

Università di Bologna
Corso di Laurea Specialistica in Scienze di Internet
A.A. 2007 – 2008

Relazione del corso di Sistemi e Reti Wireless

Lo standard IEEE 802.15.4 e ZigBee

Cristina Donati

Matricola 0000253645

INDICE

PREFAZIONE.....	1
1. INTRODUZIONE E PANORAMICA GENERALE	4
1.1 CARATTERISTICHE E OBIETTIVI DI 802.15.4.....	4
1.2 COMPONENTI DI UNA WPAN 802.15.4.....	5
1.3 TOPOLOGIE DI RETE.....	6
1.4 FORMAZIONE DELLA RETE	7
1.5 ARCHITETTURA	9
1.6 PRESENTAZIONE DELLE FUNZIONI	10
1.6.1 Superframe structure.....	10
1.6.2 Data transfer model.....	12
Data transfer to a coordinator - beacon enabled.....	13
Data transfer to a coordinator - beacon disabled.....	13
Data transfer from a coordinator - beacon enabled.....	14
Data transfer from a coordinator - beacon disabled.....	14
1.6.3 Frame structure	15
Beacon Frame.....	15
Data Frame.....	16
Acknowledgment Frame.....	17
MAC Command Frame.....	18
1.6.4 Robustness.....	19
CSMA-CA mechanism.....	19
Frame acknowledgment.....	19
Data verification.....	20
1.6.5 Consumo energetico (power consumption).....	20
1.6.6 Sicurezza.....	21
Security Services.....	21
Security Modes.....	22
2. IL LIVELLO FISICO	23
2.1 REQUISITI GENERALI E DEFINIZIONI	23
2.1.1 Range frequenze operative.....	24
2.1.2 Assegnazione canale	24
Channel Numbering.....	25
Channel Pages.....	25
2.1.3 Minimum long interframe spacing (LIFS) e short interframe spacing (SIFS) periods.....	26
2.1.4 Misura della potenza del segnale.....	27
2.1.5 Potenza della trasmissione.....	27
2.1.6 Sensibilità del ricevente.....	27
2.2 SPECIFICHE DEI SERVIZI DEL LIVELLO FISICO.....	27
2.2.1 PHY Data Service.....	28
2.2.2 PHY Management Service.....	29
2.2.3 PHY Enumeration Description.....	31
2.3 FORMATO PHY PROTOCOL DATA UNIT (PDDU)	31
2.4 PHY CONSTANTS	34
2.5 PHY PIB ATTRIBUTES	34
2.6 DETTAGLI SULLE SPECIFICHE DI OGNI FREQUENZA DI BANDA (LIMITATO A QUELLE UTILIZZATE DA ZIGBEE)	36
2.6.1 2450Mhz PHY Specification.....	36
2.6.2 868/915 MHz band binary phase-shift keying (BPSK) PHY Specification.....	37
2.7 TRANSMIT POWER.....	38
2.8 RECEIVER MAXIMUM INPUT LEVEL DEL SEGNALE DESIDERATO	38
3. IL LIVELLO MAC	39
3.1 REQUISITI GENERALI E DEFINIZIONI	39
3.2 SPECIFICHE DEI SERVIZI DEL LIVELLO MAC	39

3.2.1	<i>MAC Data Service</i>	40
3.2.2	<i>MAC Management Service</i>	42
3.2.3	<i>MAC Enumeration Description</i>	51
3.3	MAC FRAME FORMATS	54
3.3.1	<i>Formato generale</i>	54
3.3.1.1	<i>Frame control</i>	54
3.3.1.2	<i>Sequence number</i>	55
3.3.1.3	<i>Destination PAN identifier</i>	55
3.3.1.4	<i>Destination Address</i>	55
3.3.1.5	<i>Source PAN identifier</i>	55
3.3.1.6	<i>Source Address</i>	55
3.3.1.7	<i>Frame Payload</i>	55
3.3.1.8	<i>FCS (frame check sequence)</i>	55
3.3.2	<i>Beacon Frame Format</i>	56
3.3.3	<i>Data frame</i>	56
3.3.4	<i>Acknowledgment frame</i>	56
3.3.5	<i>MAC command frame</i>	56
3.4	MAC COMMAND FRAMES	57
3.5	DESCRIZIONE FUNZIONALITÀ DEL LIVELLO MAC	58
3.5.1	<i>Channel Access</i>	59
3.5.1.1	<i>Superframe</i>	59
3.5.1.2	<i>IFS</i>	60
3.5.1.3	<i>CSMA-CA</i>	61
3.5.2	<i>Inizializzare e gestire una PAN</i>	64
3.5.2.1	<i>Scansione dei canali</i>	64
3.5.2.2	<i>Risoluzione dei conflitti di PAN ID</i>	65
3.5.2.3	<i>Inizializzare una PAN</i>	65
3.5.2.4	<i>Generazione Beacon</i>	65
3.5.2.5	<i>Device Discovery</i>	65
3.5.3	<i>Associazione e dissociazione</i>	65
3.5.4	<i>Sincronizzazione</i>	66
3.5.5	<i>Gestione delle transazioni</i>	66
3.5.6	<i>Trasmissione, ricezione e ack</i>	67
3.5.6.1	<i>Trasmissione</i>	67
3.5.6.2	<i>Ricezione e scarto</i>	67
3.5.6.3	<i>Estrarre pending data da un coordinatore</i>	68
3.5.6.4	<i>Acknowledgment</i>	68
3.5.6.5	<i>Ritrasmissione</i>	69
3.5.7	<i>Allocazione e gestione GTS</i>	70
3.5.8	<i>Frame Security</i>	71
	BIBLIOGRAFIA	73
	GLOSSARIO	74

Prefazione

Questa relazione nasce con lo scopo di analizzare i livelli fisico e MAC della tecnologia ZigBee, o per meglio dire la specifica 802.15.4 visto che ZigBee si appoggia ad essa per i livelli più bassi dello stack ISO/OSI, nell'ambito del progetto di esame per il corso di Sistemi e Reti Wireless.

ZigBee è il nome di una specifica per una *suite* di protocolli di comunicazione di alto livello, basati sullo standard IEEE 802.15.4, nell'ambito delle WPAN. Il rapporto che lega IEEE 802.15.4 e ZigBee è equiparabile a quello esistente tra lo standard IEEE 802.11 e *Wi-Fi Alliance*. Le frequenze su cui opera maggiormente sono quelle assegnate a scopi industriali, specifici e medici, ovvero le frequenze ISM (*Industrial, Scientific and Medical*): 2.4 GHz su scala mondiale, 868 MHz per l'Europa e 915 MHz per gli USA.

La nascita dello standard IEEE 802.15.4 e della definizione della tecnologia ZigBee avviene in un contesto in cui la necessità era ottenere una comunicazione wireless riducendo costi, complessità e consumo energetico. Sul mercato iniziavano a proliferare soluzioni proprietarie a questi bisogni, che, senza un livello di standardizzazione, portavano grandi problemi di interoperabilità. Lo scopo principale era trovare una soluzione per consentire la comunicazione di tutti quei *device* che non necessitavano di una grande larghezza banda, ma piuttosto richiedevano un basso consumo d'energia, un basso costo di realizzazione ed una bassa latenza.

Da qui la scissione in due parti: lo standard IEEE 802.15.4, che concerne il livello MAC e il livello PHY, e la definizione del ZigBee Stack (da parte di un'associazione di vendor denominata *ZigBee Alliance*), che si occupa dei livelli superiori dello stack ISO-OSI, ovvero il *Network layer*, l'*Application Support layer* e l'*Application layer*.

Nelle WPAN si affianca alla tecnologia Bluetooth, si differenzia da essa non solo per il bitrate e il range di copertura, ma anche per il livello di complessità. I nodi ZigBee richiedono quasi la metà del codice richiesto dai nodi Bluetooth.

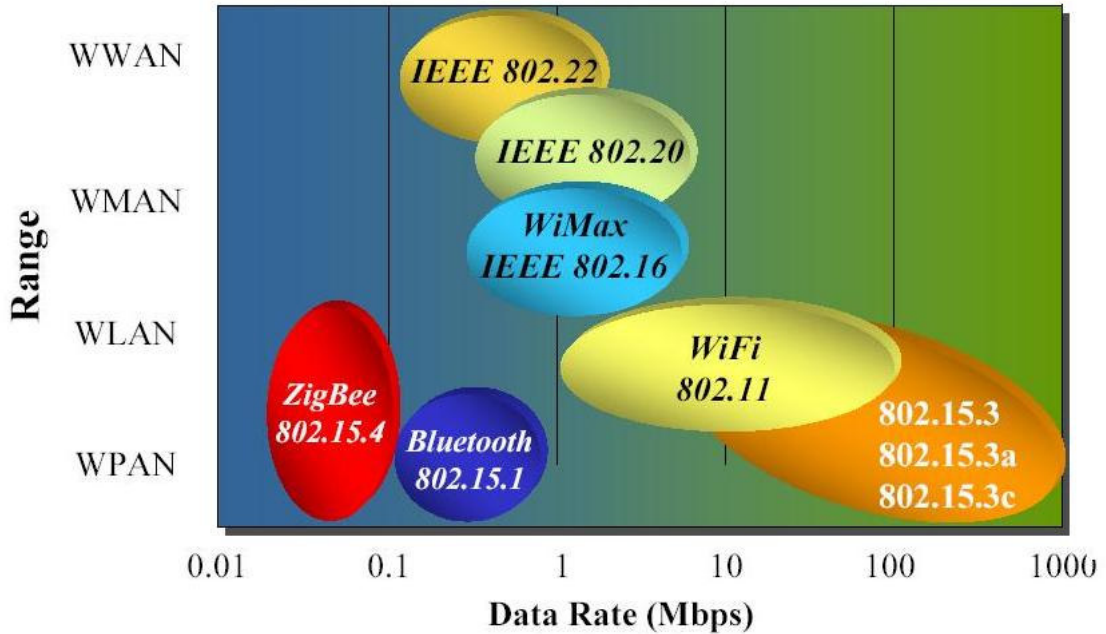


Figura 1: Wireless Space

Come possiamo notare anche dall'immagine in figura 1 e figura 2, 802.15.4 non nasce per trasportare dati multimediali come voce e video, ma come soluzione per dati di piccole dimensioni, come solo testo.

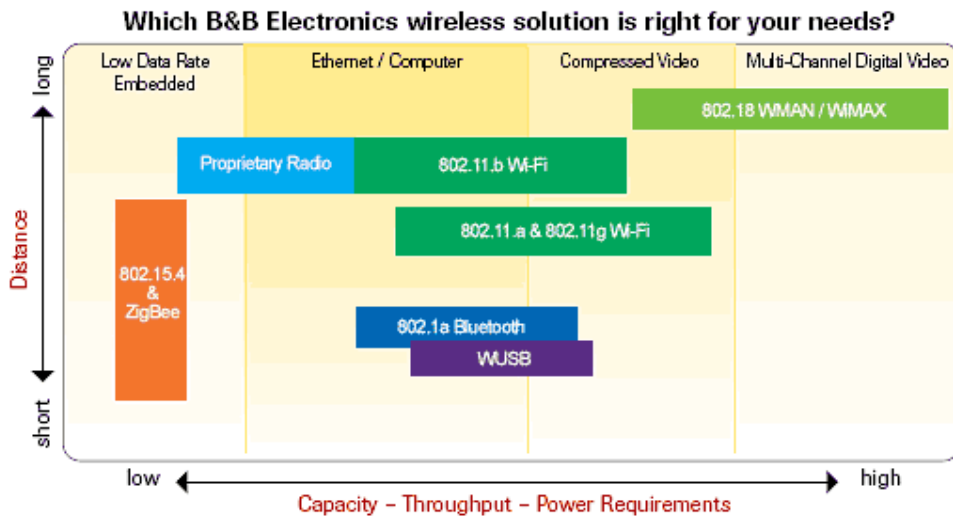


Figura 2: Wireless Market

Partecipare alla ZigBee Alliance, certificare i propri dispositivi e usare a scopi commerciali questa tecnologia ha però un prezzo: un tesseramento di

livello base alla ZigBee Alliance costa USD 3500, la certificazione invece USD 1000 per il primo dispositivo e USD 500 i successivi. Per scopi non commerciali, la specifica ZigBee è disponibile sul sito della ZigBee Alliance, non è tuttavia possibile disegnare una propria applicazione senza usare alcune API definite da questo standard. Questo rappresenta una limitazione, e ci porta, in questa relazione, ad analizzare non tanto i livelli dello stack ISO/OSI della cui specifica si occupa la ZigBee Alliance (*Network layer, l'Application Support layer e l'Application layer*), o dei vari Application Object che sono definiti dai produttori dei dispositivi hardware, quanto il livello fisico e il livello MAC che sono regolati dallo standard IEEE 802.15.4.

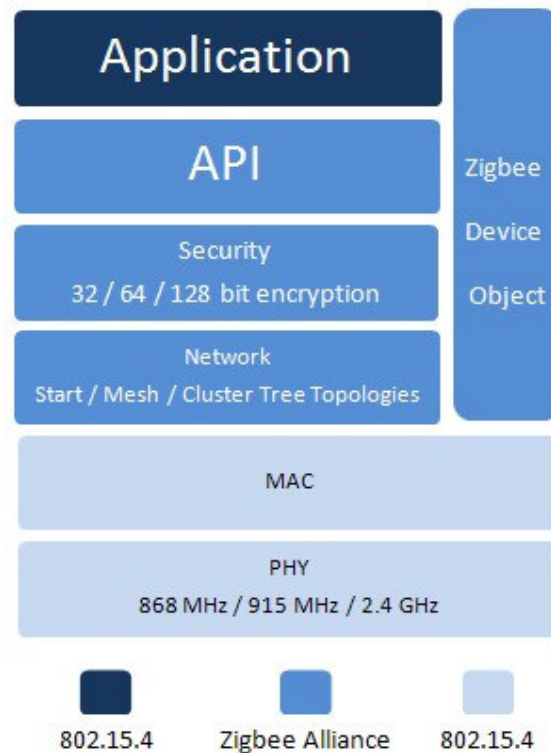


Figura 3: ZigBee Stack

Ovviamente ciascun livello è caratterizzato da funzionalità e da formato dei dati differenti, nel capitolo seguente tratteremo un'introduzione generale allo standard IEEE 802.15.4.

1. Introduzione e panoramica generale

1.1 Caratteristiche e obiettivi di 802.15.4

Il contesto delle specifiche 802.15 si occupa delle reti wireless a stretto raggio copertura, denominate wireless personal area networks (WPAN). All'interno di questa grande categoria troviamo diversi gruppi di lavoro (task group), che si occupano di standard differenti.

Come già scritto nella prefazione in questa relazione trattiamo del task group numero 4, che si pone l'obiettivo creare uno standard semplice per le reti low rate che garantisca una connessione wireless a basso costo in condizioni di risparmio energetico e modesto throughput.

Obiettivi principali:

- basso costo
- operazioni a distanza limitata
- lunga durata della batteria
- facilità di installazione
- affidabilità trasferimento dati
- protocollo semplice e flessibile

Le **caratteristiche principali di una LR-WPAN** sono le seguenti:

- Data rates of 250 kb/s, 100kb/s, 40 kb/s, and 20 kb/s
- Operazioni in tipologia di rete a stella o peer-to-peer
- Indirizzi in forma breve a 16-bit o 64-bit in forma estesa
- Allocazione opzionale di slot garantiti (guaranteed time slots GTSs)
- Modalità di accesso al canale carrier sense multiple access with collision avoidance (CSMA-CA) [nota, nella draft 2007 dello standard si aggiunge la modalità ALOHA per la banda ULTRAWIDE BAND (UWB)]
- Trasferimento affidabile dei dati tramite ack (acknowledged protocol)
- Basso consumo energetico

- Energy detection (ED)
- Link quality indication (LQI)
- 16 canali nella banda 2450 MHz, 30 canali nella banda 915 MHz, e 3 canali nella banda 868 MHz [a questi nella draft 2007 si sono aggiunti 14 canali *Overlapping Chirp Spread Spectrum (CSS)* nella banda 2450Mhz e 16 canali nella banda UWB (500Mhz, 3.1Ghz e 10.6Ghz).

1.2 Componenti di una WPAN 802.15.4

I dispositivi che si servono di questa tecnologia si dividono in due tipologie e possono rivestire 3 ruoli. Prima di tutto parliamo di dispositivi *full function device (FFD)* e di *reduced function device (RFD)*. I primi possono agire secondo tutte e tre le modalità, ovvero possono operare come *PAN Coordinator*, *Coordinator* o semplicemente *Device*. I secondi, i RFD sono dispositivi estremamente semplici e utilizzano poche risorse, per questo possono rivestire solo il ruolo di *device*. Di questo tipo sono ad esempio interruttori della luce o sensori, il cui bisogno non è quello di spedire grosse quantità di dati, e si possono associare solo ad un altro RFD per volta.

Otteniamo una rete quando due o più device all'interno dello spazio POS (personal operating space) comunicano sullo stesso canale fisico. Per costruire una rete è necessario avere almeno un dispositivo *FFD* che agisca come *PAN Coordinator*. Occorre ricordare che stiamo prendendo in esame un'area di copertura non cablata, ma wireless, pertanto non è possibile definire chiaramente quale sia lo spazio POS, poiché diversi fattori di propagazione del segnale sono dinamici ed incerti. Ad esempio basta un cambio di polarizzazione o diverso allineamento può causare cambiamenti drastici nella qualità di ricezione. Spostare un dispositivo può avere effetti che si propagano da dispositivo a dispositivo lungo il raggio di copertura della rete.

1.3 Topologie di rete

A seconda di quanto richiesto dall'applicazione le reti LR-WPAN possono operare secondo due topologie: a stella e peer to peer.

Nella **topologia a stella** la comunicazione è stabilita fra un dispositivo e il PAN coordinator. Il device collegato ha tipicamente proprie applicazioni in esecuzione e rappresenta il punto di inizio o il termine della comunicazione. Il PAN Coordinator può, invece, iniziare o terminare la comunicazione ma anche instradare la comunicazione sulla rete. Tutti i device operanti su una rete sono dotati di indirizzi a 64bit. Questo indirizzo può essere usato per comunicazioni dirette all'interno della PAN, oppure può essere rimpiazzato a discrezione del PAN coordinator dall'indirizzo breve quando il dispositivo si associa alla rete. Solitamente, viste le funzioni di rilevanza che riveste, il coordinatore è alimentato elettricamente e non da batteria come accade invece per la maggioranza dei dispositivi semplici. Le applicazioni ideali per la topologia a stella sono: home automation, periferiche PC, giochi e giocattoli e cura personale.

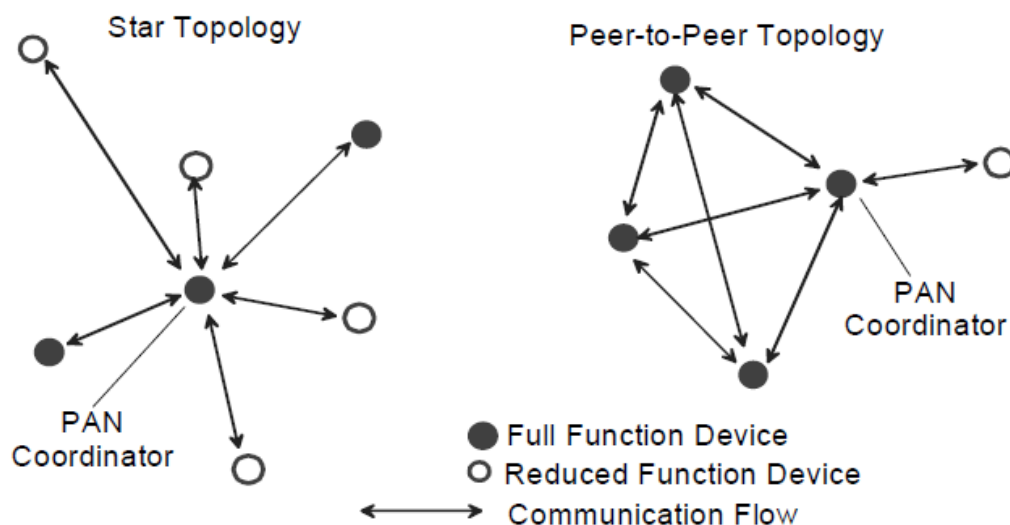


Figura 4: Topologie di rete

Anche nella **topologia peer to peer** abbiamo un PAN Coordinator, ma la differenza è rappresentata dalla possibilità dei device di comunicare fra loro direttamente. E' chiaro come questa topologia permetta la creazione di

reti molto più complesse, come evidenziato anche nella figura seguente. Può prevedere l'instradamento multi-hop fra i vari device associati alla rete, funzioni di questo tipo esulano dallo standard 802.15.4 e sono lasciate al livello di rete. Una rete peer to peer si adatta ad applicazioni in campo di controllo e monitoraggio industriale, sensoristica, inventari e gestione magazzino, agricoltura, sicurezza..., e può essere ad-hoc, self-organizing oppure self-healing. Ogni PAN sceglie un identificativo univoco, questo consente ai dispositivi associati alla rete di comunicare tra loro usando l'indirizzo breve (short address) e anche di abilitare trasmissioni fra device associati a reti indipendenti.

