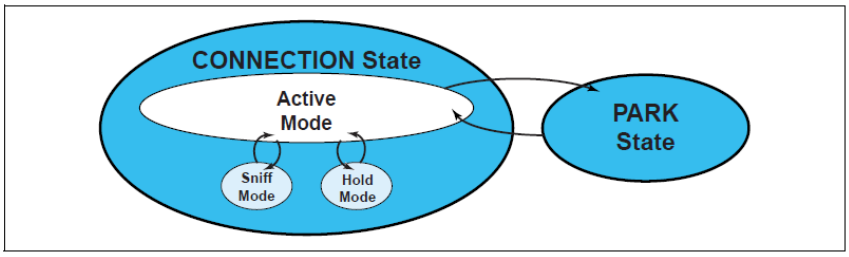

Figura 4.2: Diagramma degli stati che può assumere un dispositivo slave

Bluetooth Low Energy

Il modo in cui opera un dispositivo Bluetooth Low Energy può essere paragonato ad una macchina a 5 stati: *standby*, *advertising*, *scanning*, *initiating* e *connection*.

Come nel caso del Bluetooth Basic Rate, lo stato standby è lo stato di default in cui non ci sono scambi di pacchetti.

Un dispositivo in stato advertising può avviare una ricerca tramite l'invio di pacchetti che saranno ricevuti da dispositivi in stato initiating o scanning. La differenza tra dispositivi in stato scanning e in stato initiating è che questi

ultimi dispositivi sono disponibili ad effettuare una connessione e quindi passare allo stato connection con il ruolo di slaves mentre il dispositivo in stato advertising passerà allo stato connection con il ruolo di master della piconet.

I dispositivi in stato di advertising, scanning e initiating utilizzano i cosiddetti canali advertising per la loro comunicazione mentre i dispositivi in stato connection utilizzano i canali data.

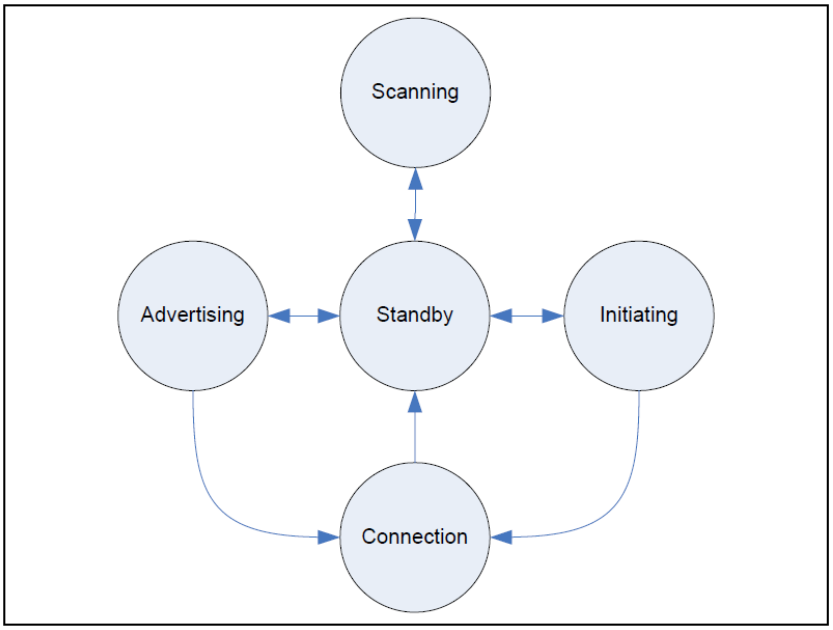

Figura 4.3: Diagramma degli stati di un dispositivo Bluetooth Low Energy

La possibilità di passare dallo stato attivo (connection) allo stato standby, permette allo slave di risparmiare energia durante gli intervalli di tempo tra una trasmissione e quella successiva. Si può notare dalla Figura 4.3 come questo passaggio possa avvenire però solo attraverso gli stati advertising e initiating; cioè la fase di connessione deve essere sempre preceduta da una fase di ricerca.

Il numero di canali advertising (3) inferiore rispetto ai canali inquiry scan e page scan (32) dello standard Bluetooth classico, riduce i tempi di ricerca dei dispositivi: infatti al caso peggiore questa fase richiede 1.2 ms contro i

22.5 ms del Bluetooth Basic Rate, ottenendo così un consumo di potenza di 10-20 volte minore.

L'uso di soli tre canali può avere degli aspetti negativi per quanto riguarda le interferenze con altre trasmissioni radio ma a questo proposito gli sviluppatori hanno avuto l'accortezza di fissare le frequenze dei tre canali tra quelle non utilizzate dai dispositivi WiFi, riducendo così il rischio di disturbo del segnale. [3]

Esiste un ulteriore limitazione per lo standard Bluetooth Basic Rate: un master può collegarsi con la massimo 7 slaves in modalità attiva e 255 slaves in modalità park. Per lo standard Bluetooth Low Energy invece non esistono limitazioni teoriche sul numero di slaves in una piconet, anche se è stato dimostrato che il numero massimo di slaves che il master può gestire nelle migliori ipotesi è 5917.

4.2 Trasmissione dei pacchetti

Vediamo ora più dettaglio come si svolgono le fasi di ricerca, connessione e trasmissione tra due dispositivi Bluetooth.

Bluetooth Basic Rate

Nella fase di ricerca e connessione, come già detto in precedenza, sono coinvolti due dispositivi che diventeranno rispettivamente master e slave della piconet.
Lo scambio di pacchetti in queste fasi avviene nei canali inquiry scan e page scan, che utilizzano le stesse frequenze ed hanno un periodo di hopping di 325 μs.
I canali solo suddivisi in slots da 625 μs e ciascun slot è riservato al master o allo slave alternativamente.
Essendo la frequenza di hopping 3200 hops/s, il master può trasmettere due pacchetti ogni slot (su canali diversi) ma la risposta dello slave sarà inviata

dopo 625 µs dall'invio del pacchetto da parte del master.
Il pacchetto utilizzato nella fase di ricerca è detto ID (identity message) ed è composto da 68 bits contenenti informazioni per la sincronizzazione.
Se la ricerca ha successo, i dispositivi si preparano per la connessione ed il master, esattamente 1250 µs dall'invio del pacchetto ID ricevuto dallo slave, trasmette un pacchetto detto FHS (Frequency Hopping Synchronization) che contiene l'indirizzo di dispositivo e il clock del master. Con l'invio del pacchetto FHS, i dispositivi possono finalmente sincronizzarsi e connettersi.

