

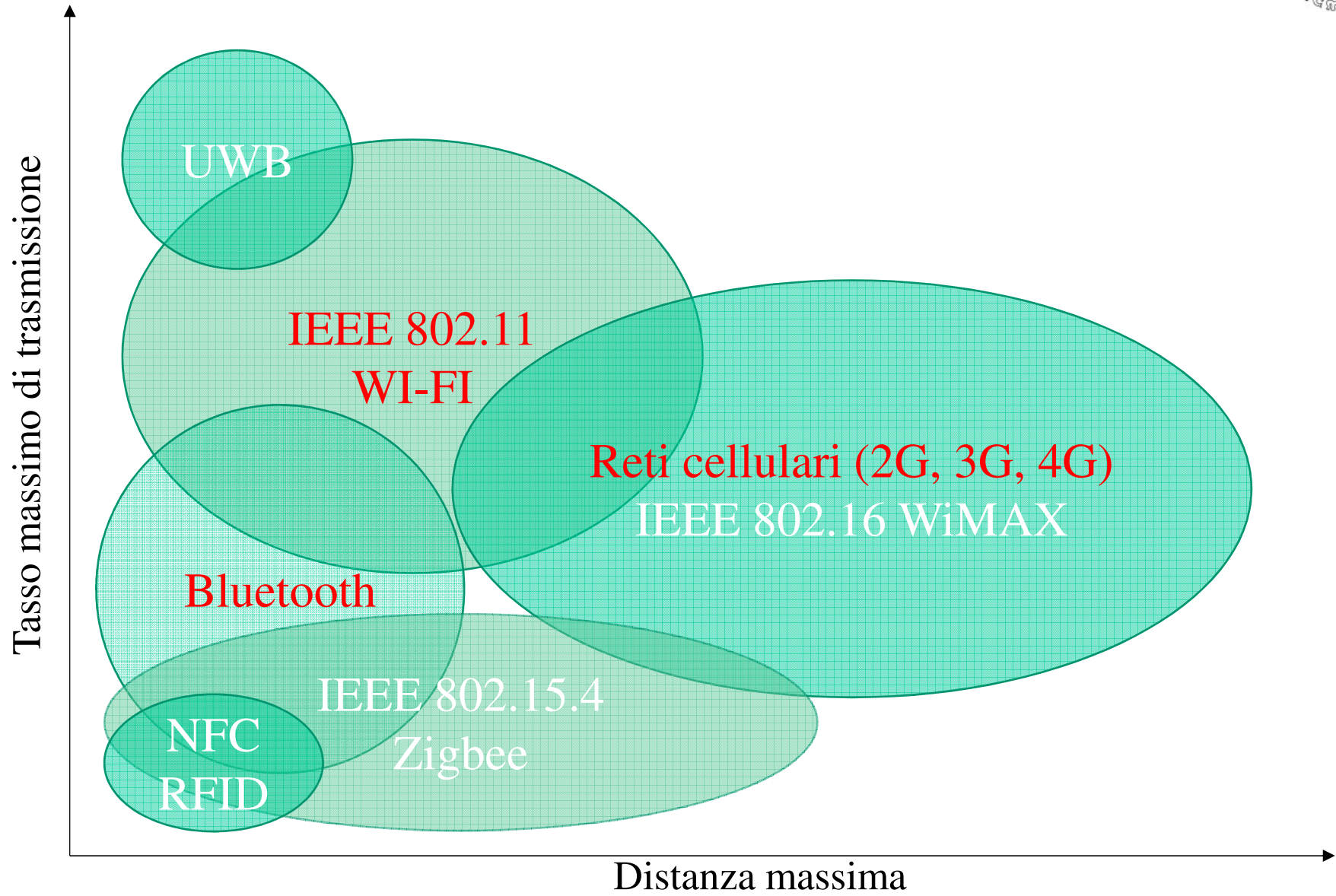


Reti di sensori

Fulvio Babich (babich@units.it)

DIA – Università di Trieste

Confronto fra tecniche wireless





Frequenze non licenziate (ISM)