1.4 Formazione della rete

La **struttura di rete a stella** si forma nel momento in cui un FFD si attiva e diventa PAN coordinator. Ogni topologia a stella è indipendente da qualunque altra risulta attiva, grazie all'identificativo scelto dal coordinatore che deve essere diverso da quelli già in uso dalle altre reti nel range di copertura. Non appena il PAN coordinator ha scelto il PAN identifier concede agli altri device nell'area (sia RFD che FFD) di associarsi alla rete.

Nella **struttura di rete peer to peer** ogni device è in grado di comunicare con qualunque altro device nella sfera di influenza. E' eletto a PAN Coordinator il primo dispositivo che comunica sul canale. Un esempio di questa topologia è rappresentato dalla rete *cluster tree*. Qui la maggioranza dei nodi sono FFD e i RFD si connettono come foglie alla fine dei vari rami, poiché ad essi è consentita una sola associazione per volta. Ogni FFD può agire come coordinatore e fornisce il servizio di sincronizzazione agli altri dispositivi e agli altri coordinatori. Il PAN Coordinator da origine al primo cluster della rete scegliendo l'identificativo univoco e inviando un beacon frame in broadcast ai dispositivi nelle vicinanze. Due dispositivi potrebbero tentare di stabilire una connessione come PAN coordinator nello stesso momento, per questo è necessario prevedere un meccanismo di risoluzione della contesa, ma esula dagli scopi dello standard. Il beacon frame inviato dal coordinatore come richiesta di associazione alla rete viene ricevuto dai device candidati a farne parte, se il

PAN coordinator concede al dispositivo di unirsi viene aggiunto come figlio nella sua neighbor list. A sua volta il dispositivo appena aggiunto setta il PAN coordinator come padre e lo aggiunge alla sua lista iniziando la trasmissione di beacon periodici. Se un dispositivo non è in grado di collegarsi al PAN coordinator cercherà un altro dispositivo padre nell'area. La forma più semplice di cluster tree è dato dal cluster singolo, ma reti molto più ampie e complesse possono essere ottenute tramite mesh di di cluster multipli vicini. Un esempio di questa forma è osservabile nella figura seguente. Il vantaggio di una topologia di questo tipo è evidente: permette un aumento notevole dell'area di copertura, anche se ciò comporta un aumento del tempo di latenza dei messaggi.

In una rete LR-WPAN possiamo collegare più di 65.534 (2^{64}) dispositivi.

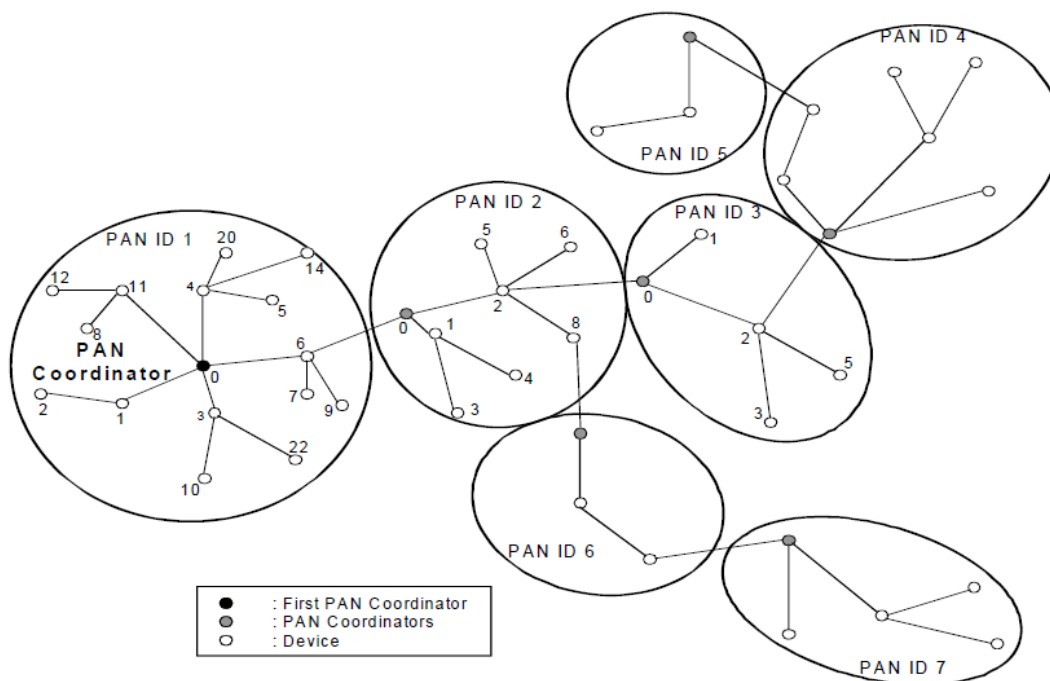
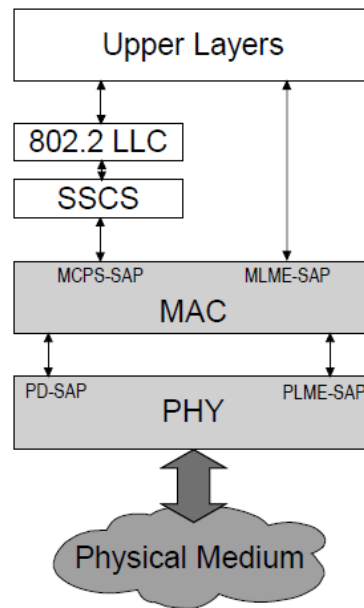


Figura 5: Cluster Tree

1.5 Architettura

Come per tanti altri protocolli, anche nel caso delle LR-WPAN, abbiamo un'architettura divisa in blocchi denominati *livelli (layer)*. Ognuno di questi è responsabile di una parte dello standard e offre servizi ai livelli superiori. Come già ripetuto più volte lo standard IEEE 802.15.4 tratta unicamente i due livelli inferiori dello stack ISO/OSI, che conta un totale di sette livelli, ovvero livello fisico e MAC.



NOTE—For MCPS-SAP, see 7.1; for MLME-SAP, see 5.4.2; for PD-SAP, see 6.2; and for PLME-SAP, see 5.4.1.

Figura 6: Architettura a livelli LR-WPAN

Il livello fisico (**PHY**) fornisce due servizi: *PHY Data Service* e *PHY Management Service Interfacing*. Questi si interfacciano con l'unità di gestione del livello fisico, denominata *Physical Layer Management Entity (PLME)*. I pacchetti dati a questo livello consistono in unità dati del livello fisico, *PHY protocol data units (PDDUs)* ed è compito del servizio PHY Data Service di abilitare la loro trasmissione e ricezione sul canale radio.

Altre funzioni rivestite da questo livello sono l'attivazione e disattivazione delle trasmissioni, energy detection (ED), link quality indication (LQI),

selezione del canale, clear channel assessment (CCA) e ovviamente l'invio e la ricezione dei pacchetti sul medium fisico.

Le frequenze su cui opera (da ricordare che sono unlicensed band, ovvero libere) sono:

- 868–868.6 MHz (e.g., Europe)
- 902–928 MHz (e.g., North America)
- 2400–2483.5 MHz (worldwide)
- 3100-10600Mhz (UWB introdotta dalla draft 2007 e variabile da paese a paese)

Il livello **MAC** fornisce due servizi, analogamente al livello fisico: *MAC Data service* e *MAC management service*. Questi si interfacciano con l'unità di gestione del livello MAC ed access point denominato *MLME-SAP (MAC sublayer management entity service access point)*. Compito del *MAC data service* è l'abilitazione della trasmissione e ricezione delle unità dati del livello MAC, ovvero dei *MPDUs (MAC protocol data units)*, attraverso il *PHY data service*.

Altre funzioni rivestite da questo livello sono la gestione dei beacon, l'accesso al canale, la gestione di *GTS (guaranteed time slot)*, la validazione dei frame, gli acknowledged frame delivery, le associazioni e dissociazioni dei dispositivi e fa, inoltre, da aggancio per implementare applicativi di sicurezza.

1.6 Presentazione delle funzioni

Qui di seguito descriveremo in breve alcune funzioni generali delle LR-WPAN, fra cui: superframe structure, modello trasferimento dati, struttura del frame, robustezza, consumo energetico, sicurezza e precision ranging.

1.6.1 Superframe structure

E' una modalità di accesso al canale in regime di beacon abilitati. Non è obbligatorio utilizzare la struttura superframe, in caso il coordinatore non la volesse usare sarà sufficiente disabilitare la trasmissione dei beacon. Il

superframe non è altro che una divisione del tempo in 16 slot di uguali dimensioni ed è fortemente legata ai beacon poiché essi sono spediti periodicamente durante il primo slot di ogni superframe e la loro funzione è quella di sincronizzare i dispositivi connessi, identificare il PAN e descrivere la struttura del superframe.

Nell'intervallo fra due beacon avviene la fase *Contention Access Period* (CAP) durante la quale i dispositivi che vogliono comunicare si contendono il canale tramite meccanismi CSMA-CA [o ALOHA introdotti dalla draft del 2007]. Ogni transazione deve comunque terminare entro il tempo previsto di invio del prossimo beacon.

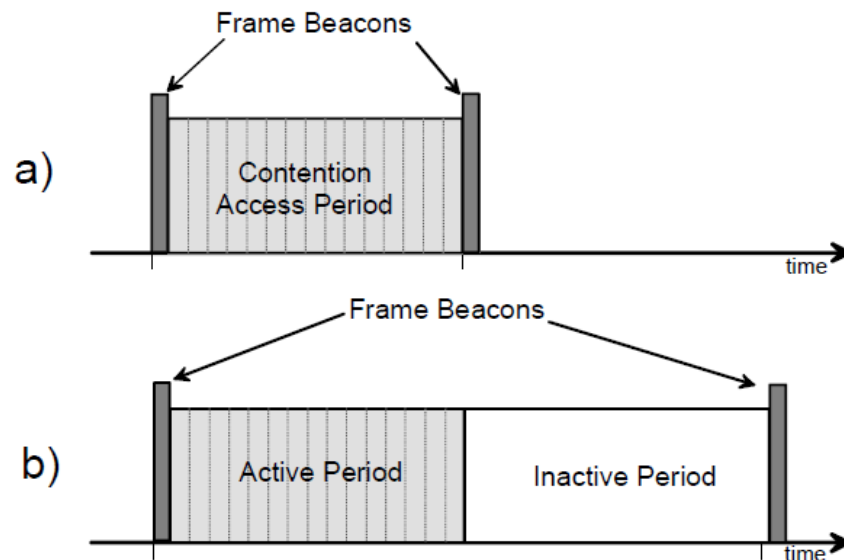


Figura 7: Contention Access Period e Periodi attivi e inattivi

Il superframe può avere porzioni attive e inattive: questo è importante per risparmiare sul consumo energetico. Durante la porzione inattiva il coordinatore può non interagire con la rete e attivare quindi una modalità a consumo ridotto.

Compito del coordinatore è anche valutare se esistono applicazioni che necessitano di bassi tempi di latenza o di una specifica bandwidth. In questi casi può riservare delle porzioni di superframe, fino a un massimo di 7 slot, ed allocarli a GTS (guaranteed time slots) creando un periodo contention free (CFP). Il contention free period, se esiste, segue sempre il contention access period.

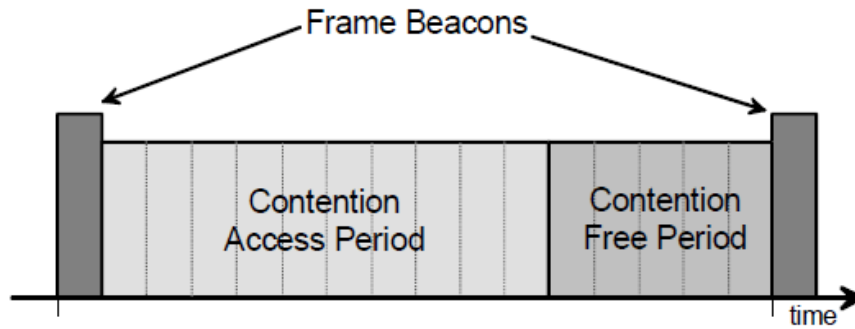


Figura 8: Contention Free Period

1.6.2 Data transfer model

Esistono tre diversi tipi di trasferimento dati:

- da un dispositivo al coordinatore (data transfer to a coordinator)
- dal coordinatore ad un dispositivo (data transfer from a coordinator)
- da un dispositivo ad un altro dispositivo (peer to peer data transfer)

In una topologia di rete a stella incontreremo solo i primi due tipi di trasferimento, mentre il terzo è tipico delle topologie peer to peer. Ogni tipo di trasferimento è regolato in maniera differente a seconda che la rete supporti la trasmissione dei beacon oppure no. L'abilitazione dei beacon è utile soprattutto in quei contesti in cui abbiamo low latency device, come il caso delle periferiche dei pc, se non ho questo genere di dispositivi si può normalmente utilizzare una modalità con beacon disabilitati per trasferimenti normali, mentre continueranno ad essere utili e necessari al momento dell'associazione dei dispositivi alla rete. Passiamo a capire come funzionano e in cosa si differenziano i vari modelli di trasferimento dati.

Data transfer to a coordinator – beacon enabled

In questa modalità quando un dispositivo vuol trasferire dati a coordinatore prima ascolta il canale in attesa del network beacon. Una volta ricevuto il beacon si sincronizza sulla struttura del superframe e quando è il momento trasmette

utilizzando la modalità di accesso al canale slotted CSMA-CA [o ALOHA introdotta dalla draft 2007]. Una volta trasmesso il data frame il coordinatore che l’ha ricevuto può inviare l’ack di conferma della ricezione. L’acknowledgment è opzionale e dipende dalle impostazioni della rete.

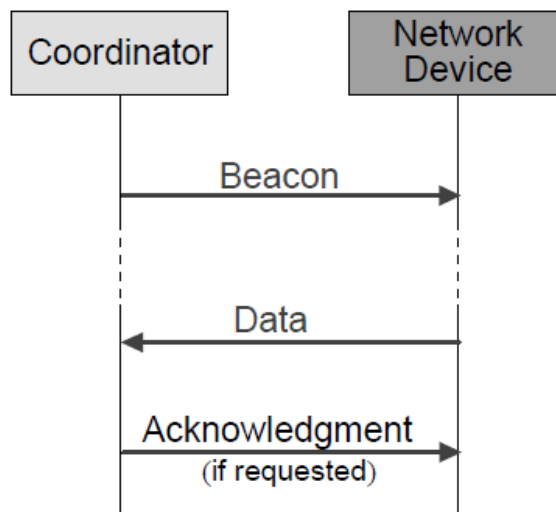


Figura 9: Comunicazione da device a coordinatore con beacon abilitati

Data transfer to a coordinator – beacon disabled

Se un device vuole trasmettere al coordinatore nel caso in cui i beacon non siano abilitati lo fa semplicemente senza ascoltare prima il canale, usando unslotted CSMA-CA [o ALOHA introdotta da draft 2007].

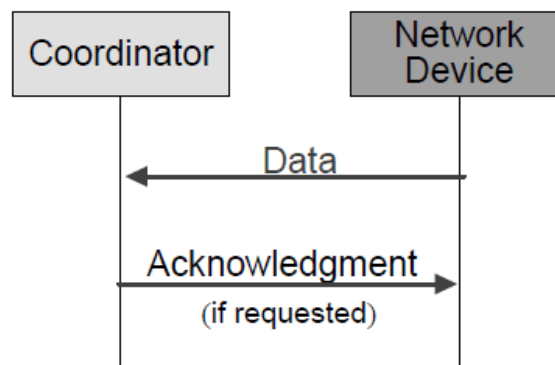


Figura 10: Comunicazione da device a coordinatore con beacon disabilitati

Data transfer from a coordinator – beacon enabled

Il coordinatore che vuole trasmettere a un dispositivo in una rete con beacon abilitati trasmette un beacon in cui indica che esistono messaggi in sospeso. I device ascoltano periodicamente il canale in attesa dei beacon e “leggendo” che esistono messaggi in sospeso inviano una richiesta MAC (*MAC command*) usando slotted CSMA-CA per richiedere il pacchetto dati.

Il data frame in attesa viene spedito a sua volta utilizzando slotted CSMA-CA, è opzionale l’invio di un ack di conferma ricezione dal device al suo ricevimento. La transazione ora è completa e l’indicazione di messaggi in sospeso viene rimossa dal beacon.

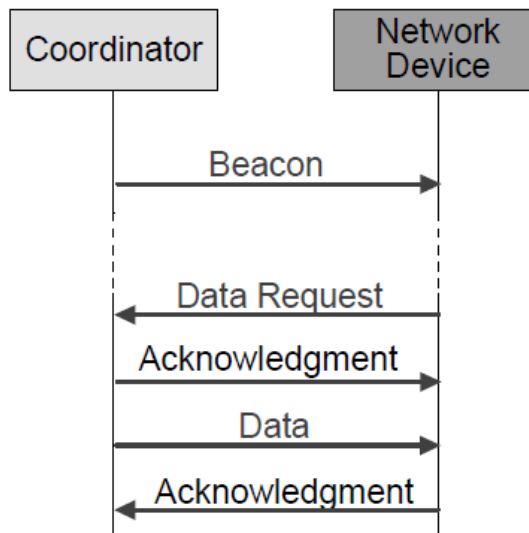


Figura 11: Comunicazione da coordinatore a device con beacon abilitati

Data transfer from a coordinator – beacon disabled

Se un coordinatore ha dati da spedire invece di comunicarlo tramite un beacon immagazzina il data frame pendente. Un device può contattare il coordinatore inviandogli un MAC command per richiedere eventuali pacchetti in attesa di invio, utilizzando unslotted CSMA-CA. A questo punto il coordinatore invia un ack relativo al ricevimento della richiesta e

successivamente invia un data frame. Nel caso non esistano dati in attesa di invio questo sarà un frame con payload a lunghezza zero. La trasmissione termina dopo la ricezione dell’ack inviato dal device al coordinatore per confermare di aver ricevuto il data frame.

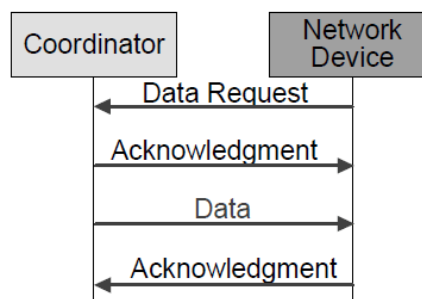


Figura 12: Comunicazione da coordinatore a device con beacon disabilitati

Peer to peer data transfer

In una PAN peer to peer ogni dispositivo può comunicare con ogni altro nella sfera radio di copertura. Per poterlo fare i device che vogliono comunicare devono ricevere costantemente o sincronizzarsi. Se stanno ricevendo in modo costante, nel momento in cui vogliono trasmettere è sufficiente che lo facciano trasmettendo i loro data frame usando unslotted CSMA-CA. In caso contrario, ovvero in caso sia necessaria la sincronizzazione sono necessari altri provvedimenti che tuttavia non sono trattati dallo standard IEEE 802.15.4.

1.6.3 Frame structure

La struttura dei frame è studiata appositamente per ridurre al minimo la complessità, ma al tempo stesso per garantire la robustezza della trasmissione su un canale che non essendo cablato è facilmente soggetto a interferenze. Ogni livello successivo dello stack ISO/OSI aggiunge rispetto a quelli qui trattati un header e footer rispettivamente a inizio e fine del frame.

La specifica LR-WPAN distingue 4 tipologie di struttura:

- *Beacon frame*
- *Data frame*
- *Acknowledgment frame*
- *MAC command frame*

La differenza sostanziale è nella parte gestita dal MAC service data unit (MSDU), ad ogni modo ora le esamineremo una ad una sia per la struttura a livello fisico che MAC.