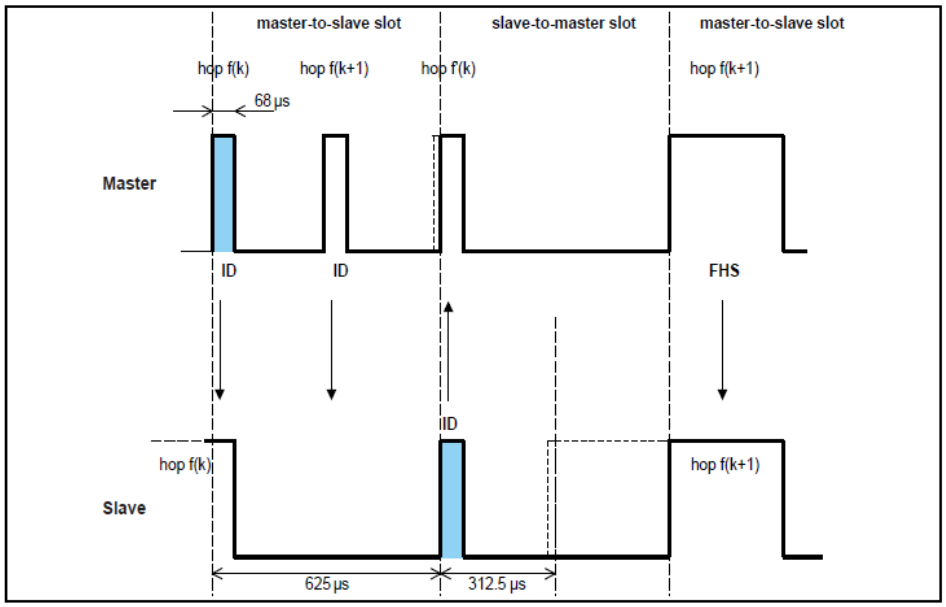

Figura 4.4: Scambio di pacchetti nelle fasi di ricerca e connessione per Bluetooth Basic Rate

Nella fase di trasmissione i dispositivi master e slave utilizzano i canali basic piconet o adapted piconet che utilizzano le stesse 79 frequenze determinate a livello fisico.
La frequenza di hopping è di 1600 hops/s che corrisponde ad un periodo di 625 µs. Ciò significa che sia il master che lo slave possono inviare al massimo un pacchetto per slot (ricordiamo che uno slot è di 625 µs) ma l'invio di un pacchetto può richiedere anche più slots fino ad un massimo di cinque.

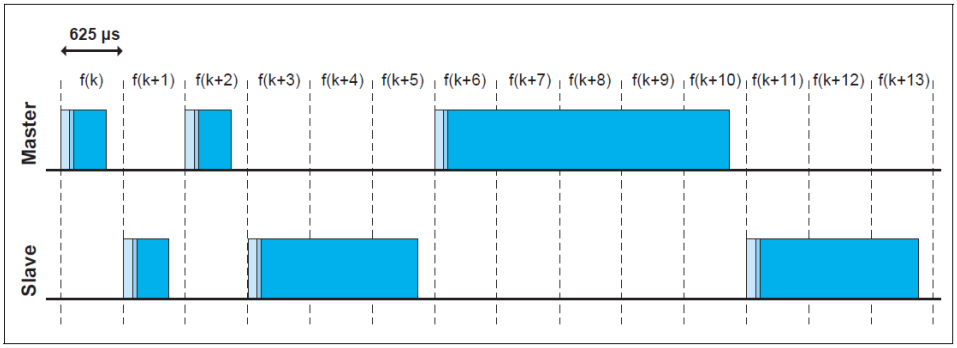

Figura 4.5: Scambio di pacchetti nella fase di trasmissione per Bluetooth Basic Rate

Bluetooth Low Energy

Nello standard Bluetooth Low Energy i canali fisici sono suddivisi in unità temporali chiamate *eventi*.

Gli eventi possono essere di due tipi: *advertising*, durante i quali avviene la ricerca di dispositivi, o *connection*, durante i quali avviene la trasmissione vera e propria.

Ciascun tipo di evento utilizza canali fisici differenti, già determinati a livello fisico: gli eventi advertising utilizzano canali advertising mentre gli eventi connection utilizzano canali data.

Gli eventi non hanno una durata prestabilita ma sono scanditi dalle decisioni del master (per eventi connection) e dell'advertiser (per eventi advertising).

Durante un evento advertising, un dispositivo in stato advertising detto *advertiser* invia un pacchetto nei diversi canali advertising; questo pacchetto può essere ricevuto da due tipi dispositivo: *scanners* (dispositivi che non intendono stabilire una connessione) e *initiators* (dispostivi che vogliono stabilire una connessione).

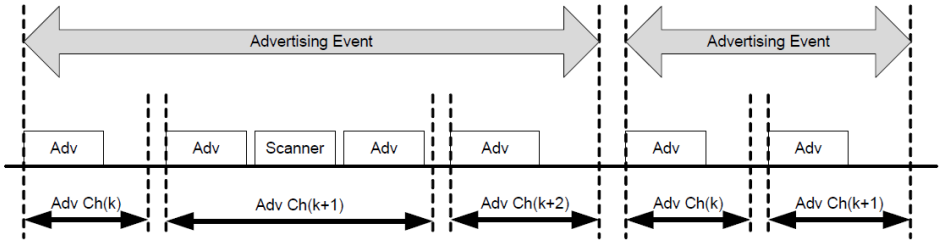

Figura 4.6: Evento advertising

Tra un evento advertising e l'altro c'è un intervallo di tempo (*T_advEvent*) che è calcolato nel seguente modo:

T_advEvent = advInterval + advDelay

Il termine *advDelay* è un valore pseudo-random compreso tra 0 e 10 ms mentre il termine *advInterval* è un intero multiplo di 0.625 ms compreso tra 20 ms e 10.24 s.

Inoltre se l'evento advertising non coinvolge dispositivi initiators, advInterval dovrà essere maggiore di 100 ms.

Esiste un ulteriore intervallo di tempo tra la fine di un pacchetto e l'inizio di quello successivo che è detto *Inter Frame Space* (T_IFS) ed ha valore 150 µs. Esso appare sia negli eventi advertising che in quelli connection, quando i pacchetti sono trasmessi nello stesso canale fisico. [4]

Una connessione può essere stabilita tra un dispositivo advertiser ed un dispositivo initiator e questi dispositivi diventeranno rispettivamente master e slave della piconet appena formata.