Fmin	Fmax	Banda	F. centrale	Regione
0	150 kHz	150 kHz	75 kHz	1 (Europa)
6.765 MHz	6.795 MHz	30 kHz	6.78 MHz	Locale
13.553 MHz	13.567 MHz	14 kHz	13.56 MHz	RFID
26.957 MHz	27.283 MHz	326 kHz	27.12 MHz	CB
40.66 MHz	40.70 MHz	40 kHz	40.68 MHz	Radio models
433.05 MHz	434.79 MHz	1.74 MHz	433.92 MHz	1 (locale)
866 MHz	868 MHz	2 MHz	867 MHz	1
902 MHz	928 MHz	26 MHz	915 MHz	2 (America)
2.4 GHz	2.4835 GHz	83.5 MHz	2.441 GHz	1,2,3 (Asia)
5.725 GHz	5.875 GHz	150 MHz	5.8 GHz	+ 150 MHz in 3
24 GHz	24.25 GHz	250 MHz	24.125 GHz	
61 GHz	61.5 GHz	500 MHz	61.25 GHz	Local
122 GHz	123 GHz	1 GHz	122.5 GHz	Local
244 GHz	246 GHz	2 GHz	245 GHz	Local



IEEE 802.15.1 – Bluetooth

- Il nome del protocollo deriva da Harold Bluetooth, Re Aroldo I di Danimarca (901 - 985), noto per le sue abilità diplomatiche.
- Sviluppato inizialmente dalla Ericsson nel 1994.
- Diffuso dall'organizzazione Bluetooth Special Interest Group (SIG: Ericsson, Intel, Nokia, Toshiba and IBM).
- Motivazione: usato per connettere diversi dispositivi wireless (cuffie, auricolari, telecamere, stampanti, ...).
- Scenario: **WPAN** in cui è necessario sostenere **traffico multimediale**.
- Obiettivo: **throughput**.



Lo standard

- Specificazione tecnica in 2 parti:
 - **Core** (radiofrequenza, operazioni in BB, link manager, ecc).
 - **Profiles** (protocolli e procedure specifici per varie applicazioni).
- Caratteristiche principali
 - Banda ISM (Industrial, Scientific, Medical) a 2.4/2.4835 GHz,
 - Frequency-hopping sulla banda (1600 hop/s),
 - Distanza massima; 100 m
 - Modulazione G-FSK
 - Bit-rate: 721 kbps (*Bluetooth Basic Rate*) 3 Mbit/s (*Enhanced Data Rate*)
 - Duplexing: TDD
 - Trasmissione asincrona (*packet switched*) o sincrona (voce)



Versioni Bluetooth

- **Versione 1.1:** IEEE 802.15.1-2002
- **Bluetooth 1.2:** IEEE 802.15.1-2005
- **Bluetooth 2.0 + Enhanced Data Rate (EDR):** Compatibile con le versioni precedenti (obsolete) introduce Enhanced Data Rate (EDR).
- **Bluetooth 2.1 + EDR:** *Extended inquiry response* (EIR) migliore filtraggio dei dispositivi prima del collegamento
- **Bluetooth 3.0 + HS:** possibilità di sfruttare connessioni Wi-Fi (solo quando necessario)
- **Bluetooth 4.0:** Low Energy.
- **Bluetooth 4.1:** risolve problemi di compatibilità con LTE mediante verifica utilizzo della banda.
- **Bluetooth 4.2:** connessione diretta a Internet.
- **Bluetooth 5.0:** Copre 200 metri e raggiunge i 4 Mbps. Utilizzato per le applicazioni Internet of Things (IoT).



Bluetooth

- **Bluetooth Basic Rate/Enhanced Data Rate (BR/EDR)**, (versioni 2.x): stabilisce una connessione wireless, a breve distanza; ideale per applicazioni anche a tasso elevato (streaming audio).
- **Bluetooth High Speed (HS)** (versioni 3.x): Le applicazioni possono utilizzare standard trasmissivi di prestazioni superiori (802.11).
- **Bluetooth with low energy (LE)**, (versioni 4.0/4.1/4.2): trasmissione di pacchetti corti, in modo discontinuo, anche a grande distanza; ideale per applicazioni che richiedono un basso consumo di energia, per incrementare la durata della batteria (IoT).
- **Dual-Mode**: chipset compatibili sia con la versione BR/EDR, che con la versione LE (utilizzati dagli smartphone che hanno bisogno sia di collegamenti a larga banda, ad esempio per connettersi alle cuffie, che di collegamenti con dispositivi a bassa energia, quali i sensori personali).