Beacon Frame

E' usato dal coordinator nella modalità beacon enabled per trasmettere i beacon per l'appuntamento. Il frame può essere identificato come suddiviso in tre parti: un'intestazione, un corpo centrale e una coda. Il corpo centrale è il MAC service data unit (MSDU) ed è formato da: specifica del superframe, specifica degli indirizzi sospesi, lista indirizzi e campi beacon payload e GTS. L'intestazione, MAC header (MHR), contiene campi di controllo del

frame MAC, il beacon sequence number (BSN) e campi indirizzo. La coda, il MAC footer (MFR) contiene 16bit *frame check sequence (FCS)*. Tutte le tre parti unite formano il MAC beacon frame (*MPDU*).

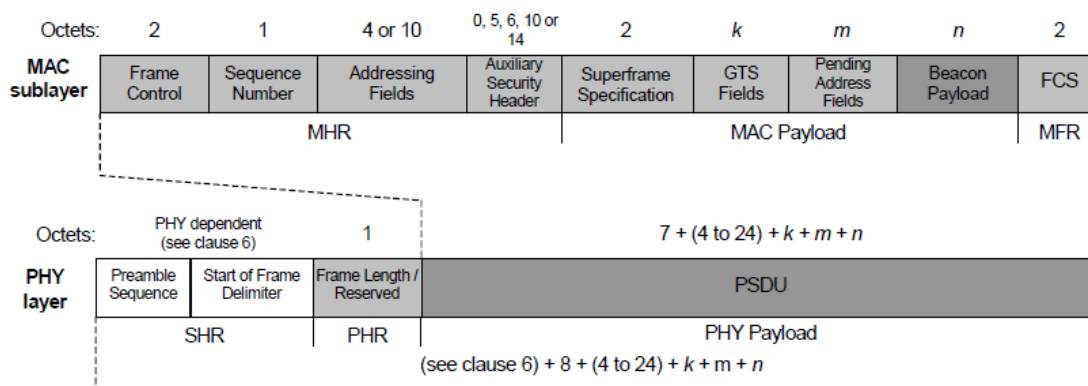


Figura 13: beacon frame

Il MAC beacon frame viene passato al livello fisico come *PHY service data unit (PSDU)*. Il livello fisico aggiunge un'ulteriore intestazione, composta dal *synchronization header (SHR)* e dal *PHY header (PHR)*. La prima contiene la preamble sequence, che serve ad abilitare il ricevente ad ottenere i simboli della sincronizzazione, e i campi *start-of-frame delimiter (SFD)*. L'header del livello fisico (PHR), invece, contiene la lunghezza in byte del PSDU. Queste tre parti costituiscono il *PHY beacon packet (PPDU)*.

Data Frame

Il frame è diviso in tre parti: un'intestazione, un corpo centrale e una coda. Il corpo centrale è il MAC service data unit (MSDU) ed è formato dai dati, l'intestazione è il MAC header e contiene frame control, sequence number (DSN) e campi indirizzo, mentre la coda è il MAC footer e contiene 16 bit *frame check sequence (FCS)*. Tutte le tre parti unite formano il MAC data frame (*MPDU*).

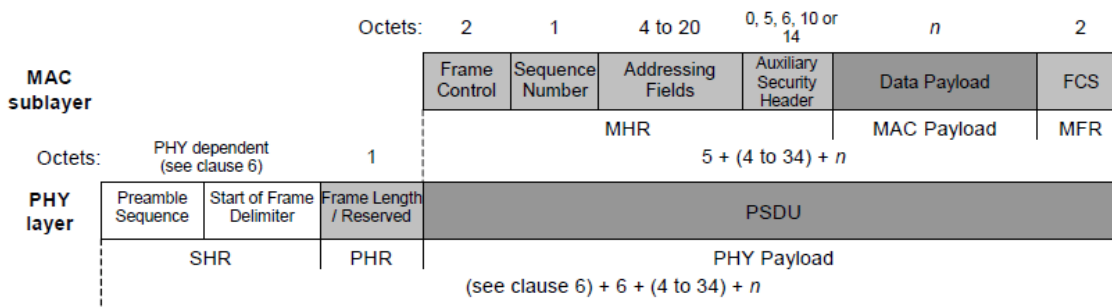


Figura 14: data frame

Il MAC data frame viene passato al livello fisico come *PHY service data unit (PSDU)* ovvero la parte centrale che contiene i dati. Il livello fisico aggiunge un'ulteriore intestazione, composta dal *synchronization header (SHR)* e dal *PHY header (PHR)*. La prima contiene la *preamble sequence*, che serve ad abilitare il ricevente ad ottenere i simboli della sincronizzazione, e i campi *start-of-frame delimiter (SFD)*. L'header (PHR) del livello fisico, invece, contiene la lunghezza in byte del PSDU. Queste tre parti costituiscono il *PHY data packet (PPDU)*.

Acknowledgment Frame

L'acknowledgment frame è creato dal livello MAC. E' formato unicamente da intestazione (MHR) e coda (MFR), non esiste la parte centrale contenente dati. L'header contiene i campi di controllo propri dei frame MAC e DSN (data sequence number). Il footer è composto come nelle altre tipologie di frame da 16 bit *frame check sequence (FCS)*. Le due parti unite formano il MAC acknowledgment frame (*MPDU*).

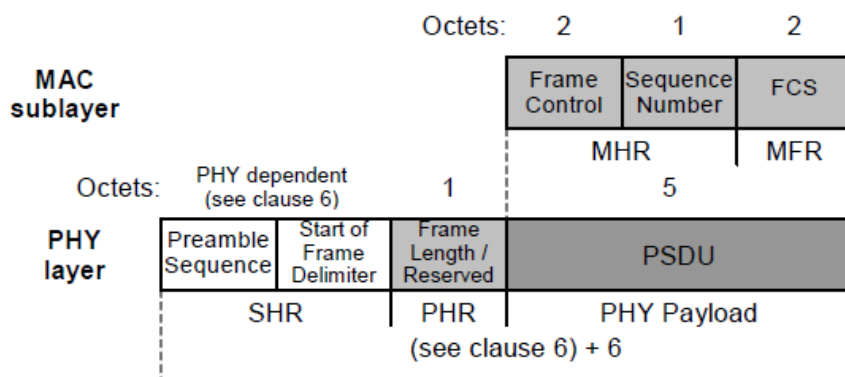


Figura 15: acknowledgment frame

Il MAC acknowledgment frame viene passato al livello fisico come *PHY service data unit (PSDU)* ovvero la parte centrale che contiene i dati. Il livello fisico aggiunge un'ulteriore intestazione, composta dal *synchronization header (SHR)* e dal *PHY header (PHR)*. La prima contiene la preamble sequence, che serve ad abilitare il ricevente ad ottenere i simboli della sincronizzazione, e i campi *start-of-frame delimiter (SFD)*. L'header del livello fisico, invece, contiene la lunghezza in byte del PSDU. Queste tre parti costituiscono il *PHY data packet (PPDU)*.

MAC Command Frame

Il MAC command frame è creato dal livello MAC. La parte data contiene il tipo di comando MAC e sarà affrontata più nel dettaglio nel corso di questo documento. Al payload sono aggiunti come nelle altre strutture di frame un'intestazione (MHR) e coda (MFR). L'header contiene i campi di controllo propri dei frame MAC e DSN, i campi indirizzo ed eventualmente intestazioni ausiliarie di sicurezza. Il footer è composto come nelle altre tipologie di frame da 16 bit *frame check sequence (FCS)*. MAC payload, MHR e MFR formano il MAC acknowledgment frame (*MPDU*).

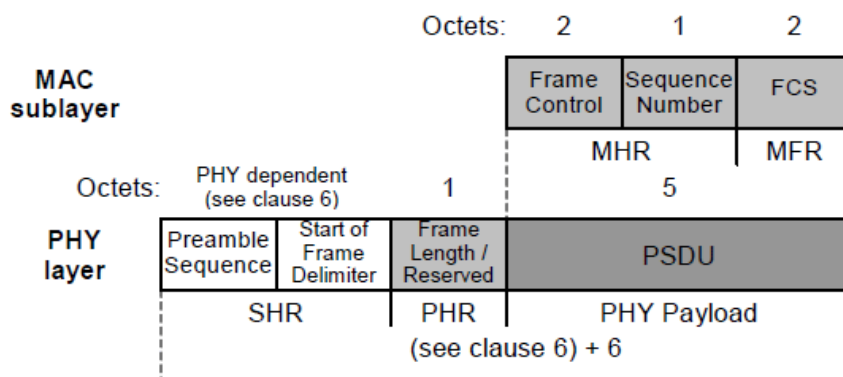


Figura 15: acknowledgment frame

Il MAC command frame viene passato al livello fisico come *PHY service data unit (PSDU)* ovvero la parte centrale che contiene i dati (payload). Il livello fisico aggiunge un'ulteriore intestazione, composta dal *synchronization header (SHR)* e dal *PHY header (PHR)*. La prima contiene la preamble sequence, che serve ad abilitare il ricevente ad ottenere i simboli della sincronizzazione, e i campi *start-of-frame delimiter (SFD)*. L'header del livello

fisico, invece, contiene la lunghezza in byte del PSDU. Queste tre parti costituiscono il *PHY data packet (PPDU)*.

1.6.4 Robustness

Le reti LR-WPAN si servono di diversi meccanismi per assicurare la robustezza della trasmissione. Questi sono: la modalità di accesso CSMA-CA, i frame acknowledgment e la verifica dei dati (data verification). Li esamineremo qui di seguito.

CSMA-CA mechanism

LR-WPAN usa due tipi alternativi di accesso al canale, quale di questo sia quello in uso dipende dalle configurazioni della rete.

Nelle reti con beacon disabilitati l'accesso al canale è gestito tramite unslotted CSMA-CA. Ogni volta che un dispositivo vuole trasmettere aspetta per un periodo a casuale, se il canale è trovato libero, seguendo il random backoff, inizia a trasmettere. Se il canale risulta occupato seguendo il random backoff aspetta un altro periodo casuale prima di provare ad accedere nuovamente al canale. Gli ack vengono poi spediti senza seguire il meccanismo CSMA-CA.

Nelle reti con beacon abilitati, invece, l'accesso al canale è gestito tramite slotted CSMA-CA. All'inizio di ogni trasmissione beacon i backoff slot vengono sincronizzati. Quando un device vuole trasmettere data frames durante il CAP (contention access period), deve aspettare il backoff slot successivo e aspettare per un numero casuale di slot. Se il canale è occupato occorre attendere per un altro numero random di slot, altrimenti può iniziare a trasmettere all'inizio dello slot successivo. Anche in questa modalità gli ack, ma anche i beacon, sono spediti senza utilizzare questo meccanismo.

Frame acknowledgment

Al termine della ricezione e della validazione di un data frame o di un MAC command frame il dispositivo può in forma opzionale confermare il buon fine della trasmissione per mezzo di un ack. Ovviamente in caso di

mancata ricezione l'acknowledgment non viene spedito. Se il mittente originale non riceve l'ack in un certo lasso di tempo assume che la trasmissione non sia andata a buon fine e può scegliere se ritentare l'invio. Se l'ack non è richiesto il mittente assume che la comunicazione sia andata a buon fine.

Data verification

Il trasferimento dei dati è molto suscettibile soprattutto nelle reti wireless ad interferenze o perdite di segnale che potrebbero danneggiare i pacchetti trasmessi. Per questo a livello MAC è incluso un footer composto da 16 bit International Telecommunication Union–Telecommunication Standardization Sector (ITU-T) cyclic redundancy check (CRC) volti alla detenzione degli errori.

1.6.5 Consumo energetico (power consumption)

Abbiamo già parlato in precedenza nel corso di questo capitolo come facilmente esista la possibilità che i device siano alimentati unicamente per mezzo di batterie. E' facile pensare come sia impraticabile l'idea di cambiarle in tempi brevi, per questo motivo il consumo energetico è un punto fondamentale di questo standard, che pone l'obiettivo di ridurre al minimo il consumo energetico e garantire periodi anche superiori all'anno per la durata delle batterie. Per ottenere questo scopo i device senza alimentazione autonoma passano la maggior parte del tempo dormienti, ascoltando, ad ogni modo, periodicamente il canale in attesa di eventuali messaggi in sospenso. E' possibile configurare la rete e i dispositivi in modo da bilanciare il trade off fra ascolto e consumo. Al contrario i dispositivi autoalimentati possono ascoltare in modo continuato il canale.

Questa tecnologia nasce rivolta ai dispositivi a basso consumo e alimentati a batteria, tuttavia in certi casi l'alimentazione autonoma è un requisito fondamentale al funzionamento della rete.

1.6.6 Sicurezza

Riguardo alla sicurezza a livello MAC, diverse funzioni sono necessarie a garantire un livello base di sicurezza e l'interoperabilità. Questo livello minimo include: ACL (access list control), ovvero tenere traccia degli accessi e l'utilizzo di chiavi simmetriche per proteggere i frame trasmessi. Da notare che le precedenti sono abilità che devono essere garantite anche se non è detto che siano poi utilizzate, la scelta dipende da device a device e sono i livelli superiori a decidere se servirsi delle funzioni di sicurezza a livello MAC. Anche la gestione delle chiavi, la protezione e l'autenticazione sono lasciate ai livelli più alti.

Security Services

La sicurezza è basata su chiavi simmetriche, che come scritto qualche riga sopra, sono fornite dai livelli più alti dello stack ISO/OSI. La gestione e l'implementazione di queste è lasciata all'implementatore, mentre al contrario lo standard IEEE 802.15.4 tramite i security services a livello MAC si occupa di come queste siano generate, salvate e trasmesse in modo affidabile e sicuro. Vediamo qui di seguito quali sono i servizi forniti dal livello MAC:

- Access Control: è un servizio che permette a un device di scegliere con chi vuole comunicare. Se questo servizio è fornito i dispositivi possono tenere in memoria una lista degli altri dispositivi da cui si aspettano di ricevere frame.
- Data encryption: è un servizio che cripta i dati con chiave simmetrica. La chiave può essere condivisa da un gruppo di dispositivi oppure semplicemente da due soli device. Questo servizio è fornito in beacon payload, command payload e data payload.
- Frame integrity: è un servizio che protegge il messaggio dall'essere modificato (tramite MIC message integrity code) in assenza della chiave crittografica. Questo servizio è fornito solo per beacon

frame, data frame e MAC command frame. La chiave può essere condivisa da un gruppo o da due soli peer.

- Sequential freshness: è un servizio che scarta i data frame non nuovi. Il livello di “freschezza” di un frame (freshness) viene indicato da un valore numerico e questo servizio si occupa di confrontarlo con il valore precedente. Se il valore è più nuovo il frame passa, altrimenti viene scartato.

Security Modes

Il livello MAC a seconda della modalità in cui un device sta operando e della modalità di sicurezza prescelta può attivare o meno diversi profili:

- Unsecured Mode: tutti i servizi di sicurezza sono disabilitati.
- ACL Mode: servizi di sicurezza limitati. Ad esempio la crittografia è disabilitata.
- Secured Mode: i servizi forniti dipendono dalla suite di sicurezza in uso. Possono essere forniti: access control, data encryption, frame integrity e sequential freshness.

2. Il livello fisico

2.1 Requisiti generali e definizioni

Le responsabilità del livello fisico sono le seguenti:

- Attivare e disattivare il trasmettitore
- Energy detection (ED)
- Link quality indicator (LQI) per i pacchetti ricevuti
- Clear channel assessment (CCA) per carrier sense multiple access collision avoidance (CSMA-CA)
- Selezionare la frequenza del canale
- Trasmettere e ricevere dati.

Lo standard specifica quattro frequenze e canali fisici (PHY):

- 868/915 MHz direct sequence spread spectrum (DSSS) PHY che utilizza la modulazione binary phase-shift keying (BPSK)
- 868/915 MHz DSSS PHY che utilizza la modulazione offset quadrature phase-shift keying (O-QPSK) [introdotto dalla specifica del 2006, non esisteva nella prima formulazione del 2003]
- 868/915 MHz parallel sequence spread spectrum (PSSS) PHY che utilizza la modulazione BPSK e amplitude shift keying (ASK) [introdotto dalla specifica del 2006, non esisteva nella prima formulazione del 2003]
- 2450 MHz DSSS PHY che utilizza la modulazione O-QPSK

La banda 868/915 offre un buon trade off fra complessità e data rate. Entrambe le frequenze introdotte dalla specifica del 2006, grazie al sistema di modulazione più complesso, garantiscono un bitrate superiore rispetto a 868/915 MHz BPSK PHY, parliamo di 20kb/s per la frequenza 868MHz e 40kb/s per la frequenza 915MHz contro i 250kb/s che possono essere raggiunti su entrambe le frequenze 868/915MHz tramite la modulazione ASK. Questo bitrate eguaglia quello raggiunto dalla frequenza 2450MHz.

Utilizzando la modulazione O-QPSK raggiungiamo invece i 100kb/s sulla frequenza 868Mhz e 250kb/s sulla banda dei 915MHz.

[Nella draft 2007 sono stati aggiunti ulteriori 2 PHY, precisamente 2 HIGH RATE PHY UWB operanti nella fascia fra i 3-10Ghz].

2.1.1 Range frequenze operative

I dispositivi usano la modalità fisica per cui stati istruiti ad operare, sebbene siano in grado di operare su diversi PHY e di passare da un ad un altro dinamicamente. Qui di seguito riportiamo una tabella riassuntiva dei diversi PHY con relative frequenze, tipo modulazione e bitrate.

PHY (MHz)	Frequency band (MHz)	Spreading parameters		Data parameters		
		Chip rate (kchip/s)	Modulation	Bit rate (kb/s)	Symbol rate (ksymbol/s)	Symbols
868/915	868–868.6	300	BPSK	20	20	Binary
	902–928	600	BPSK	40	40	Binary
868/915 (optional)	868–868.6	400	ASK	250	12.5	20-bit PSSS
	902–928	1600	ASK	250	50	5-bit PSSS
868/915 (optional)	868–868.6	400	O-QPSK	100	25	16-ary Orthogonal
	902–928	1000	O-QPSK	250	62.5	16-ary Orthogonal
2450	2400–2483.5	2000	O-QPSK	250	62.5	16-ary Orthogonal

Tabella 1 – frequenze e data rates

2.1.2 Assegnazione canale

Con l'introduzione nella specifica del 2006 di due nuovi PHY i 32 channel numbers previsti dalla versione precedente si sono dimostrati non più sufficienti. Per supportare questa crescita è stato necessario definire un nuovo criterio, stabilito dalla combinazione di channels number e channel pages.

I 5 bit più significativi (MSBs) dei 32-bit channel bitmaps nell'attributo *phyChannelsSupported* sono usati per specificare il valore intero dei 32 possibili channel pages. I 27 bit meno significativi sono usati per specificare il channel number all'interno del channel page.

Channel Numbering

Vi sono un totale di 27 canali numerati da 0 a 26 disponibili per ogni channel page.

Channel page 0: 27 canali numerati da 0 a 26 disponibili su 3 differenti frequenze. 17 sono nella banda 2450Mhz, 10 nella 915Mhz e 1 nella 868Mhz. E' stato stabilito nella specifica del 2003 e la frequenza è definita secondo la seguente formula:

$$F_c = 868.3 \text{ in megahertz, per } k = 0$$

$$F_c = 906 + 2 (k - 1) \text{ in megahertz, per } k = 1, 2, \dots, 10$$

$$\text{and } F_c = 2405 + 5 (k - 11) \text{ in megahertz, per } k = 11, 12, \dots, 26$$

dove

k è il channel number.

Channel page 1 e 2: 11 canali numerati da 0 a 10 disponibili su 2 differenti frequenze, 1 che supporta 868 Mhz ASK e 10 nella banda 915 Mhz O-QPSK. La frequenza è definita secondo la seguente formula:

$$F_c = 868.3 \text{ in megahertz, per } k = 0$$

$$\text{e } F_c = 906 + 2 (k - 1) \text{ in megahertz, per } k = 1, 2, \dots, 10$$

dove

k è il channel number.

Channel Pages

Sono disponibili un totale di 32 channel pages, tuttavia di questi sono realmente disponibili e utilizzati solo quelli da 0 a 2. I channel pages compresi fra 3 e 31 sono riservati per usi futuri.

Qui di seguito riportiamo una tabella riassuntiva dei channel pages utilizzati e relativi channel numbers.