Durante un evento connection, master e slave utilizzano lo stesso canale fisico, scelto tra uno dei 37 disponibili.

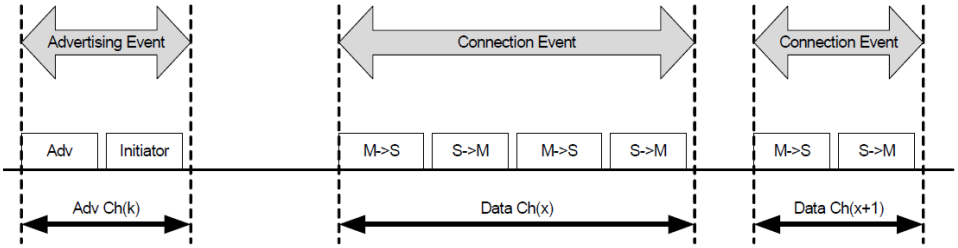

Figura 4.7: Evento connection

Tra due eventi connection consecutivi c'è un intervallo di tempo (*connInterval*) di valore multiplo di 1.25 ms e compreso tra 7.5 ms e 4 s.
Un altro termine importante è la latenza dello slave (*connSlaveLatency*), parametro compreso tra 0 e 500 che definisce il numero di eventi connection nei quali lo slave non è obbligato ad "ascoltare" il master e quindi può restare nello stato standby.
Maggiore è il valore di connInterval e connSlaveLatency, migliori sono le prestazioni in termine di consumo di potenza, anche se ciò può allungare il tempo di *latenza*, inteso come il tempo che impiega un pacchetto ad arrivare a destinazione.[5]
La latenza nel caso base in cui i dispositivi sono già connessi e l'informazione trasmessa è nulla, vale 3 ms (nel Bluetooth Basic Rate invece vale 100 ms).

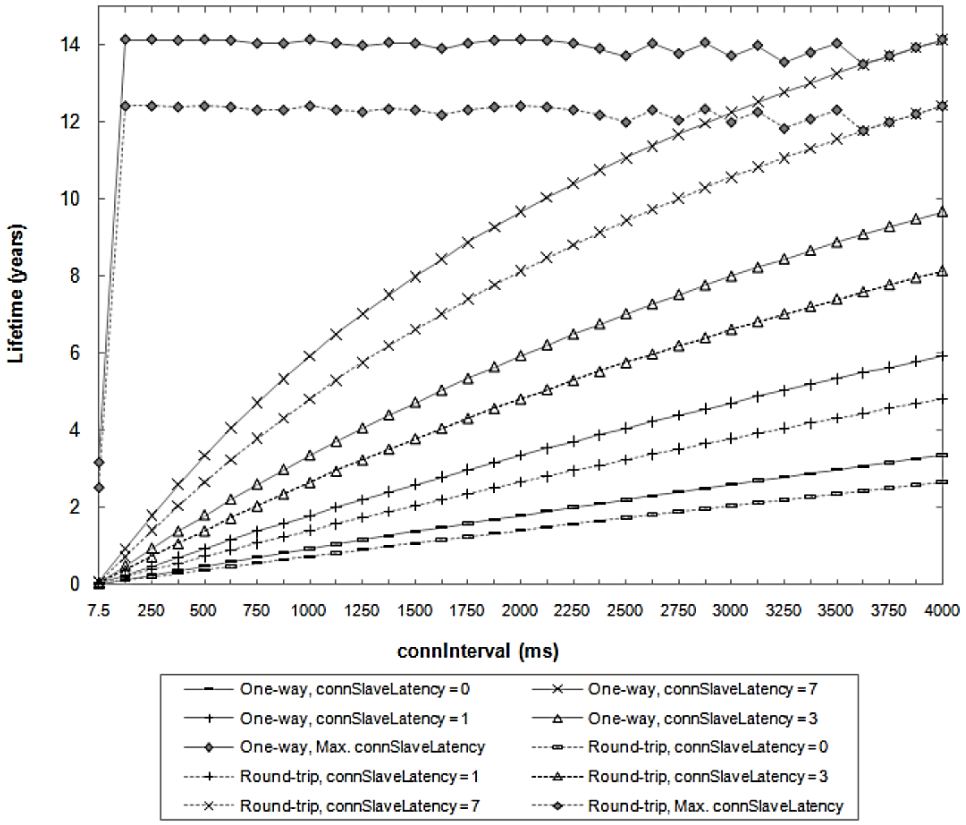

Figura 4.8: Relazione tra connInterval e durata di una batteria a bottone di capacità 220 mAh e voltaggio nominale di 3 V

Come si può notare dalla Figura 4.8, lo standard Bluetooth Low Energy riesce ad ottenere bassi consumi di potenza riducendo al minimo il tempo che lo slave deve restare attivo. Inoltre, aumentando connSlaveLatency e mantenendo basso connInterval, si possono garantire ottime prestazioni di consumo senza allungare troppo i tempi di latenza.

4.3 Trasporto Logico

Nello standard Bluetooth Basic Rate vengono definiti 5 tipi di trasporto logico:

- Synchronous Connection-Oriented (SCO) logical transport: è un trasporto simmetrico tra master e slave dove gli slots sono assegnati periodicamente allo slave.
- Extended Synchronous Connection-Oriented (eSCO) logical transport: funziona come il trasporto SCO con la differenza che questo tipo di trasporto supporta una finestra di ritrasmissione dopo gli slots riservati
- Asynchronous Connection-Oriented (ACL) logical transport: gli slots a differenza del trasporto sincrono non sono riservati ma vengono utilizzati nel momento in cui il master ha necessità di trasmettere
- Active Slave Broadcast (ASB) logical transport: permette traffico undirezionale tra il master e i suoi slaves, che devono essere in modalità active
- Parked Slave Broadcast (PSB) logical transport: è utilizzato per la comunicazione tra il master e i suoi slaves in modalità park.

Il trasporto sincrono (SCO e eSCO) è particolarmente indicato per le trasmissioni audio/video, dove il flusso dati è regolare ed ha un rate preciso; il trasporto asincrono invece è più utile per le trasmissioni dati ed è l'unico tipo di trasporto logico previsto dallo standard Bluetooth Low Energy, che per questo motivo non è indicato per auricolari e cuffie. [6]

4.4 Formato dei pacchetti

Bluetooth Basic Rate

Esistono diversi tipi di pacchetti, a seconda del trasporto logico utilizzato per la trasmissione (ACL, SCO, eSCO).
Il formato generale di un pacchetto standard Bluetooth Basic Rate è rappresentato nella Figura 4.9 e consiste di 3 campi: *access code* (68 o 72 bits), *header* (54 bits) e *payload* (da 0 a 2745 bits).