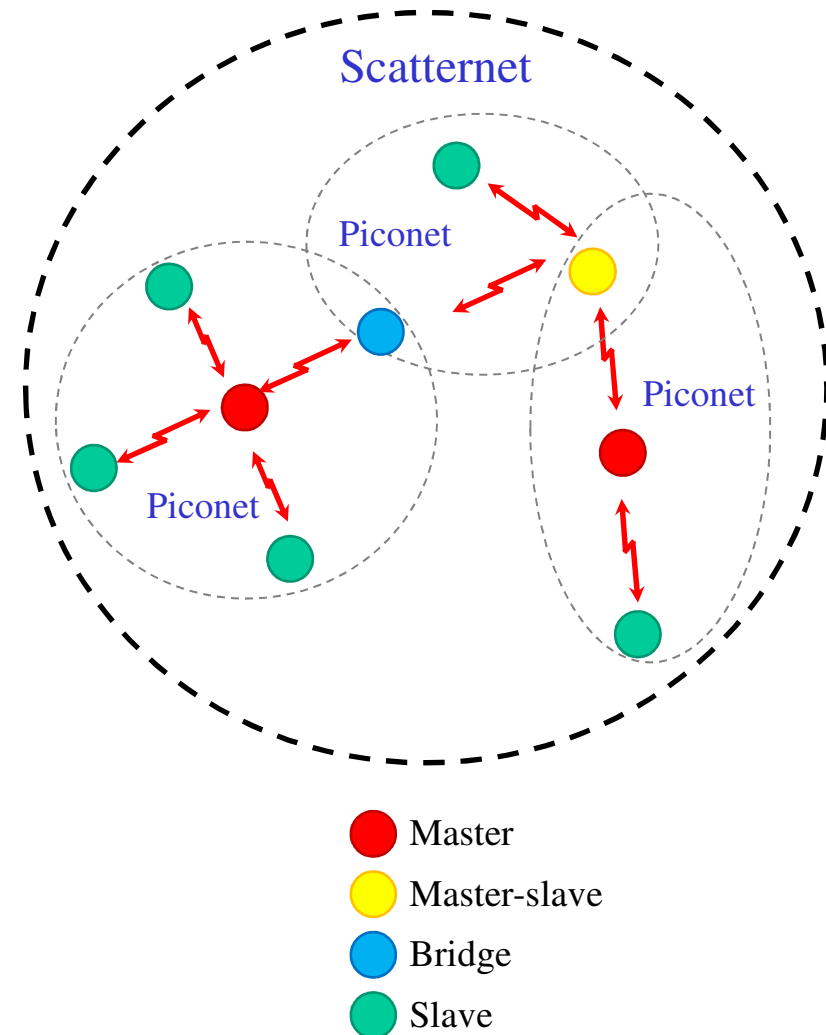


Bluetooth BR/EDR

- La trasmissione Basic Rate / Enhanced Data Rate (BR/EDR) utilizza l'intervallo di frequenze ISM a 2.4 GHz.
- Il sistema utilizza la tecnica frequency hopping per diversità (1600 hop/secondo). Sono disponibili 79 frequenze, spaziate di 1 MHz, nella banda ISM.
- La trasmissione BR utilizza la GFSK con tasso pari a 1 Mbit/s.
- La trasmissione EDR opera a un tasso di 2 (DQPSK) o 3Mbit/s (8 PSK).
- Il canale è condiviso da un gruppo di stazioni sincronizzate, che eseguono pattern FH ortogonali tra loro.
- Il pattern di sincronizzazione è fornito da uno dei dispositivi connessi, detto master. Gli altri dispositivi sono detti slave.
- Una rete così configurate è detta **piconet**.
- Due o più piconet possono cooperare per formare una **scatternet** (non è previsto alcun handover tra le piconet)

Topologia Bluetooth

- **Accesso centralizzato** (slotted): struttura master-slave, in cui il master coordina tutti gli slave tramite **polling**.
- Tutti gli slave che sono coordinati dal master formano una **piconet**.
- Più piconet possono essere unite a formare una **scatternet**, in cui un master di una piconet può fare da slave in un'altra piconet ed alcuni master o slave possono fare da bridge.