Channel page (decimal)	Channel page (binary) (b ₃₁ , b ₃₀ , b ₂₉ , b ₂₈ , b ₂₇)	Channel number(s) (decimal)	Channel number description
0	0 0 0 0 0	0	Channel 0 is in 868 MHz band using BPSK
		1–10	Channels 1 to 10 are in 915 MHz band using BPSK
		11–26	Channels 11 to 26 are in 2.4 GHz band using O-QPSK
1	0 0 0 0 1	0	Channel 0 is in 868 MHz band using ASK
		1–10	Channels 1 to 10 are in 915 MHz band using ASK
		11–26	Reserved
2	0 0 0 1 0	0	Channel 0 is in 868 MHz band using O-QPSK
		1–10	Channels 1 to 10 are in 915 MHz band using O-QPSK
		11–26	Reserved
3–31	0 0 0 1 1 - 1 1 1 1	reserved	Reserved

Tabella 2 – Channel pages e channel number

2.1.3 *Minimum long interframe spacing (LIFS) e short interframe spacing (SIFS) periods*

La durata minima per LIFS e SIFS è riportata nella tabella seguente ed espressa in simboli come unità di misura.

PHY	<i>macMinLIFSPeriod</i>	<i>macMinSIFSPeriod</i>	Units
868–868.6 MHz BPSK	40	12	Symbols
902–928 MHz BPSK	40	12	Symbols
868–868.6 MHz ASK	40	12	Symbols
902–928 MHz ASK	40	12	Symbols
868–868.6 MHz O-QPSK	40	12	Symbols
902–928 MHz O-QPSK	40	12	Symbols
2400–2483.5 MHz O-QPSK	40	12	Symbols

Tabella 3 – Periodi minimi LIFS e SIFS

Come notiamo, l'indicazione minima è la medesima per tutte le frequenze di banda anche indipendentemente dal metodo di codifica utilizzato.

2.1.4 Misura della potenza del segnale

Se non è specificato diversamente, sia in fase di trasmissione sia in fase di ricezione la misura della potenza del segnale deve essere fatta dall'apposito trasmittente sul connettore dell'antenna. Il dispositivo con cui effettuare la misurazione deve essere adatto all'impedenza dell'antenna connector, oppure deve essere corretta in qualche maniera per ogni non corrispondenza. Per i dispositivi che non hanno antenna connector la misura deve essere interpretata come effective isotropic radiated power (EIRP) (i.e., a 0 dBi gain antenna) e ogni misura deve essere corretta per compensare il guadagno dell'antenna nell'implementazione.

2.1.5 Potenza della trasmissione

La potenza massima della trasmissione deve seguire le regolamentazioni locali (solitamente in termini di EIRP).

2.1.6 Sensibilità del ricevente

Packet error rate (PER): è la frazione media dei pacchetti trasmessi che non sono stati individuati correttamente. Si misura sui pacchetti PSDU.

Receiver sensitivity: è la soglia di potenza del segnale ad uno specifico PER. Si intende in condizione di PSDU pari a 20byte, PER <1%, assenza di interferenza e potenza misurata al termine dell'antenna.

2.2 Specifiche dei servizi del livello fisico

Il livello fisico funge da interfaccia fra il livello MAC e il canale radio fisico, tramite il radio frequency (RF) firmware e software. Concettualmente include un'entità di gestione denominata PLME che a sua volta fornisce un'interfaccia ai servizi che possono essere invocati dalle funzioni. E' di sua competenza anche la gestione del database degli oggetti gestiti, il quale è riferito al PHY PAN information base (PHY PIB).

I servizi forniti sono due e l'accesso ad essi avviene tramite due service access point (SAP) differenti, il PHY data SAP (PD-SAP) relativo al servizio PHY data service e il PLME-SAP relativo al servizio PHY management service. Nei paragrafi seguenti andremo ad analizzare meglio ogni servizio e i tipi di primitive che supporta.

2.2.1 PHY Data Service

Il servizio PHY Data Service supporta tramite il suo SAP, PD-SAP, il trasporto di unità dati a livello MAC (ovvero MPDUs). PD-SAP supporta tre tipi di primitive:

- PD-DATA request: richiede il trasferimento di un MPDU dal livello MAC al livello fisico. Questa primitiva è composta da PSDU (frame a livello MAC viene inserito in un pacchetto a livello fisico, tutto il MPDU conferirà nel PSDU) e psduLenght. Il tipo del primo parametro è un set di byte, dimensione variabile, il secondo è un numero intero rappresentante la dimensione in byte del PSDU e per ovvie ragioni la sua dimensione deve essere inferiore alla dimensione totale del pacchetto a livello fisico. Ha per effetto la spedizione del PSDU, per cui viene attivata la trasmittente e il PSDU viene inglobato in un'unità di livello fisico PDDU. A trasferimento completato viene generato il PD-data.confirm con status= SUCCESS.
- PD-DATA confirm: conferma la fine della trasmissione dal livello MAC dell'entità locale al livello MAC di un altro peer. E' formato dal parametro *status* i cui valori ammessi sono SUCCESS (nel caso in cui la trasmissione sia stata completata) e RX_ON o TRX_OFF che sono messaggi di errore, il primo riferito al caso in cui PD-DATA.request sia ricevuta mentre il ricevente è abilitato, la seconda se è disabilitato.
- PD-DATA Indication: indica il trasferimento di un MPDU dal livello fisico al livello MAC locale. E' composto dai seguenti parametri: psduLenght, psdu, ppduLinkQuality. I primi due sono i medesimi che troviamo nel PD-DATA.request, il terzo è un intero nel range compreso fra 0x00 e 0xff ed è un valore misurato durante la ricezione del PPDU. E' generato dal

livello fisico che deve trasferire un PSDU ricevuto al livello MAC. Come effetto il livello MAC dovrà confermare la ricezione tramite il PHY Data Service.

2.2.2 PHY Management Service

Il servizio PHY Management Service supporta tramite il suo SAP, PLME-SAP, il trasporto dei comandi di gestione fra PLME e MLME. Supporta le seguenti primitive:

- PLME-CCA:
 - *PLME-CCA.request*: non ha parametri, è generato dal MLME e passato al PLME quando l'algoritmo CSMA-CA sta valutando il canale. Porta il livello fisico ad eseguire CCA (clear channel assessment), che il cui risultato apparirà tramite PLME-CCA.confirm con status BUSY oppure IDLE, in caso di errore avremo status RX_ON o TRX_OFF, il primo riferito al caso in cui il ricevente sia abilitato, la seconda in caso sia disabilitato.
 - *PLME-CCA.confirm*: ritorna il risultato della CCA. Ha un parametro status che riporta IDLE, BUSY, RX_ON oppure TRX_OFF. Il ricevimento di questa primitiva viene poi notificato a MLME.
- PLME-ED:
 - *PLME-ED.request*: richiede esecuzione di misura del consumo energetico (ED energy detection). E' generata da MLME e poi passata a PLME, non ha parametri e come esito produce PLME-ED.confirm con esito SUCCESS oppure con errore di tipo RX_ON o TRX_OFF.
 - *PLME-ED.confirm*: ritorna il risultato della misura del consumo energetico. Ha due parametri: status (come citato sopra SUCCESS, RX_ON o TRX_OFF) e EnergyLevel, composto da un numero nel range da 0x00 a 0xff che riporta il livello di energy detection del canale corrente.

- PLME-GET:
 - *PLME-GET.request*: richiede informazioni su un dato PHY PIB. Come parametro viene passato l'attributo del PAN information base. E' generato dal MLME e al suo ricevimento il PLME va a ricercare nel database l'attributo richiesto, generando un PLME-GET.confirm con parametro status uguale a SUCCESS se il PIB richiesto è trovato, oppure ad UNSUPPORTED_ATTRIBUTE in caso contrario.
 - *PLME-GET.confirm*: ritorna il risultato di PLME-GET.request. Contiene tre parametri: status (SUCCESS oppure UNSUPPORTED_ATTRIBUTE), PIBAttribute, PIBAttributeValue
- PLME-SET-TRX-STATE:
 - *PLME-SET-TRX.request*: è una richiesta di modificare lo stato operativo interno del trasmettitore. Il suo parametro è status. I tre stati possibili, citati sopra come possibili errori di altre primitive, sono: TRX_OFF (trasmittente disabilitato), TX_ON (trasmittente abilitato) oppure RX_ON (receiver abilitato). Il suo effetto produce il cambiamento dello status come richiesto in caso di successo o errore in caso sia da rimandare alla fine di una trasmissione esistente.
 - *PLME-SET-TRX.confirm*: è la risposta alla richiesta di cui sopra e riporta come parametro lo status attuale: TRX_OFF, TX_ON, RX_ON, BUSY_RX, BUSY_TX. Questi ultimi due sono usati nel caso in cui non sia stato possibile modificare lo stato immediatamente.
- PLME-SET:
 - *PLME-SET.request*: è una richiesta di modifica dell'attributo PHY PIB a un dato valore e contiene come parametri PIBAttribute e PIBAttributeValue. Il cambiamento di dato valore può avere esito positivo oppure errore (UNSUPPORTED_ATTRIBUTE, INVALID_PARAMETER).
 - *PLME-SET.confirm*: ritorna il risultato di PLME-SET.request. Contiene due parametri, status (SUCCESS,

UNSUPPORTED_ATTRIBUTE, INVALID_PARAMETER) e PIBAttribute.

2.2.3 PHY Enumeration Description

Elencando i vari parametri delle primitive abbiamo spesso enunciato tipi numerici compresi nel range 0x00 e 0xff. Ognuno di questi corrisponde ad un messaggio specifico, come ad esempio gli status SUCCESS, RX_ON etc. Di seguito riportiamo una tabella che li vede nel dettaglio singolarmente.

Enumeration	Valore	Descrizione
BUSY	0x00	Canale occupato individuate da CCA
BUSY_RX	0x01	Trasmittente ha richiesto di cambiare lo stato durante ricezione
BUSY_TX	0x02	Trasmittente ha richiesto di cambiare lo stato durante trasmissione
FORCE_TRX_OFF	0x03	Trasmittente passato a OFF forzatamente
IDLE	0x04	CCA ha individuato canale inattivo (IDLE)
INVALID PARAMETER	0x05	Una richiesta SET o GET contiene un parametro fuori dal range
RX_ON	0x06	Trasmittente configurato per essere in stato di ricezione abilitata
SUCCESS	0x07	Un'operazione SET o GET, ED o transceiver state ha avuto esito positive
TRX_OFF	0x08	Trasmittente configurato in stato di trasmissione disabilitata
TX_ON	0x09	Trasmittente configurato con stato di trasmissione abilitata
UNSUPPORTED_ATTRIBUTE	0x0a	Una richiesta SET/GET è stata inviata con come identificatore un attributo non supportato

Tabella 4 – Descrizione PHY enumeration

2.3 Formato PHY Protocol Data Unit (PDDU)

Nel descrivere il formato PDDU troveremo più a sinistra nelle immagini i campi che sono trasferiti per primi. Quando un campo è composto da più byte, sono trasferiti per primi i byte più significativi.

		Octets		
		1	variable	
Preamble	SFD	Frame length (7 bits)	Reserved (1 bit)	PSDU
SHR		PHR		PHY payload

Figura 16 – PPDU Format

Ogni pacchetto PDDU è composto da:

SHR, synchronization header che consente al ricevente di sincronizzarsi e ottenere simboli e chip. Al suo interno troviamo due campi: preamble e SFD. Il primo nella specifica del 2003 era composto da 32 zero binari, mentre ora la sua lunghezza è variabile a seconda del canale utilizzato. Di seguito è riportato uno schema riassuntivo, ad ogni modo oscilla fra circa 4-5 byte e un numero fra 2 e 32 simboli.

PHY	Length		Duration (uS)
868–868.6 MHz BPSK	4 octets	32 symbols	1600
902–928 MHz BPSK	4 octets	32 symbols	800
868–868.6 MHz ASK	5 octets	2 symbols	160
902–928 MHz ASK	3.75 octets	6 symbols	120
868–868.6 MHz O-QPSK	4 octets	8 symbols	320
902–928 MHz O-QPSK	4 octets	8 symbols	128
2400–2483.5 MHz O-QPSK	4 octets	8 symbols	128

Tabella 5 – Preamble field length

SFD analogamente nella specifica del 2003 era posto pari 8bit fissi, mentre ora il suo valore è variabile come segue. Il suo scopo è indicare la fine del preamble e l'inizio del pacchetto dati.

PHY	Length	
	868–868.6 MHz BPSK	1 octet
902–928 MHz BPSK	1 octet	8 symbols
868–868.6 MHz ASK	2.5 octets	1 symbol
902–928 MHz ASK	0.625 octets	1 symbol
868–868.6 MHz O-QPSK	1 octet	2 symbols
902–928 MHz O-QPSK	1 octet	2 symbols
2400–2483.5 MHz O-QPSK	1 octet	2 symbols

Tabella 5 – SFD field length

PHR, PHY header che contiene le informazioni sulla lunghezza del frame. In totale corrisponde a 8bit, 7 dedicati ad esprimere la lunghezza del frame e 1 riservato. Fra i valori che il campo lunghezza frame può assumere ne troviamo alcuni riservati e altri con un valore specifico. Sono riportati nella tabella seguente.

Valore Frame Length	Payload
0-4	Riservato
5	MPDU (ack)
6-7	Riservato
Da 8 a aMaxPHYPacketSize	MPDU

Tabella 5 – Valori Frame length

Payload, ovvero PSDU, di lunghezza variabile che contiene il vero carico di dati. Se la dimensione supera i 7byte o è di 5 byte solitamente è segno che all'interno del PSDU è inglobato il frame MAC (ad es. MPDU).

2.4 PHY Constants

Le seguenti PHY Constants definiscono le caratteristiche del livello PHY, sono dipendenti dall'hardware e variano a seconda di esso. Non possono essere modificate durante il corso delle operazioni.

Constant	Description	Value
<i>aMaxPHYPacketSize</i>	The maximum PSDU size (in octets) the PHY shall be able to receive.	127
<i>aTurnaroundTime</i>	RX-to-TX or TX-to-RX maximum turnaround time (in symbol periods) (see 6.9.1 and 6.9.2)	12

Tabella 6 - PHY Constants

Le due costanti sopra citate indicano il valore massimo assumibile e la descrizione.

2.5 PHY PIB Attributes

Servono a gestire il device a livello fisico. Gli attributi possono essere letti o scritti tramite *PLME-GET.request* e *PLME-SET.request*. Alcuni di questi possono solo essere letti e non modificati tramite *PLME-SET*. Per distinguerli dagli altri sono indicati da una croce (†), altri permettono la modifica solo di alcuni bit e sono indicati con un asterisco (*).

Attribute	Identifier	Type	Range	Description
<i>phyCurrentChannel</i>	0x00	Integer	0–26	The RF channel to use for all following transmissions and receptions (see 6.1.2).
<i>phyChannelsSupported</i> [†]	0x01	Array	An R x 32 bit array, where R ranges from 1 to 32	The array is composed of R rows, each of which is a bit string with the following properties: The 5 MSBs (b ₂₇ , ..., b ₃₁) indicate the channel page, and the 27 LSBs (b ₀ , b ₁ , ..., b ₂₆) indicate the status (1=available, 0=unavailable) for each of the up to 27 valid channels (b _k shall indicate the status of channel k as in 6.1.2) supported by that channel page. The device only needs to add the rows (channel pages) for the PHY(s) it supports.
<i>phyTransmitPower</i> *	0x02	Bitmap	0x00–0xbf	The 2 MSBs represent the tolerance on the transmit power: 00 = ± 1 dB 01 = ± 3 dB 10 = ± 6 dB and shall be read-only. The 6 LSBs, which may be written to, represent a signed integer in twos-complement format, corresponding to the nominal transmit power of the device in decibels relative to 1 mW. The lowest value of <i>phyTransmitPower</i> is interpreted as less than or equal to -32 dBm.
<i>phyCCAMode</i>	0x03	Integer	1–3	The CCA mode (see 6.9.9).
<i>phyCurrentPage</i>	0x04	Integer	0–31	This is the current PHY channel page. This is used in conjunction with <i>phyCurrentChannel</i> to uniquely identify the channel currently being used.
<i>phyMaxFrameDuration</i> [†]	0x05	Integer	55, 212, 266, 1064	The maximum number of symbols in a frame: = <i>phySHRDuration</i> + $\text{ceiling}([a\text{MaxPHYPacketSize} + 1] \times \text{phySymbolsPerOctet})$
<i>phySHRDuration</i> [†]	0x06	Integer	3, 7, 10, 40	The duration of the synchronization header (SHR) in symbols for the current PHY.
<i>phySymbolsPerOctet</i> [†]	0x07	Float	0.4, 1.6, 2, 8	The number of symbols per octet for the current PHY.

Tabella 7 – PHY Attributes

2.6 Dettagli sulle specifiche di ogni frequenza di banda (limitato a quelle utilizzate da Zigbee)

2.6.1 2450Mhz PHY Specification

Data Rate: 250kb/s

Modulazione: O-QPSK modulation, 16-ary quasi-orthogonal modulation technique. Durante ogni data symbol period sono usati 4 bit di informazione per selezionare una delle 16 orthogonal pseudo-random noise (PN) più vicine. Le PN per i simboli successivi sono concatenate e la chip sequence aggregata viene modulata sul carrier usando O-QPSK (offset quadrature shift keying)

Il diagramma di riferimento per la modulazione è rappresentato nell'immagine seguente.

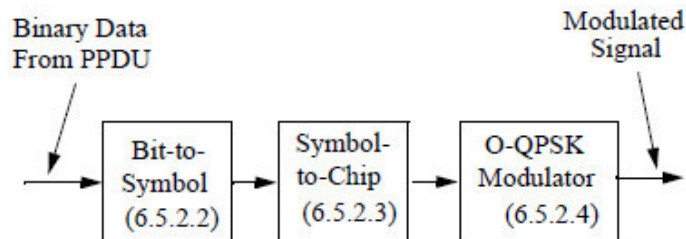


Figura 17 - Modulation e spreading functions

Un esempio di symbol to chip mapping è indicato nella tabella seguente, in cui vengono convertiti in una sequenza PN a 32 bit numeri da 0 a 15.

Data symbol (decimal)	Data symbol (binary) ($b_0 b_1 b_2 b_3$)	Chip values ($c_0 c_1 \dots c_{30} c_{31}$)
0	0000	11011001110000110101001000101110
1	1000	11101101100111000011010100100010
2	0100	00101110110110011100001101010010
3	1100	00100010111011011001110000110101
4	0010	01010010001011101101100111000011
5	1010	00110101001000101110110110011100
6	0110	11000011010100100010111011011001
7	1110	10011100001101010010001011101101
8	0001	10001100100101100000011101111011
9	1001	10111000110010010110000001110111
10	0101	01111011100011001001011000000111
11	1101	01110111101110001100100101100000
12	0011	00000111011110111000110010010110
13	1011	01100000011101111011100011001001
14	0111	10010110000001110111101110001100
15	1111	11001001011000000111011110111000

Tabella 8 – Symbol to chip mapping

Receiver sensitivity: un device conforme allo standard deve essere in grado di avere una sensibilità di almeno -85 dBm.

Receiver jamming resistance: Adjacent channel rejection 0dB, Alternate channel rejection 30dB.

2.6.2 868/915 MHz band binary phase-shift keying (BPSK) PHY Specification

Data Rate: 20 kb/s nella frequenza 868 MHz,
40 kb/s nella frequenza 915 MHz

Modulazione: direct sequence spread spectrum (DSSS) con BPSK usato per chip modulation e differential encoding usato per data symbol encoding.

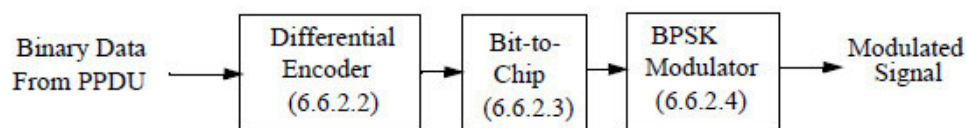


Figura 18 – Modulation e spreading functions

Ogni bit del PPDU è processato tramite differential encoding, bit-to-chip mapping e modulation functions in ordine di byte, iniziando dal campo Preamble e terminando con l'ultimo byte del PSDU.

Ogni bit viene mappato in una sequenza PN a 15 chip.

Input bits	Chip values (c_0 c_1 ... c_{14})
0	1 1 1 1 0 1 0 1 1 1 0 0 1 0 0 0
1	0 0 0 0 1 0 1 0 0 1 1 0 1 1 1 1

Tabella 9 – Symbol to chip mapping

Frequency range: 868.0–868.6 MHz e 902–928 MHz

Receiver sensitivity: almeno -92Dbm

Receiver jamming resistance: si applica solo alla frequenza 902-928Mhz, poiché la frequenza 868-868.6Mhz ha un unico canale.

Adjacent channel rejection 0dB, alternate channel rejection 30dB.