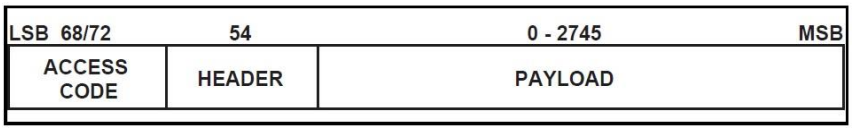

Figura 4.9: Formato pacchetto per Bluetooth Basic Rate

L'access code si trova all'inizio di ogni pacchetto ed è di 72 bits se è succeduto dall'header, altrimenti è di soli 68 bits ed in questo caso viene detto *shortened access code*. Quest'ultimo viene utilizzato per la sincronizzazione e identificazione tra dispositivi nella fase di ricerca e connessione.
L'access code identifica tutti i pacchetti trasmessi nello stesso canale fisico, che in questo caso avranno access code uguale.
L'header è una serie di 54 bits che contiene informazioni di controllo sul collegamento. Una delle informazioni che trasporta è l'indirizzo di trasporto logico, una sequenza di 3 bits che identifica uno slave attivo di una piconet. Un altro campo importante dell'header è il codice di 4 bits relativo al trasporto logico utilizzato che distingue 16 diversi tipi di pacchetto.
Il payload infine trasporta l'informazione vera e propria e può essere di due tipi a seconda che il trasporto logico sia sincrono o asincrono.

Il formato generale di un pacchetto per lo standard Bluetooth Enhanced Data Rate (Figura 4.10) è identico a quello per il Bluetooth Basic Rate per

quanto riguarda la prima parte (access code e header) e si differenzia per la seconda parte , che viene trasmessa con una modulazione diversa.

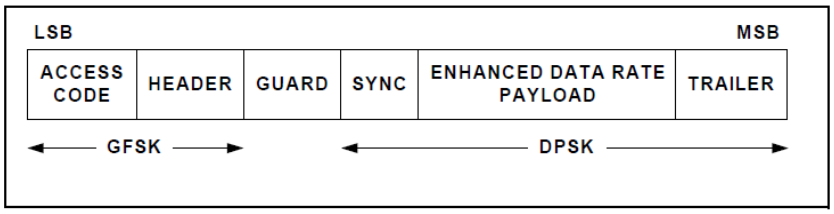

Figura 4.10: Formato pacchetto per Bluetooth Enhanced Data Rate

Tra l'header del pacchetto e l'inizio della sequenza di sincronizzazione (SYNC) c'è un intervallo di guardia (GUARD) che dura dai 4.75 μs ai 5.25 μs.

Il campo SYNC rappresenta una sequenza di 11 simboli generata seguendo la codifica della modulazione utilizzata.

Alla fine del pacchetto sono aggiunti due simboli (TRAILER) , {00, 00} per la modulazione π/4-DQPSK e {000, 000} per la modulazione 8DPSK.

I tipi di pacchetto più comuni sono cinque:

- il pacchetto ID (identity): contiene solo l'access code ed è di lunghezza fissa 68 bits
- il pacchetto NULL: contiene solo access code ed header ed è di lunghezza 126 bits
- il pacchetto POLL: come il pacchetto NULL non ha payload ma richiede una conferma da parte del dispositivo che lo riceve
- il pacchetto FHS: è un speciale pacchetto di controllo che contiene l'indirizzo di dispositivo e clock di chi lo spedisce
- il pacchetto DM1: è un pacchetto che trasporta solo dati d'informazione ed occupa un singolo slot (625 μs).

Bluetooth Low Energy

Per lo standard Bluetooth Low Energy esiste un unico formato che descrive i pacchetti utilizzati sia nei canali advertising che in quelli data ed è rappresentato nella Figura 4.11.
La lunghezza di un pacchetto può variare da 80 a 376 bits ed è composto di quattro campi: *preamble, access address, PDU (Protocol Data Unit), CRC (Cyclic Redundancy Check).*

Figura 4.11: Formato pacchetto per Bluetooth Low Energy

Tutti i pacchetti hanno all'inizio una sequenza di 8 bits chiamata preamble, che è utilizzata dal ricevitore per la sincronizzazione.
I pacchetti trasmessi nei canali advertising hanno preamble di valore 10101010 mentre i pacchetti dei canali data possono avere valore 10101010 o 01010101 a seconda del valore del bit meno significante (Least Significant Bit) dell'access address.

L'access address è una serie di 32 bits che succede il preamble ed ha valori diversi per pacchetti dei canali advertising e data. L'access address di qualunque pacchetto trasmesso nei canali advertising ha valore 10001110100010011011111011010110.
Per i pacchetti dei canali data invece, l'access address è un valore random di 32 bits che deve rispettare i seguenti requisiti:

- non deve avere più di sei bits di valore 0 (o 1) consecutivi
- deve avere valore diverso rispetto all'access address dei pacchetti dei canali advertising di almeno 2 bits
- i quattro ottetti non devono essere tutti uguali
- non deve avere più di 24 transizioni (coppie 01 e 10)

- deve avere almeno due transizioni nei 6 bits più significanti.

Il campo PDU ha lunghezza variabile (da 2 a 39 ottetti) ed ha forma diversa a seconda del tipo di canale dove è utilizzato (data o advertising).
La forma del PDU trasmesso su canale advertising è raffigurata in Figura 11: i primi 16 bits formano il cosiddetto header dove sono indicati tipo di pacchetto e lunghezza del payload (il secondo campo che compone il PDU). Esistono 7 varianti che può assumere il PDU a seconda della funzione del pacchetto trasmesso.

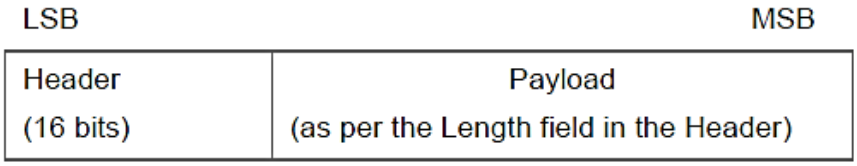

Figura 4.12: Advertising channel PDU

Come il PDU dei canali advertising, anche il PDU dei pacchetti trasmessi su canali data ha una serie di 16 bits iniziali che compongono l'header ed un campo payload la cui lunghezza è specificata nell'header. Gli ultimi 32 bits formano il MIC (Message Integrity Check), un codice di autenticazione utilizzato nelle comunicazioni criptate.