Caratteristiche tecniche



Livello	Funzione	Basic Rate	Low Energy
Data Link	Lunghezza pacchetti	68-2871 bit	80-376 bit
	Trasporto	Sincrono asincrono	Asincrono
	Trasmissione	Slot da 625 μ s	Eventi di lunghezza variabile
	Stati dispositivo	3 stati (<i>standby, connection, park</i>) e 7 sottostati Slave. 3 modalità (<i>active, sniff, hold</i>)	5 stati: <i>standby, advertising, scanning, initiating, connection</i> (master/slave)
Fisico	Canali	79 canali da 1 MHz	40 canali da 2 MHz suddivisi in canali data e canali advertising
	Modulazione	GFSK (BR), OQPSK (EDR 2Mbs), 8DPSK (EDR 3Mbs)	GFSK
	Trasmittitore	4 classi di potenza	Potenza minima e massima



Il livello fisico (I)

Classi di potenza	Potenza massima	Potenza minima	Distanza
1	100 mW (20 dBm)	1 mW (0 dBm)	100 m
2	2.5 mW (4 dBm)	0.25 mW (-6 dBm)	10 m
3	1 mW (0 dBm)	N/A	1 m
4	0.5 mW (-3 dBm)	N/A	0.5 m

Classi di potenza per trasmettitori Bluetooth Basic Rate

Classi di potenza	Potenza massima	Potenza minima	Distanza
Unica	10 mW (10 dBm)	0.01 mW (-20 dBm)	50 m

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



Livello fisico (II)

- Parametri **modulazione G-FSK**, con scostamento $\pm f_d$ dalla frequenza della portante f_c .
- Indice di modulazione: $m=2f_d T$, dove $T=1 \mu s$ è l'intervallo di segnalazione.
 - Bluetooth Basic Rate: $m=0.28 \div 0.35$ ($f_d=140 \div 175$ kHz)
 - Bluetooth Low Energy: $m=0.45 \div 0.55$ ($f_d=225 \div 275$ kHz)
- Banda canale (delimitata dal filtro gaussiano): $W=1/2T$.

Luogo	Intervallo	Guardia inf.	Guardia sup.	Canali
USA, Europa	2.400-2.4835 GHz	2 MHz	3.5 MHz	79
Spagna	2.445-2.4750 GHz	4 MHz	4 MHz	23
Francia	2.4465-2.4835 GHz	7.5 MHz	7.5 MHz	23
Giappone	2.4710-2.4970 GHz	2 MHz	2 MHz	23

Banda ISM (Intervallo di frequenze disponibili)



Canali radio

Luogo	Canali radio
USA, Europa	$f=2402+k$ MHz, $k=0\dots,78$
Spagna	$f=2449+k$ MHz, $k=0\dots,22$
Francia	$f=2454+k$ MHz, $k=0\dots,22$
Giappone	$f=2473+k$ MHz, $k=0\dots,22$

Canali Bluetooth Basic Rate

$$f=2402+2k \text{ MHz, } k=0, \dots, 39$$

Canali Bluetooth Low Energy

- I canali alle frequenze di 2402 MHz (canale 37), 2426 MHz (canale 38) e 2480 MHz (canale 39) sono compatibili con i canali 1, 6, 11 di 802.11b (primo gruppo di canali non sovrapposti).
- Gli altri canali (da 2404 MHz, canale 0, a 2478 MHz, canale 36) sono canali di traffico.



Profili

- Un profilo rappresenta un insieme di caratteristiche comuni a diversi dispositivi che garantiscono l'utilizzo di nuove funzionalità
- Solo dispositivi che hanno lo stesso profilo sono in grado di scambiarsi informazioni
 - Generic Access Profile (GAP)
 - Service Discovery Application Profile (SDAP)
 - Cordless Telephony Profile (CTP)
 - Serial Port Profile (SPP)
 - Headset Profile (HSP)
 - Dial-up Networking Profile (DUNP)
 - LAN Access Profile (LAP)
 - File Transfer Profile (FTP)
 - Synchronisation Profile (SP)



Stati Bluetooth BR/ER

- Stati principali:
 - **standby**: stato di default del dispositivo. Disabilitata trasmissione/ricezione dati.
 - **connection**: fase scambio dati. I dispositivi si dividono in master e slave.
 - *Active*: un dispositivo in questo stato è sempre acceso e disponibile
 - *Sniff*: il dispositivo slave passa allo stato active periodicamente
 - *Hold*: lo slave passa allo stato active dopo un tempo concordato con il master
 - **park**: lo slave si sincronizza periodicamente con il master.
- Sottostati utilizzati in fase di ricerca di dispositivi e di connessione:
 - page
 - page scan
 - inquiry
 - inquiry scan
 - master response
 - slave response
 - inquiry response.