2.7 Transmit power

Un transmitter compatibile deve essere in grado di trasmettere almeno a -3dBm. I dispositivi devono essere in grado di trasmettere alla minor potenza possibile quando necessario in modo da ridurre le interferenze ad altri dispositivi e sistemi. La massima potenza di trasmissione è stabilita da regolamenti nazionali.

2.8 Receiver maximum input level del segnale desiderato

Il massimo livello di input del receiver rispetto al segnale desiderato è misurato in decibel relativi a 1mW. Il ricevente deve avere un receiver maximum input level uguale o superiore a -20 dBm.

3. Il livello MAC

3.1 Requisiti generali e definizioni

Il livello MAC è responsabile di:

- Generare i network beacon in caso in cui il dispositivo sia coordinatore
- Sincronizzarsi ai beacon
- Supportare le PAN association e disassociation
- Supportare sicurezza dei device
- Utilizzare CSMA-CA per l'accesso al canale
- Gestire e mantenere meccanismo guaranteed time slot (GTS)
- Fornire un canale affidabile fra due peer MAC entities.

3.2 Specifiche dei servizi del livello MAC

Il livello MAC si occupa di interfacciare il service specific convergence sublayer (SSCS) e il livello fisico (PHY). L'entità di gestione del livello MAC è denominata MLME (MAC sublayer management entity). Questa si occupa di supportare le funzioni che possono essere invocate e di gestire il database degli oggetti che è referenziato al MAC PIB (pan information base).

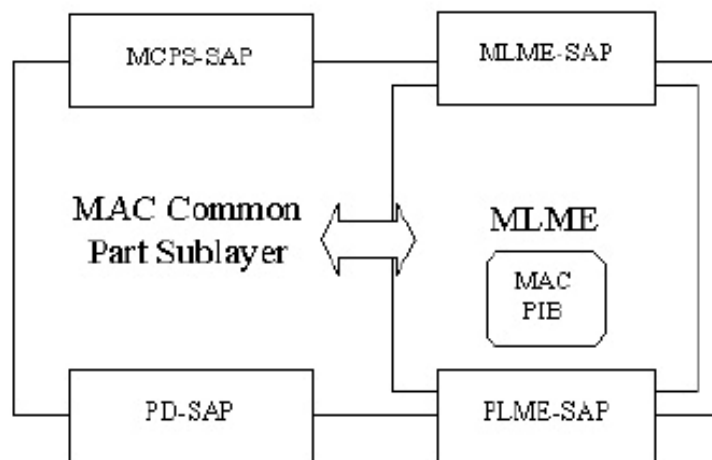


Figura 19 – MAC sublayer reference model

Il livello MAC fornisce due servizi, cui si accede tramite due service access point (SAP):

- MAC data service, tramite MCPS-SAP (MAC common part sublayer service access point);
- MAC management service, tramite MLME-SAP (MAC sublayer management entity service access point).

Questi due servizi si interfacciano esternamente a SSCS e PHY tramite PD-SAP e PLME-SAP (ovvero i service access point del livello fisico), e internamente fra loro, consentendo a MLME di usare il servizio MAC data service.

Come per il livello fisico, nel seguito esamineremo i vari servizi e i comandi supportati.

3.2.1 MAC Data Service

MCPS-SAP supporta il trasporto di SSCS protocol data unit (SPDU) fra differenti entità SSCS. I comandi supportati sono:

- MCPS-DATA.request richiede il trasferimento di un data SPDU (ad esempio un MSDU) da un singolo SSCS a un altro. Supporta parametri quali *SrcAddrMode* -modalità di indicazione dell'indirizzo, valori ammissibili no address, short o extended (valori fra 0x00 e 0x03), *SrcPANId* -indirizzo a 16 del PAN, indirizzo del device, indirizzo del destinatario (anche in questo caso abbiamo due parametri, uno per la modalità dell'indirizzo, uno per l'indirizzo), identificativo del PAN del ricevente, lunghezza MSDU, *msduHandle* un intero che funge da identificativo numerico, *TxOption* che indica la modalità di trasmissione, 0x01 ack transmission, 0x02 GTS transmission, 0x04 indirect transmission, 0x08 security enabled transmission.

E' generata da un'entità SSCS quando un data SPDU (i.e. MSDU) è trasmesso a una SSCS entity di un peer. Il suo effetto è l'inizio della trasmissione del MSDU.

- MCPS-DATA.confirm riporta il risultato della MCPS-DATA.request. Come parametri ha *msduHandle* che riporta il collegamento alla request e *status* il cui valore indica l'esito della trasmissione, *timestamp*

il cui valore viene utilizzato solo se l'esito della trasmissione ha avuto successo. E' generato in risposta a MCPS-DATA.request e come effetto notifica l'esito della trasmissione a SSCS.

- MCPS-DATA.indication indica il trasferimento di un data SPDU (i.e. MSDU) dal livello MAC alla locale entità SSCS. Supporta diversi attributi fra cui alcuni della request (come gli indirizzi), altri relativi alla link quality e alla sicurezza. E' generato dal livello MAC e spedito al SSCS al ricevimento di un data frame. Al suo ricevimento il SSCS sa che stanno arrivando dati al device.
- MCPS-PURGE.request (opzionale per RFD – dispositivi con funzioni ridotte) permette al livello superiore di eliminare un MSDU dalla lista di attesa delle transazioni. Supporta un parametro, *msduHandle*, ovvero l'identificativo del MSDU. E' generato dal livello superiore quando un MSDU deve essere eliminato dalla transaction queue. Al suo ricevimento il livello MAC controlla l'esistenza del MSDU indicato, se esiste invia una confirm con esito success.
- MCPS-PURGE.confirm (opzionali per RFD – dispositivi con funzioni ridotte) è la risposta alla MCPS-PURGE.request. Supporta due parametri *msduHandle* e *status* che indica il successo o meno dell'operazione.

La sequenza di messaggi necessari al trasferimento di dati fra due device è quella riportata nella figura seguente:

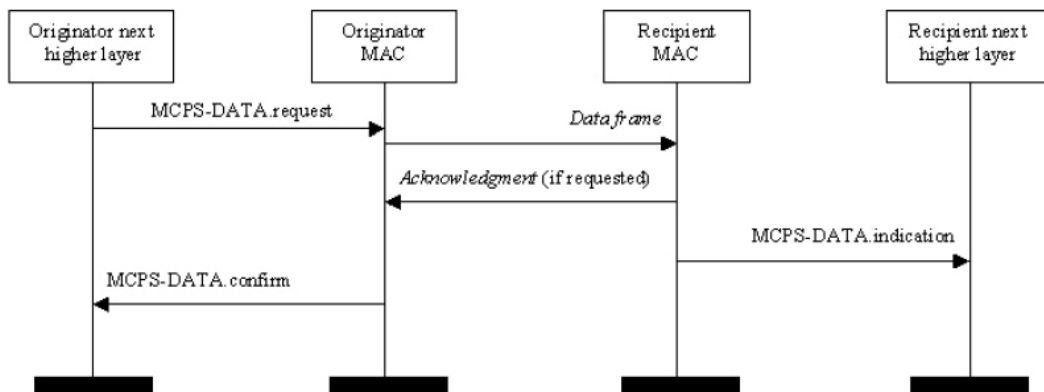


Figura 20 – MAC sublayer reference model

3.2.2 MAC Management Service

MLME-SAP permette il trasporto dei comandi fra il livello successivo dello stack e MLME. I comandi supportati sono:

- **MLME-ASSOCIATE** relativi a come un device si associa a una PAN.
 - MLME-ASSOCIATE.request richiede l'associazione a un coordinatore. È generata dal livello superiore e come effetto genera una associate.confirm
 - MLME-ASSOCIATE.indication (opzionale per RFD – dispositivi con funzioni limitate) è usato per indicare la ricezione di una MLME-ASSOCIATE.request, è generata da MLME e recapitata al livello superiore, il quale risponde con MLME-ASSOCIATE.response
 - MLME-ASSOCIATE.response (opzionale per RFD – dispositivi con funzioni limitate) è generata dal livello superiore e spedita a MLME in risposta a una MLME-ASSOCIATE.indication.
 - MLME-ASSOCIATE.confirm è usata per informare il livello superiore del successo o meno di una MLME-ASSOCIATE.request.

La sequenza dell'associazione di un device a una PAN è riassunta dallo schema seguente:

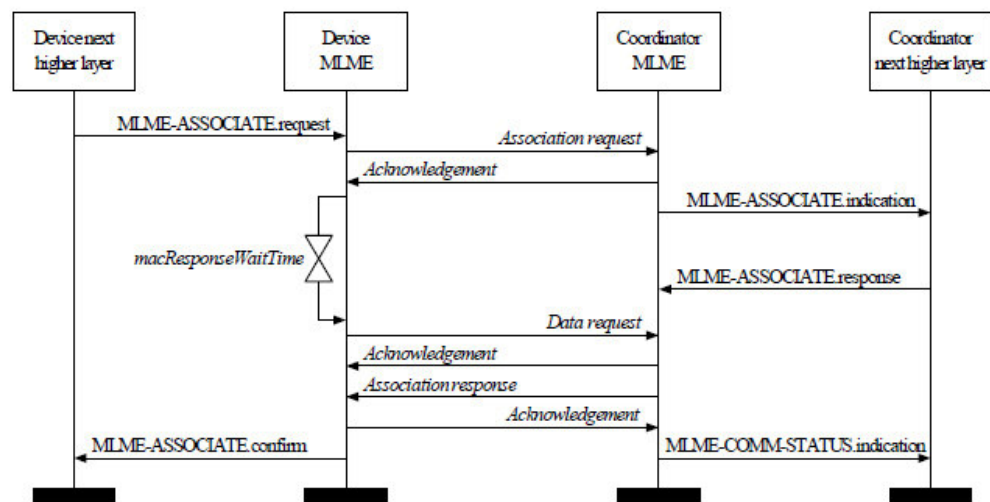


Figura 21 – Diagramma sequenza messaggi per ASSOCIATION

- **MLME-DISASSOCIATE** relativi a come un device può dissociarsi da una PAN.
 - *MLME-DISASSOCIATE.request* usata per notificare a un coordinatore la volontà di lasciare una PAN, è anche usata dai coordinatori per istruire i device su come lasciare la rete. Supporta come parametri l'indirizzo del device, la ragione per la dissociazione e un booleano che indica se la sicurezza è attivata o meno per questo trasferimento. E' generata dal livello superiore e inviata al MLME. Come effetto produce la *MLME-DISASSOCIATE.confirm*.
 - *MLME-DISASSOCIATE.indication* è utilizzata per indicare la ricezione di una richiesta di dissociazione. E' generata da MLME e recapitata al livello superiore. Ha l'effetto di notificare al livello superiore la ragione della disconnessione.
 - *MLME-DISASSOCIATE.confirm* riporta l'esito della *MLME-DISASSOCIATE.request*. Supporta il parametro *status* in cui viene appunto indicato l'esito della richiesta

La sequenza dell'associazione di un device a una PAN è riassunta dallo schema seguente:

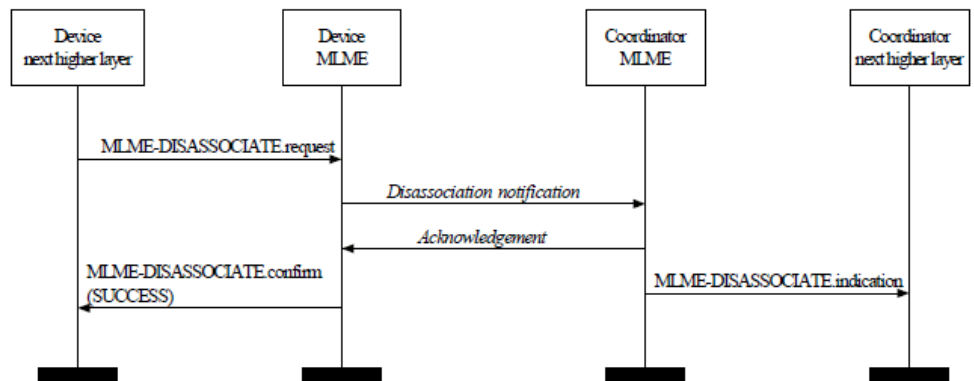


Figura 21 – Diagramma sequenza messaggi per DISASSOCIATION

- *MLME-BEACON-NOTIFY.indication* ricevuto per indicare i parametri di un beacon frame, generato da MLME e recapitato a livello superiore al ricevimento di un beacon frame quando *macAutorequest* è settato su *false* o contiene uno o più byte di payload. Il suo effetto è appunto informare il livello superiore dell'arrivo di un beacon.

▪ **Letture attributi PIB**

- MLME-GET.request richiede informazioni su un dato attributo PIB, come parametro supporta l'ID del PIB, è generato dal livello superiore e inviato a MLME. Come effetto genera MLME-GET.confirm.
- MLME-GET.confirm è la risposta alla request, supporta 3 parametri, id del PIB attributo richiesto, il suo valore e *status* che indica l'esito, SUCCESS nel caso in cui l'attributo esista, UNSUPPORTED_ATTRIBUTE altrimenti.

▪ **Gestione GTS** i comandi di questo gruppo definiscono come siano richiesti e gestiti i guaranteed time slots. I dispositivi che vogliono utilizzare questi comandi sono solitamente già tracciati dai beacon dei loro PAN coordinator.

- MLME-GTS.request (opzionale per RFD – dispositivi con funzioni limitate) inviata da un device che richiede a PAN coordinator di allocare o deallocare un GTS. Come parametri sono indicati le caratteristiche GTS e un booleano per indicare il modulo di sicurezza attivato oppure no. E' generata dal livello superiore e recapitata al MLME.
- MLME-GTS.indication (opzionale per RFD – dispositivi con funzioni limitate) indica che un GTS è stato allocato o deallocato.
- MLME-GTS.confirm (opzionale per RFD – dispositivi con funzioni limitate) ritorna il risultato della richiesta di allocare o deallocare un GTS, generata da MLME verso livello superiore.

La sequenza dei messaggi per la gestione di un GTS è riportata nella figura seguente.

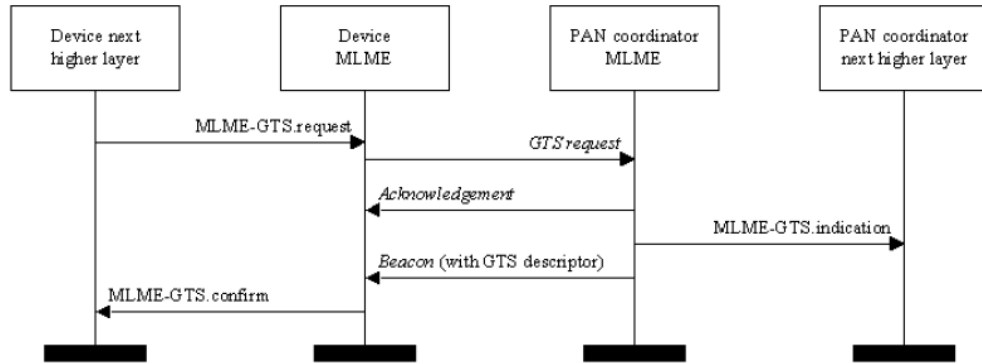


Figura 22 – Diagramma sequenza messaggi per GTS Allocation

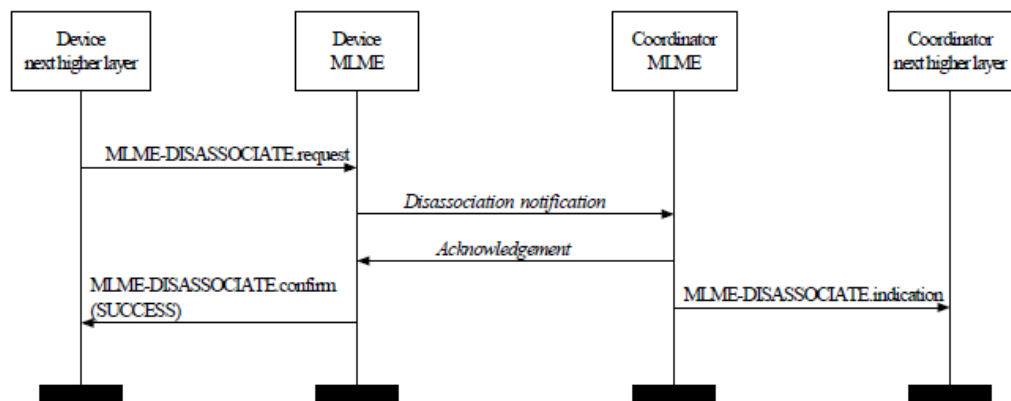


Figura 23 – Diagramma sequenza messaggi per GTS deallocation

- **ORPHAN NOTIFICATION** definiscono come un coordinatore può rilasciare una notifica su device orfani
 - *MLME-ORPHAN.indication* (opzionale per RFD – dispositivi con funzioni limitate) consente a MLME di un coordinatore di notificare al livello superiore la presenza di un orphaned device
 - *MLME-ORPHAN.response* (opzionale per RFD – dispositivi con funzioni limitate) è la risposta dal livello superiore a MLME in seguito a MLME-ORPHAN.indication

Il diagramma della sequenza dei messaggi **ORPHAN NOTIFICATION** è il seguente:

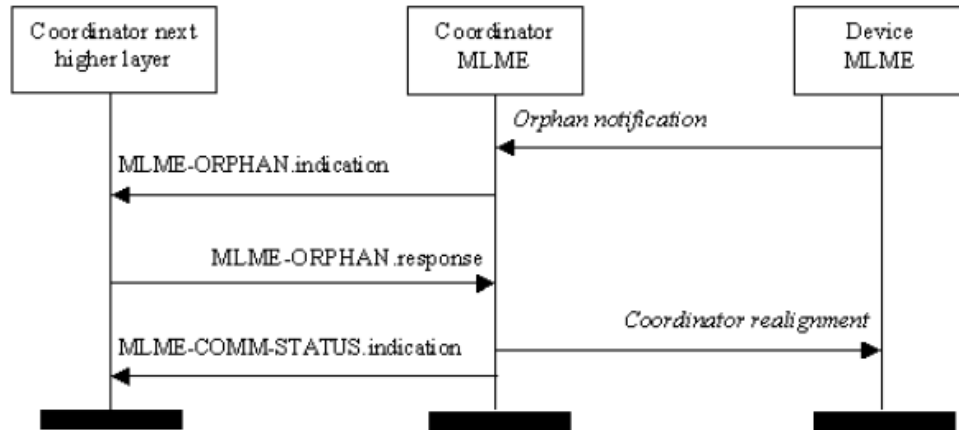


Figura 24 - Diagramma sequenza messaggi per MLME-ORPHAN

- **MLME-RESET** comandi per resettare il livello MAC e riportarlo ai valori predefiniti
 - *MLME-RESET.request* livello superiore richiede a MLME di resettare
 - *MLME-RESET.confirm* ritorna il risultato dell'operazione di reset tramite il parametro *status*.

- **MLME-RX-ENABLE** abilita o disabilita il ricevente a un dato tempo
 - *MLME-RX-ENABLE.request* permette al livello superiore di richiedere che il ricevente sia abilitato per un periodo finito di tempo.
 - *MLME-RX-ENABLE.confirm* ritorna il risultato della richiesta di abilitazione del receiver per un dato tempo nel parametro *status*.