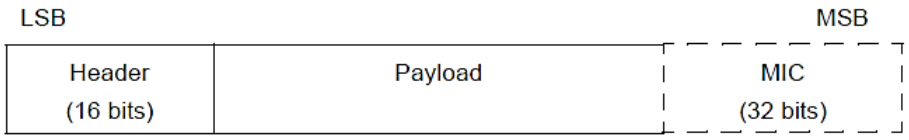

Figura 4.13: Data channel PDU

L'implementazione dei pacchetti nello standard Bluetooth Low Energy permette di omettere le informazioni già note e quindi avere pacchetti più corti rispetto allo standard classico: ciò contribuisce a rendere più basso il valore della latenza e quindi il consumo di potenza.

4.5 Sicurezza

Bluetooth Basic Rate

La sicurezza della trasmissione tra due dispositivi è garantita a livello datalink da 4 elementi:

- un indirizzo pubblico da 48 bits
- una chiave di autenticazione da 128 bits
- una chiave di criptazione da 8 - 128 bits (opzionale)
- un numero random da 128 bits.

L'indirizzo pubblico di un dispositivo Bluetooth (BD_ADDR) è unico e determinato al momento della produzione del chip secondo lo standard IEEE 802-2001.
La chiave di autenticazione (detta anche *link key*) è generata durante il processo di inizializzazione assieme all'eventuale chiave di criptazione.
Quest'ultima è ottenuta a partire dalla chiave di autenticazione e viene cambiata ogni volta che la criptazione è attivata (infatti durante i cambi di stato la criptazione deve essere disattivata).

Il processo di inizializzazione è composto da 5 fasi:
Fase 1: generazione di una chiave di inizializzazione
Fase 2: generazione della chiave di autenticazione
Fase 3: scambio della chiave di autenticazione
Fase 4: autenticazione
Fase 5: generazione della chiave di criptazione in ogni dispositivo.

La chiave di inizializzazione, utilizzata per garantire la sicurezza durante lo scambio iniziale di dati tra i due dispositivi, è ottenuta tramite un algoritmo che utilizza l'indirizzo pubblico del dispositivo, un codice PIN (Personal Identification Number), la lunghezza del PIN (in ottetti) e un numero random.

La chiave di autenticazione può essere di tre tipi:

- combination key K_{AB}, generata a partire da due dispositivi
- unit key K_A, generata da un unico dispositivo
- temporary key K_{master}, usata solo temporaneamente in alcune situazioni particolari, come ad esempio quando il master vuole trasmettere a più di due slaves contemporaneamente utilizzando la stessa chiave di criptazione.

Il processo di autenticazione consiste nella verifica della chiave di autenticazione, che deve essere uguale per entrambi i dispositivi.
Questa verifica viene effettuata tramite l'invio di un numero random RAND da parte del dispositivo A al secondo dispositivo B. Il dispositivo B elabora il numero ricevuto assieme alla link key e al suo indirizzo pubblico tramite un algoritmo E, generando un numero SRES che viene inviato al dispositivo A. A questo punto il dispositivo A deve verificare se il numero ricevuto corrisponde al numero ottenuto dall'elaborazione effettuata da A tramite lo stesso algoritmo E.
Se i due numeri coincidono, allora è verificato che i due dispositivi utilizzano la stessa link key e quindi la connessione è sicura.

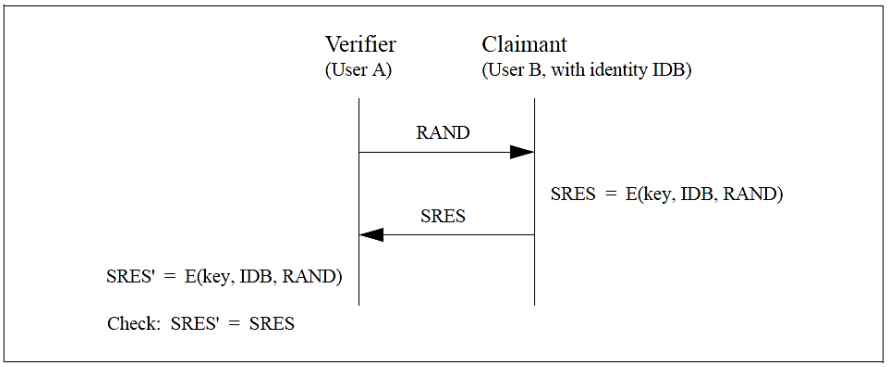

Figura 4.14: Processo di autenticazione tra due dispositivi A e B.

La criptazione di una comunicazione è invece opzionale e riguarda solo il payload dei pacchetti.

Ci sono tre modalità di criptazione disponibili nello standard:

modalità 1: nessuna criptazione;

modalità 2: criptazione dei soli messaggi inviati tra il master ed un singolo slave, questa modalità può essere attivata durante il processo di connessione o a connessione avvenuta;

modalità 3: criptazione di tutti i messaggi, anche quelli inviati a più slaves contemporaneamente, questa modalità può essere attivata solo a connessione avvenuta.

La chiave di criptazione è costruita con un algoritmo che utilizza la link key del collegamento, un numero random da 128 bits e un numero da 96 bits chiamato COF (Ciphering Offset), che viene determinato a partire dall'indirizzo di dispositivo del master (se la link key utilizzata è la master key K_{master}) o dall' ACO (Authentication Cipering Offset), un valore ottenuto nella fase di autenticazione dall'algoritmo E.
La lunghezza della chiave di criptazione varia da 8 a 128 bits, questo sia per adattarsi alle differenti imposizioni riguardo la sicurezza nei diversi paesi del mondo, sia per facilitare eventuali miglioramenti della sicurezza senza dover ridisegnare completamente gli algoritmi per la criptazione.

Bluetooth Low Energy

Il protocollo Security Manager dello standard Bluetooth Low Energy utilizza l'algoritmo per la criptazione autenticata CBC-MAC (Cipher Block Chaining Message Authentication Code), che implementa l'algoritmo di cifratura a blocchi AES (Advanced Encryption Standard).
Il CBC-MAC (abbreviato CCM) ha due parametri M=4 e L=2, che indicano rispettivamente la lunghezza del campo MIC (Message Integrity Check) e la lunghezza del campo Length in ottetti (il campo Length è presente nell'header dei pacchetti ad indicare la lunghezza del payload).