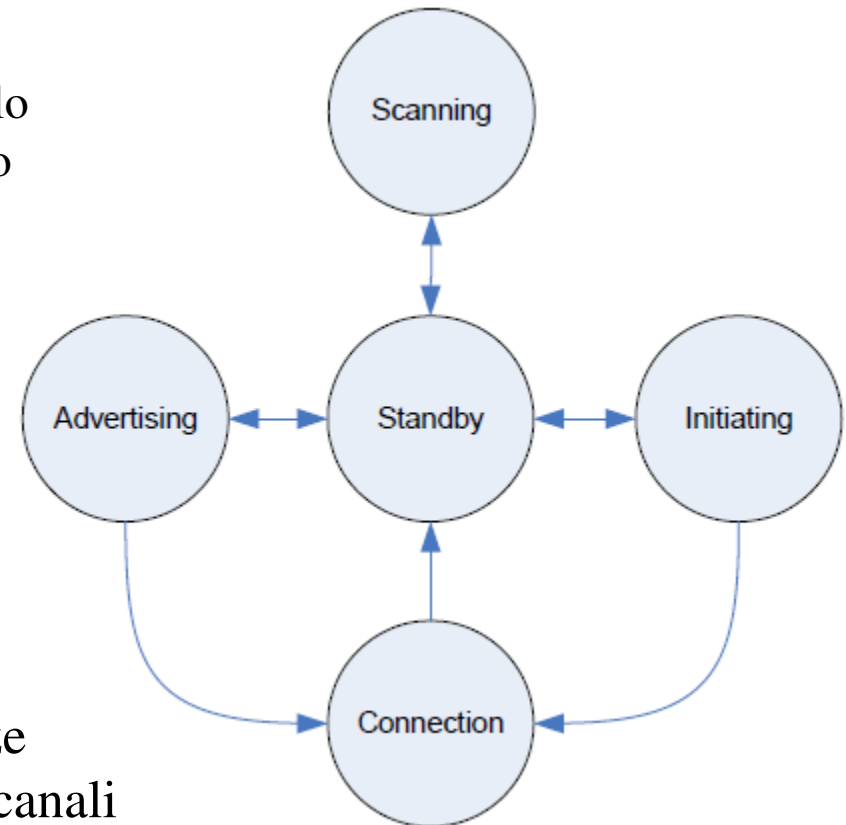


Trasmissione pacchetti BR/ER

- Durata slot: 625 μ s.
- Nella fase di ricerca la frequenza di hop raddoppia.
 - Slot usati dal master e slot usati dallo slave si alternano.
 - Il master può inviare un pacchetto ogni 312.5 μ s (cambiando frequenza).
 - Il pacchetto utilizzato nella fase di ricerca è detto ID (identity message) ed è composto da 68 bit contenenti informazioni per la sincronizzazione.
 - In caso di successo, dopo 1250 μ s (2 slot) dall'invio del pacchetto ID ricevuto dallo slave, il master trasmette un pacchetto detto FHS (Frequency Hopping Synchronization) che contiene l'indirizzo di dispositivo e il clock del master.
- Nella fase di trasmissione i dispositivi master e slave utilizzano i canali basic piconet o adapted piconet che utilizzano le stesse 79 frequenze determinate a livello fisico.
- La frequenza di hopping è di 1600 hop/s. Sia il master che lo slave possono inviare al massimo un pacchetto per slot, ma l'invio di un pacchetto può richiedere anche più slot fino ad un massimo di cinque.

Stati Bluetooth LE

- Stati
 - **standby**: trasmissione dati disabilitata.
 - **advertising**: ricerca di dispositivi negli stati di scanning e initiating; dallo stato di advertising si può passare allo stato connection in qualità di master.
 - **scanning**: usato per monitorare la rete; può essere passivo o attivo (inviando scan request).
 - **initiating**: disponibile a far parte di una rete in qualità di slave.
 - **connection**: fase scambio dati.
- Nelle fasi di scanning e advertising vengono utilizzati 3 canali (a frequenze compatibili con 802.11b), contro i 32 canali inquiry scan e page scan della versione BR/EDR, con notevole risparmio di tempo (1.2 ms contro 22.5 ms).