La sequenza dei messaggi per l'abilitazione del ricevente è la seguente:

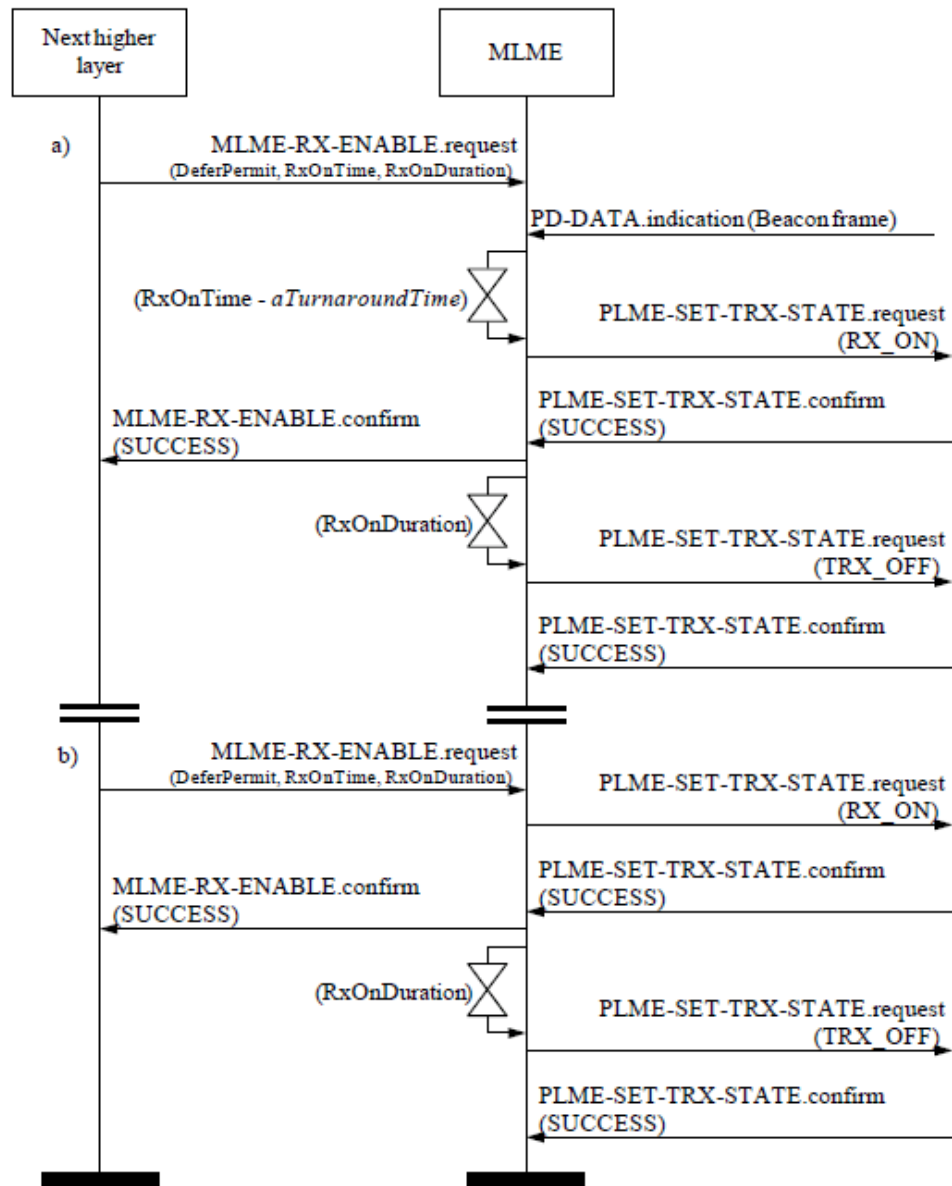


Figura 25 – Diagramma sequenza messaggi per MLME-RX-ENABLE

- **MLME-SCAN:** questi comandi determinano come un device possa determinare il consumo energetico o la presenza o l'assenza di PANs in un canale di comunicazione.
 - *MLME-SCAN.request* è usata per iniziare una scansione di un canale su una lista di canali. Un device può usare channel scan per

misurare l'energia sul canale, cercare un coordinator cui associarsi o cercare tutti i coordinator che stanno trasmettendo beacon nello spazio operativo. E' generata dal livello superiore.

- MLME-SCAN.confirm è la risposta a MLME-SCAN.request.
- **MLME-COMM-STATUS.indication** permette a MLME di indicare lo stato di comunicazione. E' generata da MLME e indirizzata a livello superiore.
- **MLME-SET:** comandi per definire come gli attributi MAC PIB possono essere scritti.
 - MLME-SET.request tenta di scrivere il valore dato nell'attributo PIB indicato. Generata dal livello superiore verso MLME. Come effetto produce MLME-SET.confirm.
 - MLME-SET.confirm riporta il risultato della MLME-SET.request tramite i parametri *status* e *PIBAtribute*.
- **Aggiornamento configurazione superframe:** definiscono come un FFD può chiedere al device di iniziare ad utilizzare una nuova configurazione del superframe per inizializzare una PAN, iniziare a trasmettere beacon, o in una PAN esistente facilitare la scoperta di nuovi dispositivi o stoppare la trasmissione di beacon.
 - MLME-START.request (opzionale per RFD - dispositivi con funzioni limitate) è una richiesta al device di iniziare ad utilizzare una nuova configurazione del superframe. E' generata dal livello superiore.
 - MLME-START.confirm (opzionale per RFD - dispositivi con funzioni limitate) è la risposta a una MLME-START.confirm. L'esito della richiesta è riportato nel parametro *status*.

Il diagramma della sequenza dei messaggi necessari a modificare la struttura di un super frame è la seguente:

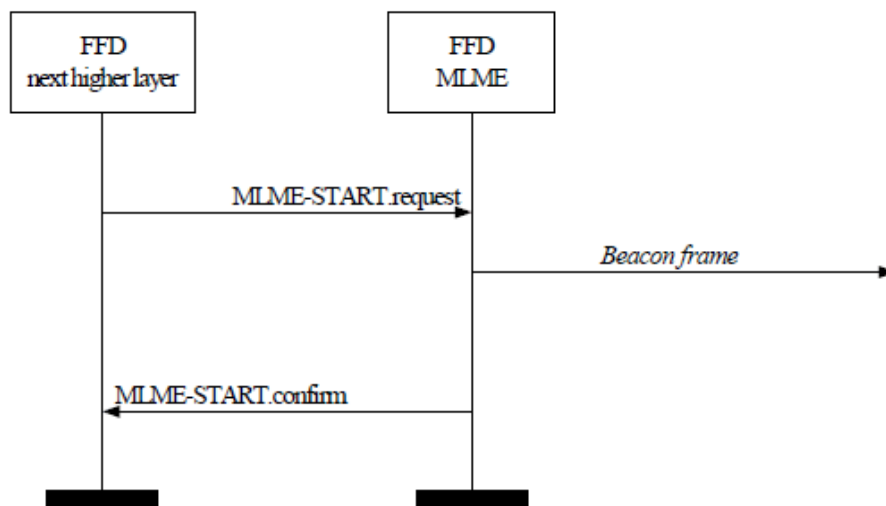


Figura 26 – Diagramma sequenza messaggi per MLME-START

- **Sincronizzazione ad un coordinatore:** i comandi seguenti definiscono come può essere ottenuta la sincronizzazione con un coordinatore e come la perdita di sincronizzazione è comunicata al livello superiore.
 - MLME-SYNC.request è una richiesta di sincronizzazione e se specificato tracciata tramite beacon. E' generata dal livello superiore di un device in una PAN con beacon abilitati.
 - MLME-SYNC-LOSS.indication è generata per indicare l'impossibilità di trovare beacon durante la ricerca ed indica la perdita di sincronizzazione ad un coordinator.

La sequenza dei messaggi relativi alla sincronizzazione ad un coordinatore è la seguente:

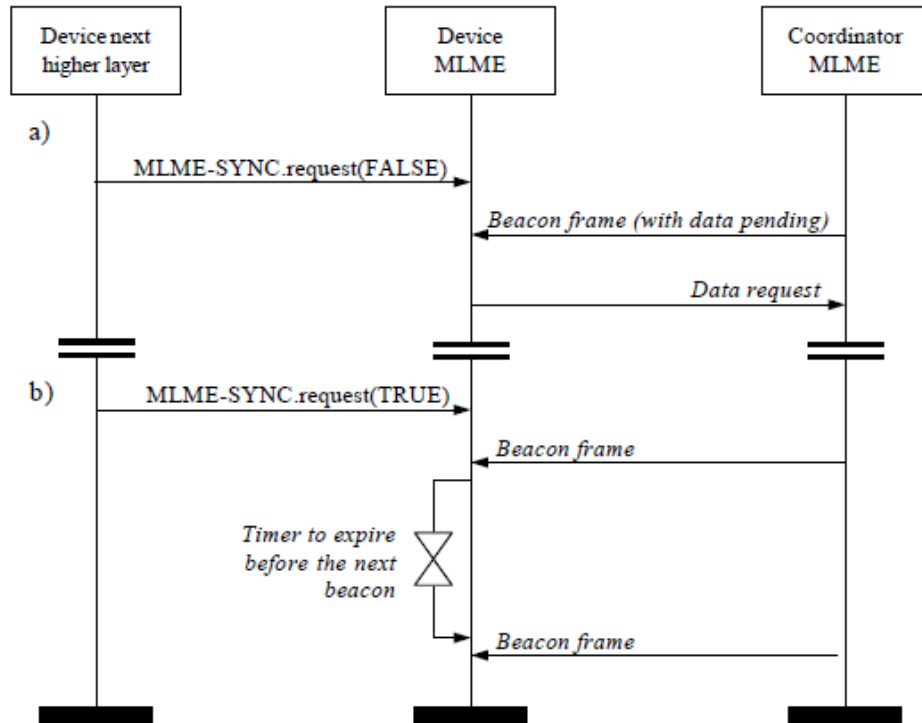


Figura 27 – Diagramma sequenza messaggi per MLME-SYNC

- **Richiedere dati a un coordinatore**
 - MLME-POLL.request incita il device a richiedere dati al coordinatore, è generata dal livello superiore quando devono essere richiesti dei dati a un coordinatore.
 - MLME-POLL.confirm ritorna il risultato di `MLME-POLL.request` tramite il parametro `status`. Informa il livello superiore della procedura per chiedere dati al coordinatore.

La sequenza dei messaggi per richiedere dati da un coordinatore è la seguente:

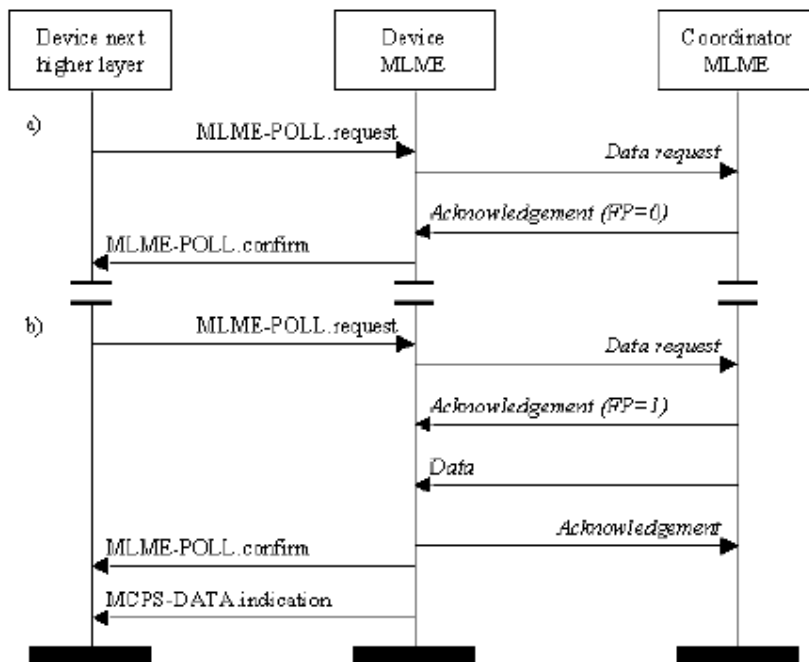


Figura 28 - Diagramma sequenza messaggi per richiedere dati da un coordinatore

3.2.3 MAC Enumeration Description

Molti parametri dei comandi MAC sono di tipo *enumeration* e ammettono un range di valori compresi fra 0x00 e 0xff. Molti di questi sono riservati ad usi futuri, altri hanno significati particolari. Li vediamo riportati nella tabella seguente.

Enumeration	Value	Description
SUCCESS	0x00	The requested operation was completed successfully. For a transmission request, this value indicates a successful transmission.
—	0x01–0xda	Reserved for MAC command status and reason code values.
—	0x80–0xda, 0xfe–0xff	Reserved.
BEACON_LOSS	0xe0	The beacon was lost following a synchronization request.
CHANNEL_ACCESS_FAILURE	0xe1	A transmission could not take place due to activity on the channel, i.e., the CSMA-CA mechanism has failed.
COUNTER_ERROR	0xdb	The frame counter purportedly applied by the originator of the received frame is invalid.
DENIED	0xe2	The GTS request has been denied by the PAN coordinator.
DISABLE_TRX_FAILURE	0xe3	The attempt to disable the transceiver has failed.
FRAME_TOO_LONG	0xe5	Either a frame resulting from processing has a length that is greater than <i>aMaxPHYPacketSize</i> or a requested transaction is too large to fit in the CAP or GTS.

Enumeration	Value	Description
IMPROPER_KEY_TYPE	0xdc	The key purportedly applied by the originator of the received frame is not allowed to be used with that frame type according to the key usage policy of the recipient.
IMPROPER_SECURITY_LEVEL	0xdd	The security level purportedly applied by the originator of the received frame does not meet the minimum security level required/expected by the recipient for that frame type.
INVALID_ADDRESS	0xf5	A request to send data was unsuccessful because neither the source address parameters nor the destination address parameters were present.
INVALID_GTS	0xe6	The requested GTS transmission failed because the specified GTS either did not have a transmit GTS direction or was not defined.
INVALID_HANDLE	0xe7	A request to purge an MSDU from the transaction queue was made using an MSDU handle that was not found in the transaction table.
INVALID_INDEX	0xf9	An attempt to write to a MAC PIB attribute that is in a table failed because the specified table index was out of range.
INVALID_PARAMETER	0xe8	A parameter in the primitive is either not supported or is out of the valid range.
LIMIT_REACHED	0xfa	A scan operation terminated prematurely because the number of PAN descriptors stored reached an implementation-specified maximum.
NO_ACK	0xe9	No acknowledgment was received after <i>macMaxFrameRetries</i> .
NO_BEACON	0xea	A scan operation failed to find any network beacons.
NO_DATA	0xeb	No response data were available following a request.
NO_SHORT_ADDRESS	0xec	The operation failed because a 16-bit short address was not allocated.

ON_TIME_TOO_LONG	0xf6	A receiver enable request was unsuccessful because it specified a number of symbols that was longer than the beacon interval.
OUT_OF_CAP	0xed	A receiver enable request was unsuccessful because it could not be completed within the CAP. The enumeration description is not used in this standard, and it is included only to meet the backwards compatibility requirements for IEEE Std 802.15.4-2003.
PAN_ID_CONFLICT	0xee	A PAN identifier conflict has been detected and communicated to the PAN coordinator.
PAST_TIME	0xf7	A receiver enable request was unsuccessful because it could not be completed within the current superframe and was not permitted to be deferred until the next superframe.
READ_ONLY	0xfb	A SET/GET request was issued with the identifier of an attribute that is read only.
REALIGNMENT	0xef	A coordinator realignment command has been received.

Enumeration	Value	Description
SCAN_IN_PROGRESS	0xfc	A request to perform a scan operation failed because the MLME was in the process of performing a previously initiated scan operation.
SECURITY_ERROR	0xe4	Cryptographic processing of the received secured frame failed.
SUPERFRAME_OVERLAP	0xfd	The device was instructed to start sending beacons based on the timing of the beacon transmissions of its coordinator, but the instructed start time overlapped the transmission time of the beacon of its coordinator.
TRACKING_OFF	0xf8	The device was instructed to start sending beacons based on the timing of the beacon transmissions of its coordinator, but the device is not currently tracking the beacon of its coordinator.
TRANSACTION_EXPIRED	0xf0	The transaction has expired and its information was discarded.
TRANSACTION_OVERFLOW	0xf1	There is no capacity to store the transaction.
TX_ACTIVE	0xf2	The transceiver was in the transmitter enabled state when the receiver was requested to be enabled. The enumeration description is not used in this standard, and it is included only to meet the backwards compatibility requirements for IEEE Std 802.15.4-2003.
UNAVAILABLE_KEY	0xf3	The key purportedly used by the originator of the received frame is not available or, if available, the originating device is not known or is blacklisted with that particular key.
UNSUPPORTED_ATTRIBUTE	0xf4	A SET/GET request was issued with the identifier of a PIB attribute that is not supported.
UNSUPPORTED_LEGACY	0xde	The received frame was purportedly secured using security based on IEEE Std 802.15.4-2003, and such security is not supported by this standard.
UNSUPPORTED_SECURITY	0xdf	The security purportedly applied by the originator of the received frame is not supported.

Tabella 10 – MAC enumeration description

3.3 MAC Frame Formats

Ogni MAC frame (MPDU) è composto da:

- MHR – header composto da frame control, sequence number, address information
- MAC payload – contiene il carico dati, varia a seconda del tipo di frame ed è di lunghezza variabile. Gli ACK ad esempio non hanno payload.
- MFR – footer, contiene FCS

Di seguito sono rappresentati nell'ordine in cui sono spediti al livello fisico, da sinistra verso destra.

3.3.1 Formato generale

Octets: 2	1	0/2	0/2/8	0/2	0/2/8	0/5/6/10/ 14	variable	2
Frame Control	Sequence Number	Destination PAN Identifier	Destination Address	Source PAN Identifier	Source Address	Auxiliary Security Header	Frame Payload	FCS
		Addressing fields						
MHR							MAC Payload	MFR

Figura 29 – General MAC Format

3.3.1.1 **Frame control**

E' composto da 16 bit e contiene informazioni sul tipo di frame, campi indirizzo e altri flag di controllo illustrati in dettaglio nella figura seguente.

Bits: 0-2	3	4	5	6	7-9	10-11	12-13	14-15
Frame Type	Security Enabled	Frame Pending	Ack. Request	PAN ID Compression	Reserved	Dest. Addressing Mode	Frame Version	Source Addressing Mode

Figura 30 – Frame control field

Frame Type: 3 bit che indicano il tipo di frame. 000: beacon, 001: Data, 010: ACK, 011 MAC command, 100-111 riservati.

Security enabled: 1 bit. Se posto a 0 indica che il frame non è crittografato, se posto a 1 indica che il frame è protetto usando le chiavi memorizzate nel MAC PIB. Le operazioni di crittografia dipendono dalla security suite selezionata per la relazione, se non è stata definita, questo campo è posto a 0.

Frame Pending: 1 bit. È posto a 1 se oltre al carico dati corrente il frame ha altri dati addizionali da spedire, in caso contrario è 0.

Questo campo può essere usato solo nei frame trasmessi durante la contention access period (CAP) da device operanti in PAN con beacon abilitati, oppure sempre in PAN con beacon disabilitati.

Acknowledgment request: 1 bit, posto ad 1 se è richiesto un ack al ricevimento del frame.

Intra PAN: 1 bit. Specifica se il frame è spedito all'interno della stessa PAN o ad una PAN esterna. Se è posto ad 1 e sia l'indirizzo di destinazione sia l'indirizzo sorgente sono presenti il frame non deve contenere il PAN id. Se posto a 0 e sia l'indirizzo di destinazione sia l'indirizzo sorgente sono presenti, il frame deve contenere entrambi i PAN id.

Destination addressing mode: 2 bit che indicano la tipologia degli indirizzi. 00: PAN id e indirizzi non presenti, 01 riservato, 10 indirizzo breve a 16 bit, 11 indirizzo esteso a 64 bit.

Source addressing mode: 2 bit che indicano la tipologia degli indirizzi. 00: PAN id e indirizzi non presenti, 01 riservato, 10 indirizzo breve a 16 bit, 11 indirizzo esteso a 64 bit.

3.3.1.2 Sequence number

8 bit che formano un identificativo univoco per il frame.

3.3.1.3 Destination PAN identifier

16 bit che rappresentano l'id della PAN del destinatario.

3.3.1.4 Destination Address

16 o 64 bit che rappresentano l'indirizzo del destinatario.

3.3.1.5 Source PAN identifier

16 bit che rappresentano l'id della PAN del mittente.

3.3.1.6 Source Address

16 o 64 bit che rappresentano l'indirizzo del mittente.

3.3.1.7 Frame Payload

Il carico dati. Se security enabled è settata a 1 i dati sono protetti dalla security suite selezionata.

3.3.1.8 FCS (frame check sequence)

Sequenza di controllo di 16 bit calcolata su MHR e MAC payload.

Questa era la descrizione del formato di un frame MAC in generale, alcuni campi variano a seconda del tipo di frame. Possiamo distinguere fra *beacon frame*, *acknowledgement*, *data and MAC command*. Di seguito saranno mostrate le strutture di ognuno di essi.

3.3.2 *Beacon Frame Format*

Octets: 2	1	4/10	0/5/6/10/14	2	variable	variable	variable	2
Frame Control	Sequence Number	Addressing fields	Auxiliary Security Header	Superframe Specification	GTS fields (Figure 45)	Pending address fields (Figure 46)	Beacon Payload	FCS
MHR				MAC Payload				MFR

Figura 31 – Beacon Frame format

3.3.3 *Data frame*

Octets: 2	1	(see 7.2.2.2.1)	0/5/6/10/14	variable	2
Frame Control	Sequence Number	Addressing fields	Auxiliary Security Header	Data Payload	FCS
MHR				MAC Payload	MFR

Figura 32 – Data Frame format

3.3.4 *Acknowledgment frame*

Octets: 2	1	2
Frame Control	Sequence Number	FCS
MHR		MFR

Figura 33 – Acknowledgment frame format

3.3.5 *MAC command frame*

Octets: 2	1	(see 7.2.2.4.1)	0/5/6/10/14	1	variable	2
Frame Control	Sequence Number	Addressing fields	Auxiliary Security Header	Command Frame Identifier	Command Payload	FCS
MHR				MAC Payload		MFR

Figura 34 – MAC command frame format

Fa parte del carico dati il command frame identifier. Questo campo comprende un range di valori che saranno analizzati al paragrafo seguente, nel quale parleremo nel dettaglio di questa tipologia di frame.