Criptazione ed autenticazione, se richieste dalla comunicazione, riguardano tutti i PDU (con lunghezza del payload diversa da zero) trasmessi su canali data.

L'autenticazione viene effettuata aggiungendo al payload il campo MIC, una sequenza di 32 bits calcolata sul payload del pacchetto stesso con un algoritmo a blocchi, e verificando che tale sequenza sia uguale nel pacchetto trasmesso e in quello ricevuto (vedi Figura 4.15).

La criptazione viene effettuata sia sul payload che sul campo MIC dei pacchetti, sempre utilizzando un algoritmo a blocchi.

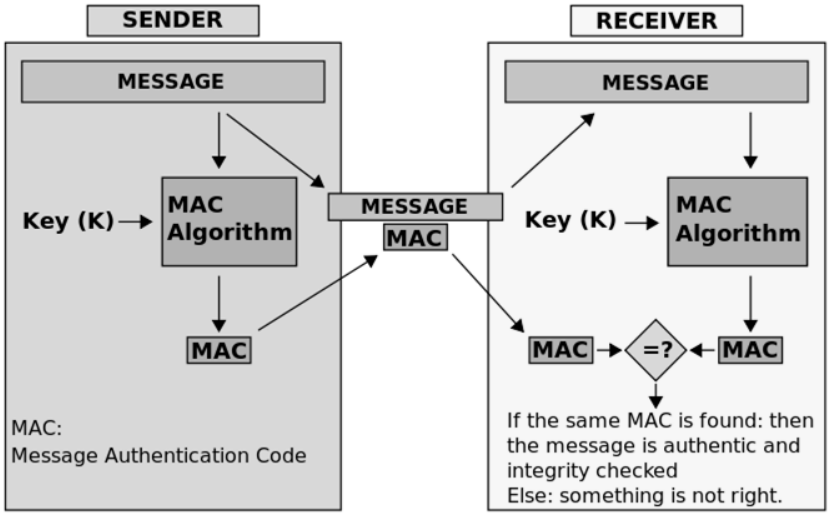

Figura 4.15: Procedura di autenticazione (MAC è un sinonimo di MIC)

Un parametro importante per l'algoritmo CBC-MAC è il *nonce*, un numero casuale lungo 13 ottetti ottenuto in modo tale che sia unico per ogni pacchetto. Questo numero viene utilizzato sia nella fase di autenticazione che in quella di criptazione e la sua unicità garantisce l'effettiva sicurezza della trasmissione.

L'algoritmo AES, da cui trae origine il CBC-MAC, è frutto di uno studio durato cinque anni da parte della NIST (National Institute of Standards and Technology), la quale ha confrontato 15 diversi algoritmi di cifratura (tra

cui l'algoritmo SAFER+ utilizzato per l'autenticazione nel Bluetooth Basic Rate) per scegliere infine quello denominato Rijndael. [7]

L'AES risulta più veloce e sicuro rispetto alla maggior parte degli algoritmi in circolazione, tanto da essere utilizzato pure dal governo degli Stati Uniti d'America; lo standard Bluetooth Low Energy è per questo motivo considerato più affidabile rispetto ai suoi predecessori.[8]

La velocità maggiore di AES rispetto all'algoritmo SAFER+ ancora una volta garantisce allo standard Bluetooth Low Energy una efficienza maggiore in termini di consumo di potenza rispetto al Bluetooth Basic Rate.

Secure Simple Pairing (SSP)

Nel 2007 allo standard classico è stata aggiunta una nuova funzione per semplificare l'accoppiamento tra dispositivi e migliorarne la sicurezza: il protocollo Secure Simple Pairing (SSP), che introduce un ulteriore livello di autenticazione affidato all'utente e non al dispositivo.

I tipi di accoppiamento che due dispositivi possono effettuare sono 4:

- Just Works (JW): non richiede interazioni da parte degli utenti, è utilizzato generalmente con dispositivi con una bassa capacità di input/output
- Numeric Comparison (NC): i dispositivi devono avere un display e avere la possibilità di inserire dati
- Passkey Entry (PE): un dispositivo (oppure entrambi) deve avere un display, l'altro deve poter inserire cifre
- Out Of Band (OOB): entrambi i dispositivi possono comunicare con altri meccanismi esterni.

Il processo di autenticazione si basa sulle seguenti 4 fasi:

Fase 1: scambio delle chiavi pubbliche

Fase 2: autenticazione parte 1

Fase 3: autenticazione parte 2

Fase 4: calcolo della Link Key

Fase 5: autenticazione LMP e cifratura

Tutte le fasi ricalcano i procedimenti già visti in precedenza, eccetto la fase 3 che introduce una autenticazione a livello applicazione.

La procedura infatti, a seconda del tipo di accoppiamento effettuato, richiederà all'utente di:

- rispondere sì oppure no ad una semplice domanda (NC)
- confrontare due numeri e verificare se sono uguali oppure no (NC)
- inserire un numero (PIN) in un dispositivo o entrambi (PE)
- non fare nulla (JW).

Il protocollo SSP è implementato anche dallo standard Bluetooth Low Energy con alcune differenze, come ad esempio i tipi di accoppiamento permessi tra i quali non risulta il Numeric Comparison.

Il Secure Simple Pairing è debole per gli accoppiamento Just Works, ma per tutti gli altri tipi di accoppiamento risulta essere una procedura efficace contro gli attacchi Man-In-The-Middle, ovvero quei tipi di attacchi in cui un terzo utente cerca di intromettersi nella conversazione. [8]

4.6 Modalità di test

Ci sono due tipi di test che un utente può effettuare su un dispositivo Bluetooth:

- non diretto (link mode): test sia sull'hardware che sul software dello stack protocollare
- diretto (non-link mode): test solo sull'hardware, sfrutta l'interfaccia HCI (Host Controller Interface).