Pacchetti BLE

- Due tipi di pacchetti
 - **Advertising packet**: sono di tipo broadcast, oppure unicast. Trasmessi sui 3 canali di advertising
 - **Data packet**: sempre unicast (dialogo master-slave). Trasmessi sui canali dati.
- Scrambler (**whitener**): utilizzato per rendere ‘0’ e ‘1’ equiprobabili:
 $g(x)=x^7+x^4+1$.
- Struttura pacchetto:
 - **Preambolo** (8 bit): 01010101 (usato se il campo successivo – indirizzo – inizia per 1), 10101010 (altrimenti).
 - Address (32 bit): 6 D E B ...
 - Advertising packets: 0x8E89BED6 (dal fondo), 0110 1011 0111 1101 ...
 - Data access address: numero casuale, con regole per evitare pattern ripetitivi
 - **Header** (8 bit): pagina successiva.
 - **Length** (8 bit): payload in bytes (advertising: da 0 a 37, data: da 0 a 31).
 - **Payload** (0-296 bit):
 - **CRC** (24 bit): $g(x)=x^{24}+x^{10}+x^9+x^6+x^4+x^3+x+1$



Header pacchetto BLE

- Il contenuto dipende dal tipo di pacchetto (Advertising o Data)
 - **Data packet**
 - Logical Link Identifier - LLI (2 bit): 11 (Control packet), 10 (Inizio Data Packet dei livelli superiori o pacchetto completo), 01 (continuazione pacchetto).
 - Next Expected Sequence Number – NESN (1 bit). Per acknowledgment.
 - Sequence Number – SN (1 bit). Parte da 0.
 - More Data - MD (1 bit)
 - Riservato (3 bit)
 - **Advertising packet**
 - Tipo di pacchetto (4 bit)
 - Riservato (2 bit)
 - Tipo di indirizzo Tx (1 bit)
 - Tipo di indirizzo Rx (1 bit)



Advertising, Initiating (1)

- Lo stato advertising è utilizzato per trasmettere un advertising packet, o per ricevere scan request (rispondendo scan response) da dispositivi in scanning attivo.
- Può essere utilizzato per inviare messaggi broadcast.
- Un dispositivo che utilizza lo stato di advertising deve avere il trasmettitore (ma potrebbe non avere il ricevitore, se non utilizza altri stati).
- Dallo stato advertising si passa allo stato connection, dopo aver ricevuto connection request da un dispositivo nello stato initiating.
- Dallo stato initiating si può passare a quello connect dopo aver trasmesso un connection request a un advertiser.



Advertising (2)

- 4 tipi: general, directed, nonconnectable, discoverable.
- **Advertising Event**: sequenza di pacchetti advertising.
 - Spedito periodicamente sui canali di advertising. Periodo multiplo di 0.625 ms, compreso fra 20 ms e 10.28 s (tranne per il directed).
All'intervallo periodico viene aggiunto un ritardo casuale, compreso tra 0 e 10 ms, per evitare collisioni sistematiche.
- **General**: un dispositivo non connesso lo invia periodicamente per indicare la disponibilità a una connessione in qualità di slave.
- **Directed**: richiesta di connessione (include l'indirizzo dell'advertiser – slave – e dell'initiator – master e nessun altro dato). Periodo: 3.75 ms (in caso di mancata connessione, termina dopo 1.28 s).
- **Nonconnectable**: utilizzato per inviare informazioni, senza essere disponibile a connessioni (richiede il solo trasmettitore).
- **Discoverable**: utilizzato per scambiare dati senza connessione.