3.4 *MAC Command Frames*

Abbiamo diversi tipi di command frame, un FFD deve supportarli tutti, mentre gli RFD devono essere in grado di trasmettere o ricevere solo alcuni di essi. Nella tabella seguente TX indica trasmissione e RX ricezione. Le due colonne servono proprio a mostrare visivamente quali comandi e in quale modalità gli RFD debbano supportare.

I comandi MAC devono essere trasmessi solo durante il contention access period in PAN con beacon abilitati. Al contrario nelle reti con beacon disabilitati possono essere trasmessi in ogni momento.

Command frame identifier	Command name	RFD	
		Tx	Rx
0x01	Association request	X	
0x02	Association response		X
0x03	Disassociation notification	X	X
0x04	Data request	X	
0x05	PAN ID conflict notification	X	
0x06	Orphan notification	X	
0x07	Beacon request		
0x08	Coordinator realignment		X
0x09	GTS request		
0x0a–0xff	Reserved		

Tabella 11 – MAC Command frame

Association request permette a un device di richiedere una richiesta di associazione a un coordinatore. I dispositivi possono richiedere l'associazione solo a PAN che lo permettono, in seguito alla procedura di scan, e può essere inviata solo da device attualmente non associati a nessuna rete. Tutti i tipi di dispositivo, sia RFD che FFD devono essere in grado di trasmettere questo comando, sebbene gli RFD non siano tenuti a supportare anche la ricezione di association request.

Association response permette a un coordinatore di rispondere a una *association request*. Deve essere spedito solo dai coordinatori a device che stanno cercando di collegarsi alla rete. Tutti i tipi di dispositivo devono essere in grado di ricevere questo comando, ma gli RFD non sono tenuti a supportare la sua trasmissione.

Disassociation notification può essere spedita sia dal coordinatore sia da un device associato alla rete e deve essere implementata da tutti i tipi di dispositivo.

Data request è spedita da un device a un coordinatore per richiedere dati. Tutti i dispositivi devono essere in grado di spedirla ma agli RFD non è richiesto di essere capaci di riceverla.

Orphan notification è usata da un dispositivo connesso a una PAN che abbia perso la sincronizzazione al suo coordinatore. Tutti i device devono essere in grado di spedirla ma è richiesto solo ai FFD di essere abili a riceverla.

Beacon request è usata da un device per localizzare tutti i coordinatori disponibili nell'area di copertura durante un'operazione di scan. E' opzionale per gli RFD.

Coordinator realignment è spedito da un coordinatore sia in seguito al ricevimento di un comando *Orphan notification* da un device che ha perso la sincronizzazione, sia nel momento in cui qualche parametro di configurazione della PAN viene modificato. Nel primo caso questo comando viene spedito solo al device che ha notificato la perdita di sincronizzazione, nel secondo viene spedito in broadcast a tutti i device sulla rete. Tutti i device devono essere in grado di ricevere questo comando ma gli RFD non sono tenuti a supportare il suo invio.

GTS allocation - deallocation (GTS request command) è usata da un dispositivo quando vuole richiedere l'allocazione di un nuovo GTS o la deallocazione di un GTS esistente. E' opzionale per gli RFD.

3.5 Descrizione funzionalità del livello MAC

Di seguito saranno analizzate nel dettaglio le varie funzioni del livello MAC: la gestione dell'accesso al canale, come inizializzare e gestire una

PAN, come associarsi o dissociarsi a una PAN, la sincronizzazione, la trasmissione, ricezione etc dei frame, allocazione e deallocazione di guaranteed time slots e la sicurezza dei frame.

3.5.1 *Channel Access*

Il livello MAC permette due differenti modalità di accesso al canale: contention free e contention based. L'accesso contention-based permette ai dispositivi di accedere al canale in modo distribuito utilizzando l'algoritmo CSMA-CA backoff. L'accesso contention-free invece è interamente controllato dal PAN coordinator tramite l'utilizzo di GTS.

3.5.1.1 *Superframe*

Un coordinatore può definire i tempi del canale tramite la superframe structure. Il superframe è definito dall'invio di un beacon frame e può avere porzioni attive e inattive. Il coordinatore può poi interagire con la rete solo durante il periodo attivo, consentendo così un risparmio energetico durante la porzione inattiva entrando in sleep mode.

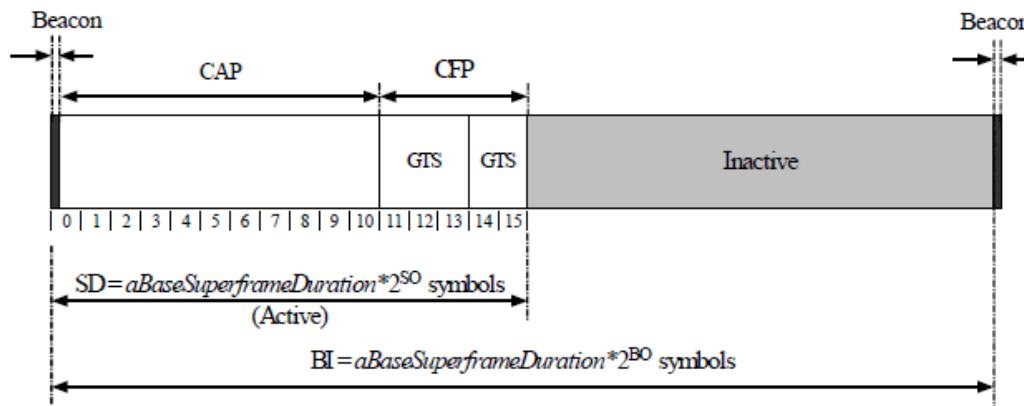


Figura 35 - Esempio di struttura superframe

La porzione attiva del superframe è divisa in tre parti: beacon, CAP (contention access period) e CFP (contention free period). Il beacon è spedito senza l'utilizzo di CSMA all'inizio dello slot 0 e il CAP solitamente viene subito dopo. Il CFP può non essere presente, in caso ci sia viene subito dopo il CAP. Se esistono GTS sono collocati durante il CFP.

L'attivazione e l'utilizzo del superframe sono dettati da due attributi, *macSuperFrameOrder* e *macBeaconOrder*. La struttura del superframe è utilizzata se il valore di *macBeaconOrder* è compreso fra 0 e 14 e

macSuperFrameOrder è compreso fra 0 e il valore di *macBeaconOrder*. Se *macSuperFrameOrder* è pari a 15 il superframe non viene utilizzato al termine della trasmissione del beacon. In caso di PAN con beacon disabilitati per non utilizzare il superframe entrambi i valori devono essere posti uguali 15.

Il **CAP** inizia subito dopo il trasferimento del beacon e deve terminare prima dell'inizio del CFP, in caso questo fosse settato a zero, allora deve terminare entro la fine del superframe. Tutti i frame ad esclusione degli acknowledgment frame, o frame che si comportino come tali, sono trasmessi utilizzando il slotted CSMA-CA per l'accesso al canale. Un device che trasmette durante il CAP deve assicurare che la transazione sia completata (ricezione di ack inclusi) in un IFS period (interframe space). Se non è possibile terminare la trasmissione entro il termine del CAP, allora il dispositivo deve rinviare l'invio al CAP del superframe successivo. Tutti i comandi MAC sono trasferiti durante il CAP.

Il **CFP** parte al termine del CAP e deve terminare entro l'invio del beacon successivo. Se il coordinatore ha allocato GTS, devono essere posti in slot contigui entro il termine del periodo. Nessuna trasmissione durante il CFP è eseguita utilizzando CSMA-CA. Ogni device che vuole trasmettere in questo periodo deve assicurarsi di terminare la trasmissione in un IFS ed entro il termine del proprio GTS.

3.5.1.2 IFS

Il livello MAC ha bisogno di un tempo determinato per processare i dati ricevuti dal livello fisico, e, per permettere questo, i frame trasmessi devono essere seguiti da un IFS. Se è previsto un ack, allora l'IFS seguirà l'ack. La lunghezza dell'IFS dipende direttamente dalla lunghezza del frame trasmesso. Alcuni di questi meccanismi sono illustrati nella figura seguente.

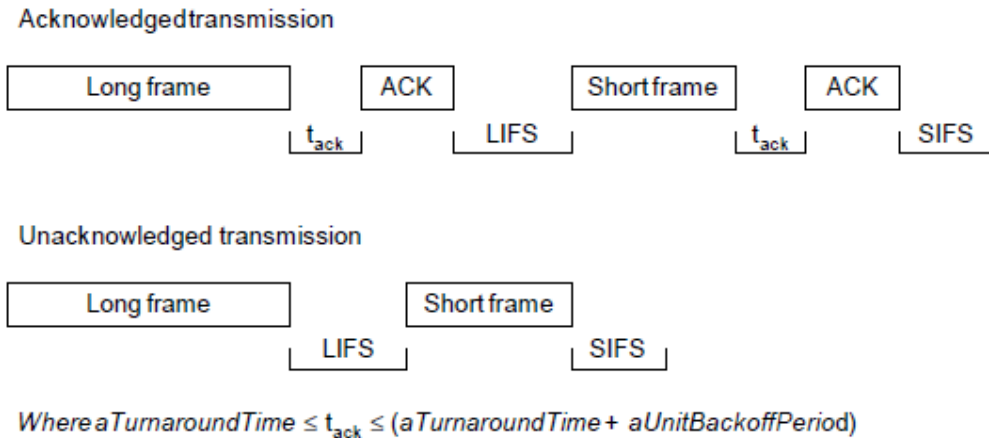


Figura 36 - IFS

3.5.1.3 CSMA-CA

Questo meccanismo di accesso è utilizzato per la trasmissione di tutti i data frame e comandi MAC durante il CAP. Fanno eccezione gli ack e i frame che possono essere trasmessi facilmente allo stesso modo, e tutti i frame trasmessi nel CFP.

Se siamo in una PAN che fa utilizzo di beacon, viene utilizzata la versione Slotted CSMA-CA, in caso contrario se i beacon sono disabilitati o non possono essere localizzati è usata la versione unslotted CSMA. In entrambi i casi le unità di tempo sono chiamate *backoff*.

I limiti dei periodi di backoff di ogni dispositivo devono essere allineati con i limiti del superframe slot del coordinatore, ovvero l'inizio del primo periodo di backoff di ogni dispositivo deve essere allineato all'inizio della trasmissione del beacon. Il livello MAC deve assicurare che il livello fisico inizi tutte le sue trasmissioni nei limiti del backoff se stiamo utilizzando slotted CSMA-CA, al contrario, in unslotted CSMA-CA i periodi di backoff di un dispositivo non sono collegati a quelli degli altri dispositivi nella PAN.

Ogni device deve tenere in memoria 3 variabili per ogni tentativo di trasmissione: *NB*, *CW* e *BE*. *NB* è un numero che indica quante volte è stato richiesto a CSMA-CA di fermarsi e non proseguire la trasmissione (backoff). Questo valore è inizializzato e resettato a 0 ad ogni nuovo tentativo di trasmissione. *CW* è la dimensione della finestra di contenzione (window

contention length), ed indica il numero di periodi di backoff durante i quali il canale va lasciato libero da ogni tentativo di trasmissione. Questo valore è inizializzato a 2 prima di ogni tentativo di trasmissione e resettato a 2 ogni volta che il canale viene trovato occupato. Unslotted CSMA-CA non fa uso della variabile CW. BE rappresenta l'esponente di backoff ed indica per quanti slot un device deve attendere prima di tentare l'accesso al canale.

Sebbene il receiver del dispositivo sia attivo durante la fase di valutazione e accertamento dello stato del canale, ogni frame ricevuto durante questo periodo viene scartato.

L'immagine seguente mostra in un diagramma e commenta i vari step di CSMA-CA.

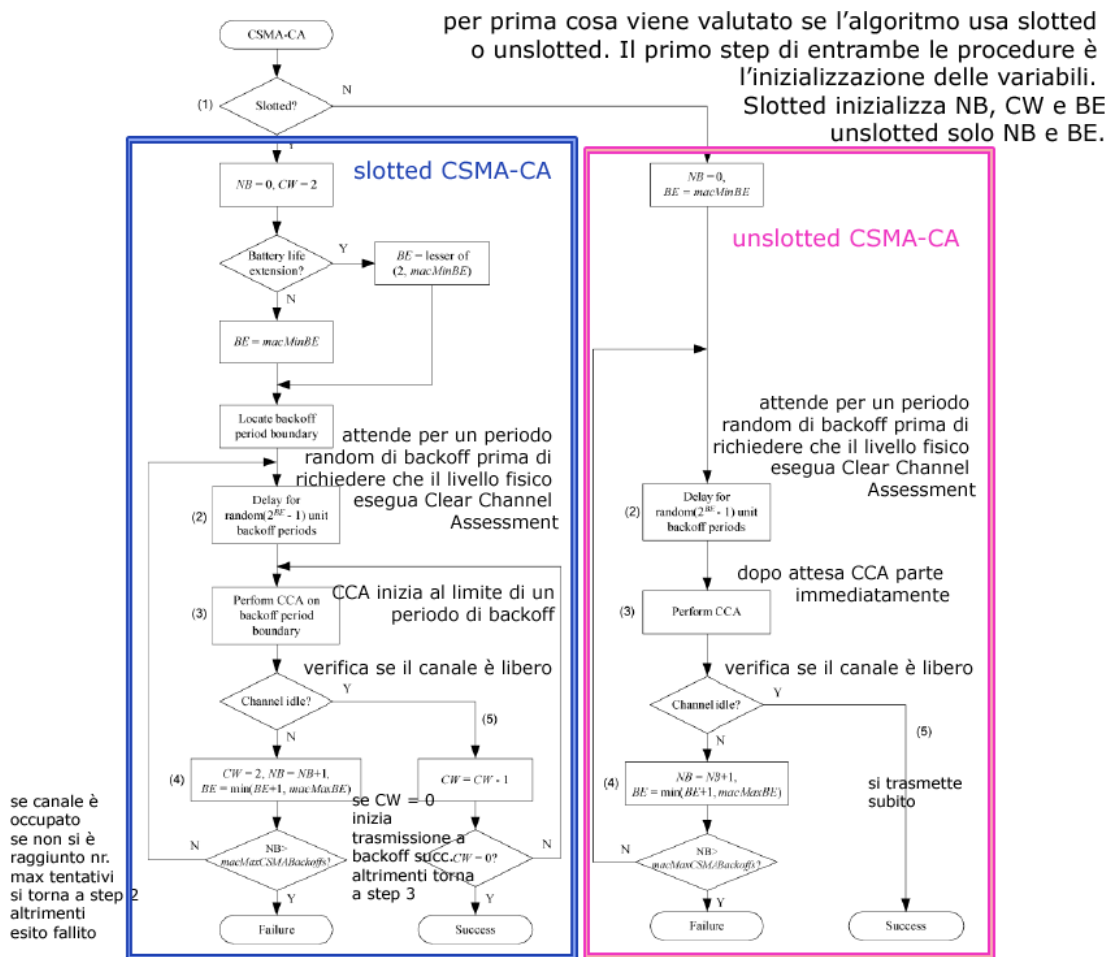


Figura 37 – CSMA-CA

Se siamo in slotted CSMA-CA e il campo battery life extension (BLE) è impostato a 0, il livello MAC deve garantire che dopo il periodo di attesa, pari a un numero random di backoff, le rimanenti transazioni di CSMA-CA

possano essere compiute e la trasmissione possa essere completata prima del termine del CAP. Se il numero random di backoff di attesa è maggiore rispetto al numero di backoff rimanenti nel corrente CAP, il livello MAC può mettere in pausa il contatore dei backoff e ripristinarlo all'inizio del CAP nel superframe successivo. Se il numero di backoff di attesa è invece minore o uguale al numero di backoff rimanenti, applicherà l'attesa random e dopo essa valuterà come procedere, infatti, potrà trasmettere solo se riuscirà a completare l'operazione (incluso ack) prima del termine del CAP. Se tutte le valutazioni hanno esito positivo, allora richiederà al livello fisico di procedere e tentare di eseguire CCA. Se l'esito delle verifiche è negativo, resterà in attesa fino al CAP del prossimo superframe per poi procedere a nuove valutazioni.

Se siamo in slotted CSMA-CA e il campo BLE è settato a 1, il livello MAC deve garantire che dopo il periodo di attesa, pari a un numero random di backoff, le rimanenti transazioni di CSMA-CA possano essere compiute e la trasmissione possa essere completata prima del termine del CAP. Il countdown backoff avviene solo al termine dell'IFS successivo al beacon, durante *macBattLifeExtPeriods*. Il livello MAC può procedere se gli step rimanenti (le due analisi CCA), la trasmissione del frame e la ricezione di ACK possono essere completati prima del termine del CAP e se la trasmissione inizierà in uno dei primi *macBattLifeExtPeriods* full backoff periods successivi all'IFS che segue il beacon. Se il livello MAC può procedere allora richiede al livello fisico di eseguire CCA nel superframe attuale. In caso contrario attenderà l'inizio del CAP nel superframe successivo e attenderà un periodo random di backoff prima di valutare se può procedere.

Se il canale è occupato, le variabili NB e BE vengono incrementate di 1, e, in slotted CSMA-CA, CW viene resettata a 2. Se NB è minore o uguale al valore massimo di tentativi possibili (*macMaxCSMABackoff*), si riparte dal secondo step, in caso contrario l'algoritmo è terminato con esito negativo (Channel access failure status).

Se il canale è libero, il livello MAC in caso di slotted CSMA-CA deve assicurarsi che la finestra di contenzione sia terminata prima di iniziare la trasmissione. Per farlo la variabile CW viene decrementata di uno, se dopo quest'operazione è uguale a 0 inizia la trasmissione all'inizio del backoff successivo, in caso contrario si torna allo step nr. 3. Al contrario, in caso di unslotted CSMA-CA, se il canale è rilevato libero inizia la trasmissione immediatamente.

3.5.2 Inizializzare e gestire una PAN

3.5.2.1 Scansione dei canali

I device che vogliono collegarsi a una PAN iniziano scansionando il canale (o i canali) cercando beacon all'interno del loro spazio operativo, oppure cercandone uno specifico se hanno perso la sincronizzazione. Esistono quattro tipi di scansione: ED channel scan, active channel scan, passive channel scan e orphan channel scan.

La prima consente a un FFD di misurare i livelli energetici in ogni canale richiesto, al fine di valutare su quale canale operare prima di inizializzare una nuova PAN. Durante una ED scan tutti i frame ricevuti sul PHY data service vengono scartati.

L'active scan channel permette a un FFD di localizzare ogni coordinatore che sta trasmettendo beacon all'interno del suo spazio operativo. Ciò può essere utile al fine di selezionare un PAN ID prima di inizializzare una nuova PAN. Durante la scansione dei canali attivi il livello MAC scarta tutti i frame ricevuti sul livello fisico che non siano beacon.

La passive channel scan permette come l'active scan di localizzare tutti i coordinatori che stanno trasmettendo beacon, ma la beacon request command non viene spedita. Questo tipo di scansione solitamente viene utilizzato prima di associarsi a una PAN. Durante la scansione dei canali attivi il livello MAC scarta tutti i frame ricevuti sul livello fisico che non siano beacon.

L'orphan channel scan permette a un device di rilocalizzare il coordinatore al quale hanno perso la sincronizzazione. Come negli altri casi, il livello MAC scarta tutti i frame ricevuti che non siano beacon. La

scansione termina quando il device riceve il comando di riallineamento dal coordinatore, oppure quando tutti i canali logici sono stati scansionati.

3.5.2.2 Risoluzione dei conflitti di PAN ID

Nel caso in cui si voglia dar luogo a una nuova PAN la scansione dei canali è effettuata al fine di trovare e selezionare un canale e un PAN ID non utilizzato e appropriato. E' tuttavia possibile che all'interno di uno spazio operativo due PAN si sovrappongano con lo stesso identificativo e per questo esiste un'apposita procedura di risoluzione e detenzione del conflitto. Questa procedura è opzionale per i RFD. Quando un conflitto viene identificato, per prima cosa il coordinatore effettua una scansione dei canali e sulla base delle informazioni ricevute seleziona un nuovo PAN identifier. In seguito alla selezione dell'identificativo può spedire un comando di riallineamento in broadcast, indicando il nuovo id della rete e una volta spedito il riallineamento può procedere alla modifica del PAN id.