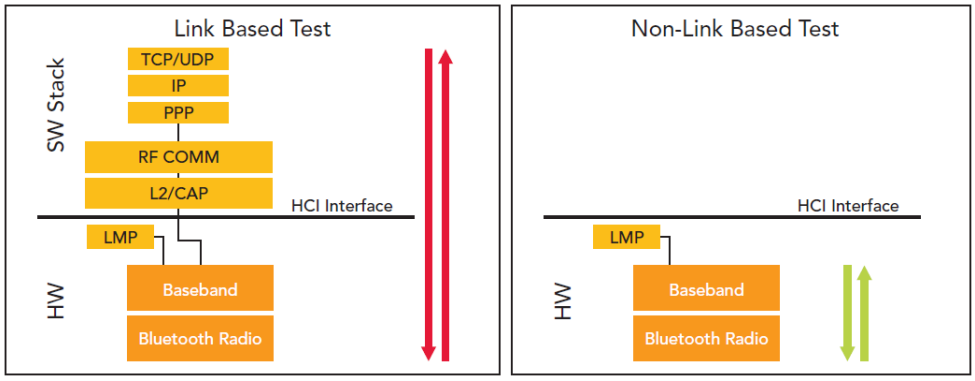

Figura 4.16: Modalità di test non diretta e diretta

Questi test sono principalmente utilizzati dalle aziende produttrici di chip Bluetooth per misurare i parametri di potenza e modulazione del trasmettitore e la sensibilità del ricevitore, in modo tale da verificare la qualità del prodotto.
Lo standard classico dà la possibilità di testare sia l'hardware dei dispositivi che il software implementato su di essi attraverso il test non diretto.
Questo tipo di test però è più lento (perché la trasmissione dei pacchetti coinvolge più livelli) e più costoso (perché richiede un software di test) rispetto al test non diretto.
Per questo motivo nel nuovo standard Bluetooth Low Energy viene implementata la modalità di test non diretta, più conveniente e più semplice da utilizzare nelle aziende produttrici.

Bluetooth Basic Rate

Lo standard Bluetooth classico prevede solo la possibilità di fare test non diretti sui dispositivi, sfruttando l'interfaccia specifica TCI (Test Control Interface), e definisce due modalità per effettuare questo test: Transmitter Test Mode e Loopback Test Mode.

Nel Transmitter Test Mode il dispositivo Bluetooth da testare invia dei pacchetti al tester in seguito ad una richiesta di quest'ultimo.

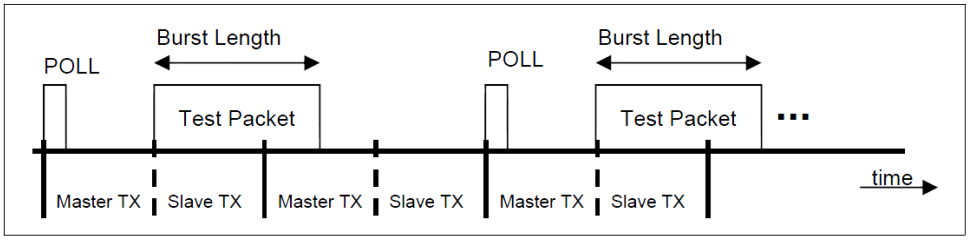

Figura 4.17: Timing di trasmissione dei pacchetti nel Transmitter Test Mode

Nel Loopback Test Mode invece il dispositivo Bluetooth da testare invia al tester (master) un pacchetto dello stesso tipo e con stesso payload del pacchetto inviatogli dal tester stesso in precedenza.
Se il pacchetto trasmesso dal tester non è ricevuto correttamente dal dispositivo, quest'ultimo invierà un pacchetto NULL. [9]

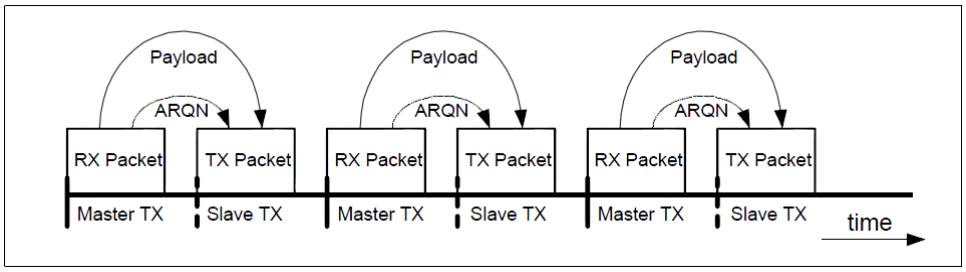

Figura 4.18: Timing di trasmissione dei pacchetti nel Loopback Test Mode

Il formato dei pacchetti inviati è lo stesso utilizzato per le trasmissioni e le informazioni trasmesse sono determinate dai parametri che si intendono testare. Il tester quindi durante la fase di configurazione deve definire il tipo di pacchetto da usare e la sua lunghezza.

Bluetooth Low Energy

Nelle specifiche dello standard Bluetooth Low Energy viene definito il test diretto, che sfrutta l'interfaccia HCI (Host Controller Interface) per inviare pacchetti e testare il livello fisico del dispositivo.

Il formato dei pacchetti utilizzati per effettuare il test è mostrato in Figura 3.18; come per i pacchetti di trasmissione, la lunghezza del payload è variabile a seconda delle esigenze.

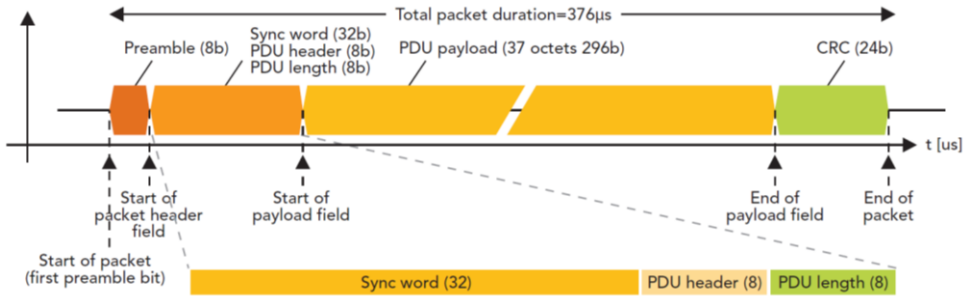

Figura 4.19: Formato dei pacchetti per test diretto

Nello standard viene data anche la possibilità di utilizzare pacchetti "sporchi" (*dirty packets*), dei pacchetti che contengono alcuni errori, per testare la sensibilità del ricevitore.

L'utilizzo dei dirty packets è molto importante perché, a parità di PER (Packet Error Rate), provocano uno shift di 1 o 2 dB sulla potenza in entrata al ricevitore. [10]

I diversi casi di test del Bluetooth Low Energy derivano da quelli per l'hardware dello standard classico, ridotti e ottimizzati per le diverse implementazioni.

Capitolo 5

Confronto a livello applicazione

A livello applicazione vengono definiti i cosiddetti *profili*, ovvero insiemi di protocolli che definiscono le funzionalità del dispositivo Bluetooth.
Un profilo generico GAP (Generic Access Profile) utilizza tutti i protocolli a livello fisico e datalink, già discussi nei capitoli precedenti, oltre ad altri protocolli definiti dallo standard Bluetooth a livello superiore tra cui il protocollo L2CAP (Logical Link Control and Adaptation Protocol) che gestisce il flusso dei dati da protocolli superiori al livello datalink (solo per comunicazioni con trasporto asincrono).
Gli altri protocolli necessari alla creazione di un profilo si differenziano tra Bluetooth Basic Rate e Bluetooth Low Energy.

Bluetooth Basic Rate

Lo standard Bluetooth Basic Rate definisce un ulteriore protocollo fondamentale per la creazione di un profilo: il protocollo SDP (Service Discovery Protocol), che permette al dispositivo di capire quali servizi sono disponibili, che caratteristiche hanno e su cui si basa il profilo Service Discovery Application (SDAP).
Lo standard inoltre definisce altri protocolli, come ad esempio RFCOMM (Radio Frequency Communication), che emula una porta seriale, e il protocollo TCS BIN (Telephony Control protocol Specification Binary), necessario per gestire chiamate voce e dati.

Su questi protocolli standard è possibile implementare protocolli definiti da altre organizzazioni, come:

- PPP (Point-to-Point Protocol): protocollo per stabilire una connessione tra due nodi di una rete
- TCP (Transmission Control Protocol) e UDP (User Datagram Protocol): protocolli base della suite di protocolli Internet (IP)
- OBEX (Object Exchange): protocollo per lo scambio di oggetti
- WAP (Wireless Application Protocol): protocollo che permette la connessione ad internet ai cellulari.

I profili Bluetooth Basic Rate vengono principalmente divisi in tre gruppi, a seconda del protocollo che utilizzano:

- gruppo Serial Port Profile, si basa sul protocollo RFCOMM
- gruppo Generic Object Exchange, si basa sul protocollo OBEX
- gruppo Telephony Control Protocol Specification, si basa sul protocollo TCS BIN.

Bluetooth Low Energy

La creazione di profili specifici con lo standard Bluetooth Low Energy avviene a partire dal profilo generico GATT (Generic Attribute Profile), che utilizza solo il protocollo ATT (Attribute Protocol) in aggiunta ai protocolli inferiori.

Il protocollo ATT definisce due ruoli: server e client. Il server è in grado di contenere dei dati (*attributi*) che sono accessibili dal client tramite il protocollo.

Gli attributi sono definiti da tre parametri:

- Type: definisce il tipo di attributo (ad esempio: temperatura, nome dispositivo, stato della batteria, ecc.)
- Handle: un valore che caratterizza ogni singolo attributo
- Value: valore effettivo dell'attributo.

Gli attributi possono essere accessibili in lettura, in scrittura o entrambi e possono richiedere una autenticazione o criptazione per effettuare queste azioni.

Il profilo generico GATT utilizza il protocollo ATT, introducendo la suddivisione degli attributi conservati nel server in *servizi* e *caratteristiche.*
I servizi possono contenere un insieme di caratteristiche, che a loro volta comprendono un singolo valore (accessibile dal client) ed altri dati numerici che descrivono la caratteristica in questione. [11]

La creazione di un profilo da parte di un utente richiede innanzitutto di stabilire quali parametri del dispositivo si vogliono conoscere e verificare se sono già definiti dei servizi o caratteristiche utili a tale scopo.
Sul portale ufficiale della SIG dedicato ai sviluppatori (https://developer.bluetooth.org) sono disponibili alcuni servizi e caratteristiche già sviluppate.

La procedura di creazione di un profilo nello standard Bluetooth Low Energy è stata quindi notevolmente semplificata: non sono necessari altri protocolli oltre a quelli già definiti ed il sistema servizi-caratteristiche è più intuitivo e semplice da utilizzare.
Purtroppo data la grande differenza tra i protocolli implementati, i profili Bluetooth Low Energy non sono compatibili con i profili Bluetooth.
Per risolvere in parte questo problema, si è pensato di produrre chip su cui vengono implementati entrambi gli standard (chip dual-mode) e i dispositivi con tale chip, contrassegnati con il logo Bluetooth Smart Ready®, possono comunicare con tutti i tipi di dispositivo.

Bibliografia

[1] *Bluetooth*
http://en.wikipedia.org/wiki/Bluetooth

[2] Jay Tyzzer, *One Small Step for Bluetooth Low Energy Technology*, 27 Agosto 2013
http://www.wirelessdesignmag.com/articles/2010/08/one-small-step-bluetooth-low-energy-technology

[3] Raajit Lall , *Too Many Cooks in the 2.4 GHz Kitchen?*, 4 Febbraio 2013
http://zone.ni.com/devzone/cda/pub/p/id/1685

[4] *BLUETOOTH SPECIFICATION Version 4.0* (PDF), 30 Giugno 2010
https://www.bluetooth.org/en-us/specification/adopted-specifications

[5] C.Gomez, J. Oller, J. Paradells, *Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology*, 29 Agosto 2012
www.mdpi.com/journal/sensors

[6] L. Vangelista, N. Laurenti, T. Erseghe, R. Corvaja, A. Zanella, M. Rossi, L. Badia, *Principles of Communications Networks and Systems*, Ed.: N. Benvenuto, M. Zorzi, Wiley, 2011

[7] *Advanced Encryption Standard*
http://it.wikipedia.org/wiki/Advanced_Encryption_Standard

[8] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, *Performance Comparison of the AES Submissio* (PDF), 3 Gennaio 1999
http://www.ussrback.com/crypto/aes/aes-performance.pdf

[9] *Bluetooth® Measurement Fundamentals* (PDF), 12 Ottobre 2006
http://cp.literature.agilent.com/litweb/pdf/5988-3760EN.pdf

[10] Marta Gaia Zanchi, *Bluetooth® Low Energy – LitePoint* (PDF), Giugno 2012
http://www.litepoint.com/whitepaper/Bluetooth%20Low%20Energy_WhitPaper.pdf

[11] Roger Garvert, *Bluetooth 101+* (PPT)
www.fte.com/docs/Ble_101_frontline.pps