3.5.2.3 Inizializzare una PAN

Dopo la scansione e la selezione di un canale e di un identifier un FFD può iniziare a operare come PAN coordinator.

3.5.2.4 Generazione Beacon

Tutti i beacon sono trasmessi all'inizio di ogni superframe e la loro trasmissione è prioritaria rispetto all'invio o ricezione di altre operazioni.

3.5.2.5 Device Discovery

Tramite la trasmissione di beacon un FFD comunica ad altri dispositivi l'esistenza di una PAN. Se il FFD non è il coordinatore, può trasmettere beacon solo se si è completamente associato alla PAN.

3.5.3 Associazione e dissociazione

Possono associarsi ad una PAN solo i device non associati ad altre reti. In caso abbiano già un'associazione attiva, devono prima dissociarsi e poi procedere alla nuova associazione. Ricevere un ack ad una richiesta di associazione non equivale ad essere associati, occorre ricevere l'apposita

risposta e controllare l'attributo status. Infatti se non sono disponibili sufficienti risorse a garantire l'associazione il comando di risposta conterrà un attributo failure con motivazione. Alla ricezione del comando di risposta all'associazione il device è tenuto ad inviare un ack di conferma.

In caso di dissociazione, il coordinator invia un comando di risposta cui il device è tenuto a rispondere tramite ack. Tuttavia anche se non viene recapitato nessun ack il coordinatore assume che la dissociazione sia andata a buon fine.

3.5.4 Sincronizzazione

Così come la scansione dei canali, anche la sincronizzazione può avvenire in modalità differenti: con beacon, senza beacon, orphan device realignment.

Nelle PAN con beacon abilitati la sincronizzazione è gestita tramite beacon. Al contrario, nelle PAN con beacon disabilitati la sincronizzazione avviene tramite POLL. La frequenza e le operazioni di polling sono a discrezione del livello superiore.

La terza modalità, di riallineamento in caso di perdita di sincronizzazione da parte di un device è stata in parte già vista sopra. Il livello superiore accorgendosi del fallimento dei tentativi di comunicazione conclude di essere orfano e parte la procedura di SCAN per cercare di riallinearsi.

3.5.5 Gestione delle transazioni

Essendo questa specifica rivolta a dispositivi con basso consumo energetico e spesso alimentati a batteria, le transazioni sono provocate dai dispositivi stessi piuttosto che dai coordinatori. I coordinatori indicano la presenza di dati in sospeso nei beacon e sta poi al dispositivo inviare una richiesta per l'invio di questi. Questo genere di trasferimenti è denominato trasmissione indiretta (indirect transmission). Nelle reti con beacon disabilitati i coordinatori usano POLL per indicare carichi pendenti.

3.5.6 Trasmissione, ricezione e ack

3.5.6.1 Trasmissione

Ogni volta che viene generato un comando frame viene incrementato di 1 il valore dell'identificativo (macDSN). La stessa cosa accade per i beacon (macBSN).

Gli indirizzi sorgente e destinatario sono codificati secondo le disposizioni della PAN a 16 o 64 bit. Sulla base dei due indirizzi, se sono completi e indicano anche il PAN identifier può essere inserito il valore anche al campo *intraPAN* che indica se i due device sono o meno sulla stessa rete. Prima di trasmettere il dispositivo resta in attesa di un eventuale beacon. Al termine del periodo di attesa se il beacon non è stato rilevato, il device tenterà di trasmettere utilizzando unslotted CSMA-CA. Al contrario, alla rilevazione di un beacon attenderà il CAP e utilizzerà l'algoritmo slotted CSMA-CA.

3.5.6.2 Ricezione e scarto

Data la natura del canale radio un device con receiver abilitato è in grado di ricevere e decodificare tutte le trasmissioni generate da device compatibili allo standard 802.15.4 che stanno operando sullo stesso canale nell'area di copertura, questo può quindi comportare interferenze. Il livello MAC è in grado di filtrare i frame in arrivo e proporre al livello superiore solo i frame di interesse.

Per filtrare i messaggi il livello MAC scarta tutti i frame che non contengono il valore corretto nel campo FCS (frame check sequence). Il livello di selezione successivo dipende da se la *promiscuous mode* è attivata o meno. Se il valore di *macPromiscuousMode*=True non sono applicati ulteriori filtri e il frame viene passato ai livelli superiori. Se l'attributo è invece settato su false i frame vengono accettati solo se soddisfano tutti i seguenti requisiti:

- frame type e frame control field devono avere valori ammessi;
- se il frame type coincide con beacon frame il PAN id deve coincidere al valore impostato come *macPANId* o essere 0xffff;
- se è indicato un destination PAN identifier anche questo deve coincidere con i valori appena indicati;

- se nel frame è incluso un short destination address deve matchare con il proprio *macShortAddress* o essere un indirizzo broadcast (0xffff), ugualmente se è incluso un extended destination address deve matchare con il proprio *aExtendedAddress*;
- se non è indicato alcun indirizzo destinatario il frame è accettato solo se il device è il coordinatore e il PAN identifier coincide con il *macPANid*.

Se anche solo uno dei requisiti precedenti non è soddisfatto il frame viene scartato.

3.5.6.3 Estrarre pending data da un coordinatore

Se siamo in una rete con beacon abilitati, se l'indirizzo del device appare nel campo indirizzi del beacon, MLME può inviare il comando per richiedere dati (data request command) al coordinatore durante il CAP.

Ci sono altri due casi in cui MLME può richiedere dati a un coordinatore. Il primo è quando riceve un MLME-POLL.request, il secondo è dopo un periodo pari ad *aResponseTime* dopo l'invio di un ack a un request command, come ad esempio durante la procedura di associazione.

Il coordinatore al ricevimento di un data request command può rispondere con un ack di conferma, in questo può essere incluso un valore che indica se esistono carichi pendenti per quel device. Se è posto a 0 il device apprende che non esistono dati in sospeso a suo carico, in caso di valore posto a 1 il device abilita il suo receiver. Nel caso in cui il coordinatore non abbia inserito l'attributo frame pending nell'ack e non esistano dati pendenti per il device, spedisce un data frame con payload pari a 0. Se il device non riceve risposta entro il periodo massimo conclude che non vi erano dati pendenti in attesa.

3.5.6.4 Acknowledgment

Le trasmissioni, come abbiamo detto più volte, possono prevedere o meno l'utilizzo di ack di conferma ricezione. Possiamo riassumere i due differenti tipi di trasmissione nelle figure seguenti.

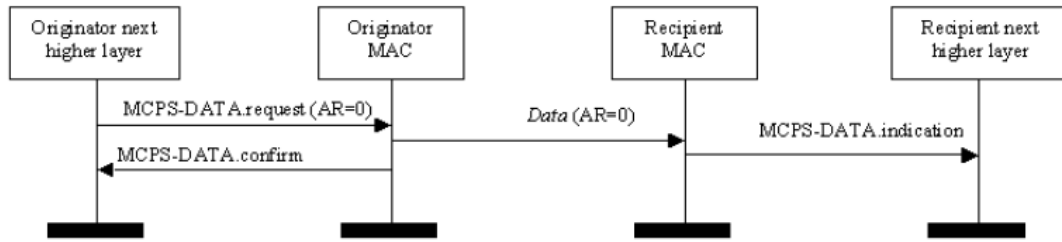


Figura 38 – Trasmissione con successo senza ACK

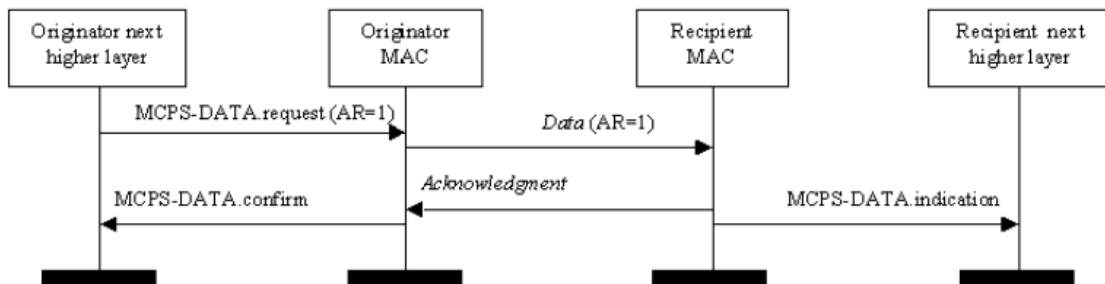


Figura 39 – Trasmissione con successo con ACK

3.5.6.5 Ritrasmissione

Se i beacon sono disabilitati quando un device trasmette assume sempre che la comunicazione vada a buon fine. In caso contrario, con beacon abilitati, se non riceve un ack di conferma entro un periodo di tempo (stabilito dall'attributo *macAckWaitDuration*), o lo riceve ma con un DSN differente, stabilisce che la trasmissione non è andata a buon fine.

Se una trasmissione indiretta non è andata a buon fine il coordinatore non ritrasmette i dati, che restano fra i carichi in sospeso. Se era una trasmissione singola il device deve riprovare il processo fino a raggiungere il massimo numero di tentativi permessi.

Se un ack non è ricevuto dopo il numero massimo di tentativi di invii il livello MAC assume che la trasmissione è fallita e riferisce l'esito al livello superiore.

Un possibile scenario di trasmissione è raffigurato nella figura seguente:

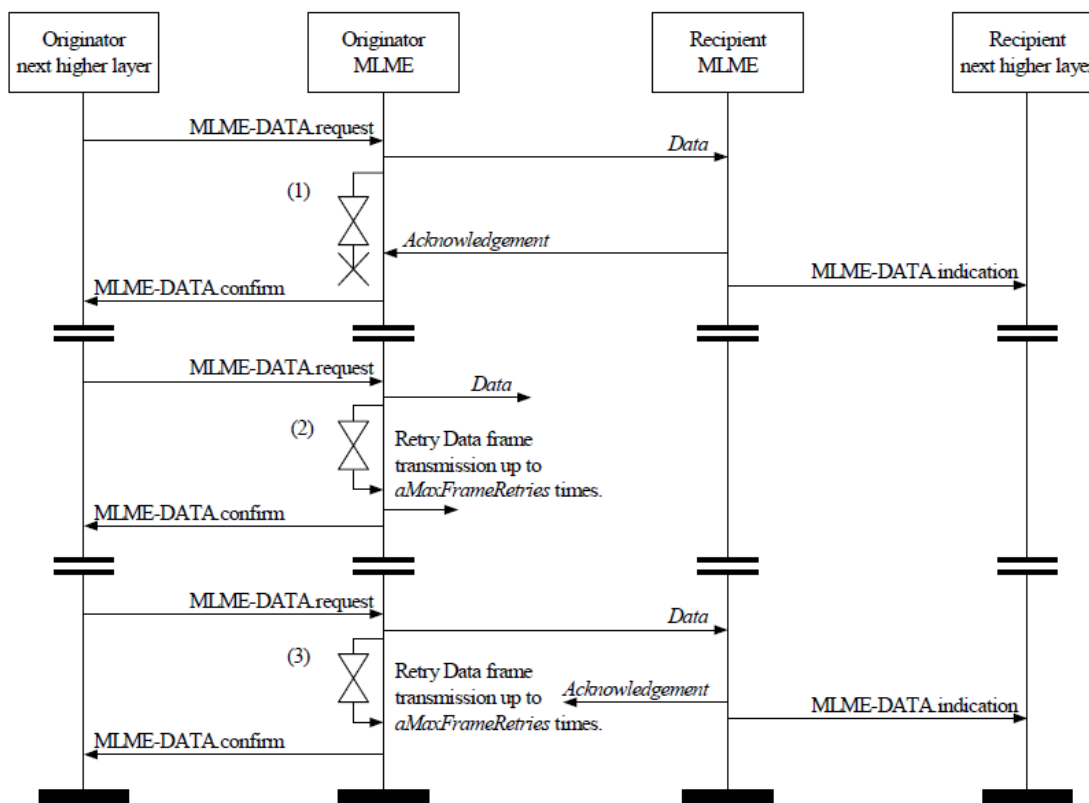


Figura 40 – esempio: Scenario di trasmissione

3.5.7 Allocazione e gestione GTS

GTS consente a un device di operare sul canale con una porzione di superframe dedicata in forma esclusiva. Sono allocati dal coordinatore e utilizzati per le comunicazioni fra coordinator e device. Un singolo GTS può anche esteso a più superframe slot consecutivi e il coordinatore può allocarne fino a un massimo di 7, e, per ognuno di essi definire la durata, l'indirizzo del device associato, la direzione (ricezione o trasmissione) e lo slot in cui inizia. Devono essere allocati prima dell'uso e possono poi essere deallocati a discrezione del coordinatore. Se ad un device è stato allocato un GTS ciò non gli toglie la possibilità di comunicare durante il CAP.

I data frame spediti durante GTS usano gli indirizzi brevi a 16bit anziché la forma estesa a 64.

Per gli RFD è opzionale supportare e usare GTS.

La deallocazione di un GTS è richiesta dal device. In seguito a questa resta uno spazio inattivo nel superframe, pertanto il coordinatore deve

riallocare il GTS aumentando, ad esempio, la finestra di CAP. Un esempio di questa procedura è mostrato nella figura seguente.

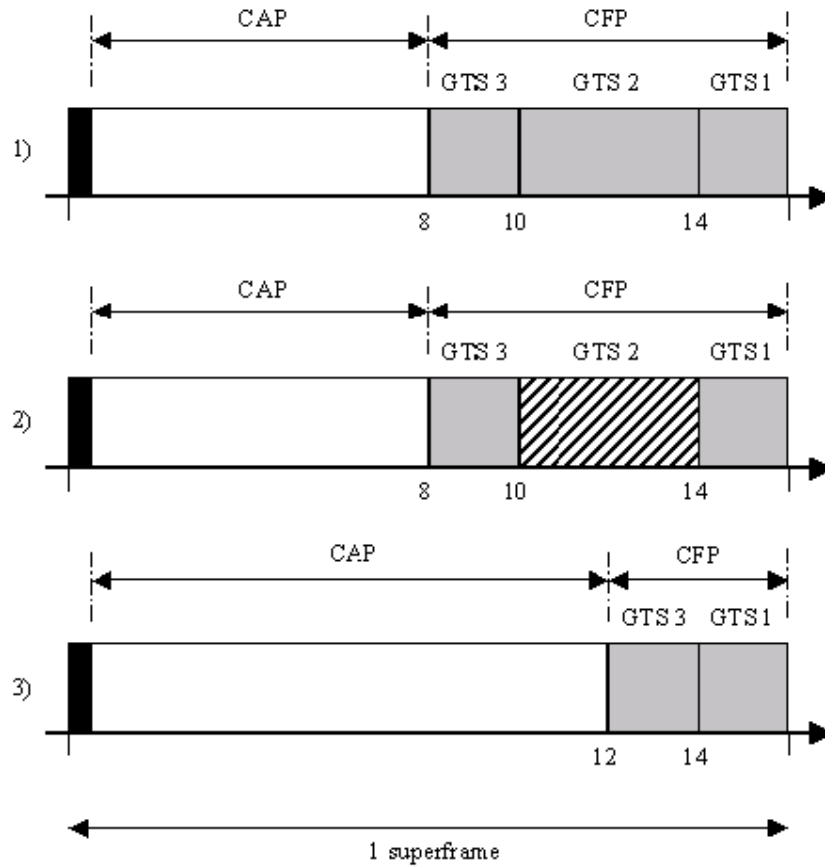


Figura 41 - segmentazione CFP e riallocazione GTS

3.5.8 *Frame Security*

Quando richiesto dai livelli superiori il livello MAC deve fornire servizi di sicurezza su specifici frame in arrivo o in partenza. I servizi supportati sono:

- Access control
- Data encryption
- Frame integrity
- Sequential freshness

A questi si aggiungono le seguenti modalità di sicurezza:

- Unsecured mode: è la modalità di default, non fa uso della ACL (access control list) e i device non effettuano operazioni relative alla sicurezza sui frame in arrivo.
- ACL mode: i device in modalità ACL non possono eseguire modifiche ai frame o eseguire operazioni di crittografia su di essi. Permette di filtrare il source address, ma non è detto che questo sia colui che l'ha originato. Dopo i controlli per filtrare i frame in arrivo, se il device trova il campo relativo alla sicurezza impostato ad 1, passa il frame al livello superiore.
- Secured mode: offre sia le funzioni dell'ACL mode che opzioni crittografiche di protezione dei frame in arrivo e in uscita.

BIBLIOGRAFIA

- ZigBee Alliance, *ZigBee Specification*, Version 1.0, December 2004;
- ZigBee Alliance, *ZigBee*, “www.zigbee.org”;
- IEEE, *IEEE 802.15.4 WPAN-LR Task Group*,
<http://www.ieee802.org/15/pub/TG4.html>
- IEEE, *IEEE 802.15.4a-2007*,
“<http://standards.ieee.org/getieee802/download/802.15.4a-2007.pdf>”
- IEEE, *IEEE 802.15.4-2006*,
“<http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf>”
- IEEE, *IEEE 802.15.4-2003*,
“<http://standards.ieee.org/getieee802/download/802.15.4-2003.pdf>”
- Wikipedia, *802.15*, “http://en.wikipedia.org/wiki/IEEE_802.15”
- Wikipedia, *ZigBee*, “<http://en.wikipedia.org/wiki/ZigBee>”

Immagini:

802 Wireless Space:

http://www.specifications.nl/zigbee/zigbee_UK.php

Wireless market: <http://digital.cyberini.com/>

ZigBee Stack <http://zone.ni.com/devzone/cda/tut/p/id/7118>

Tutte le altre immagini:

<http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf>

GLOSSARIO

AES advanced encryption standard

ASK amplitude shift keying

AWGN additive white Gaussian noise

AWN affected wireless network

BE backoff exponent

BER bit error rate

BI beacon interval

BLE battery life extension

BO beacon order

BPSK binary phase-shift keying

BSN beacon sequence number

CAP contention access period

CBC-MAC cipher block chaining message authentication code

CCA clear channel assessment

CCM counter with CBC-MAC (mode of operation)

CCM* extension of CCM

CFP contention-free period

CRC cyclic redundancy check

CSMA-CA carrier sense multiple access with collision avoidance

CTR counter mode

CW contention window (length)

DSN data sequence number

DSSS direct sequence spread spectrum

ED energy detection

EIRP effective isotropic radiated power

EMC electromagnetic compatibility

ERP effective radiated power

EVM error-vector magnitude

FCS frame check sequence
FFD full-function device
FH frequency hopping
FHSS frequency hopping spread spectrum
GTS guaranteed time slot
IFS interframe space or spacing
ISM industrial, scientific, and medical
IUT implementation under test
IWN interfering wireless network
LIFS long interframe spacing
LLC logical link control
LQI link quality indication
LPDU LLC protocol data unit
LR-WPAN low-rate wireless personal area network
LSB least significant bit
MAC medium access control
MCPS MAC common part sublayer
MCPS-SAP MAC common part sublayer service access point
MFR MAC footer
MHR MAC header
MIC message integrity code
MLME MAC sublayer management entity
MLME-SAP MAC sublayer management entity service access point
MSB most significant bit
MPDU MAC protocol data unit
MSDU MAC service data unit
NB number of backoff (periods)
OCDM orthogonal code division multiplexing
O-QPSK offset quadrature phase-shift keying

OSI open systems interconnection
PAN personal area network
PC personal computer
PD PHY data
PD-SAP PHY data service access point
PER packet error rate
PHR PHY header
PHY physical layer
PIB PAN information base
PICS protocol implementation conformance statement
PLME physical layer management entity
PLME-SAP physical layer management entity service access point
PN pseudo-random noise
POS personal operating space
PPDU PHY protocol data unit
PSD power spectral density
PSDU PHY service data unit
PSSS parallel sequence spread spectrum
RF radio frequency
RFD reduced-function device
RX receive or receiver
SD superframe duration
SER symbol error rate
SFD start-of-frame delimiter
SHR synchronization header
SIFS short interframe spacing
SIR signal-to-interference ratio
SNR signal-to-noise ratio
SO superframe order

SPDU SSCS protocol data units

SRD short-range device

SSCS service-specific convergence sublayer

SUT system under test

TRX transceiver

TX transmit or transmitter

WLAN wireless local area network

WPAN wireless personal area network