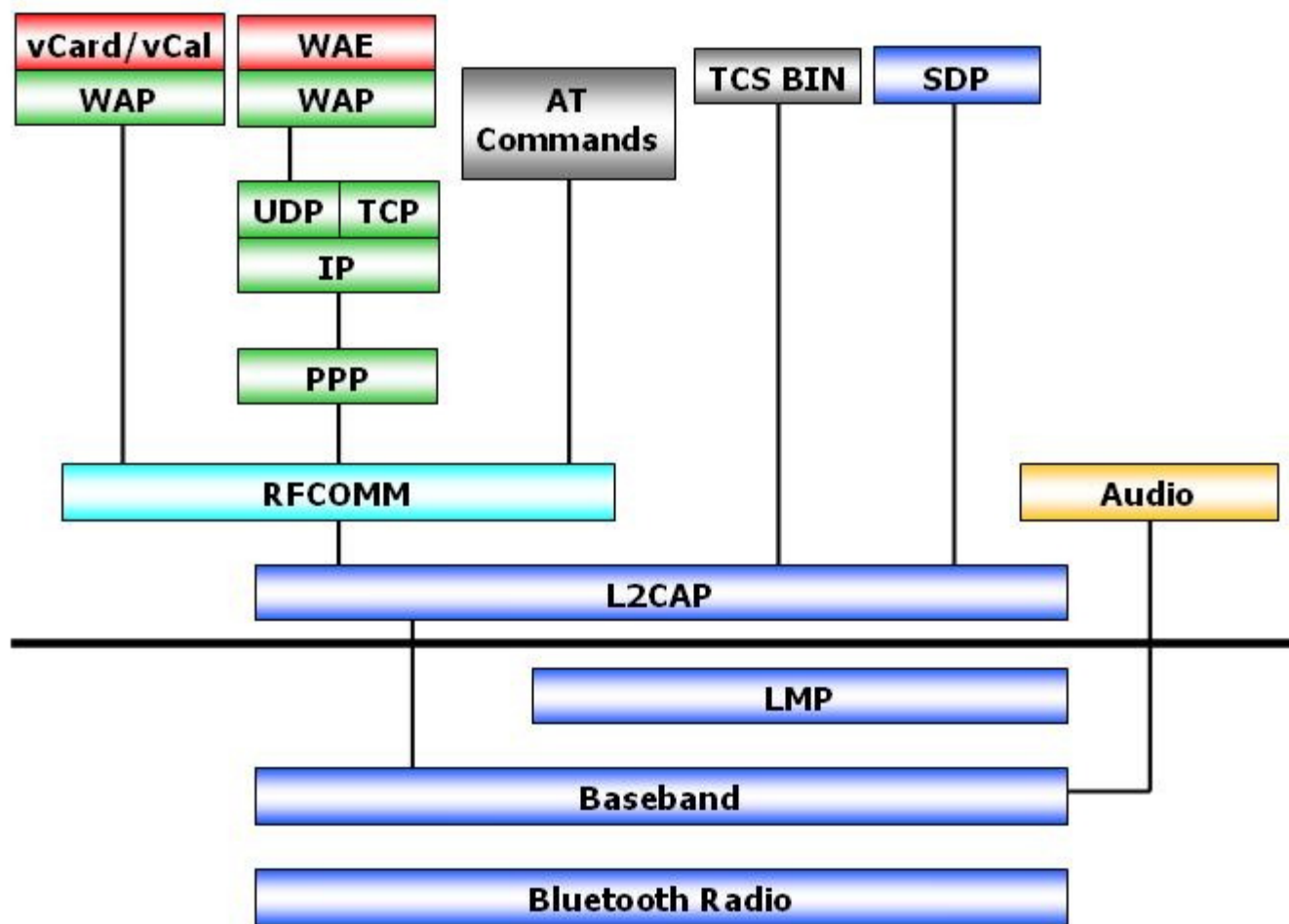


Connection

- La connessione è utilizzata per trasmettere dati in modo sistematico e affidabile.
- Iniziata da un Advertiser (ADV_IND) e richiesta da un Initiator (CONNECT_REQ)
- **Connection Event**
 - Una volta connessi, gli scambi avvengono mediante Connection Event (iniziato dal master).
 - I Connection Event si ripetono con periodo multiplo di 1.25 ms, tra 7.5 ms e 4 secondi (Connection Interval).
 - All'interno di un Connection Event, uno o più pacchetti vengono trasmessi con spaziatura di 0.15 ms, su una sola frequenza.
 - Uno slave può ignorare la richiesta di Connection Event per un certo numero di volte (Slave Latency; delimitata dal Supervision Timeout).
Esempio: Connection Interval: 100 ms, Latency: 9, Supervision Timeout: 6 secondi; lo slave deve ascoltare almeno 1 Connection Event al secondo, e ci devono essere almeno 6 eventi prima che la connessione sia chiusa.



Bluetooth Protocol Stack

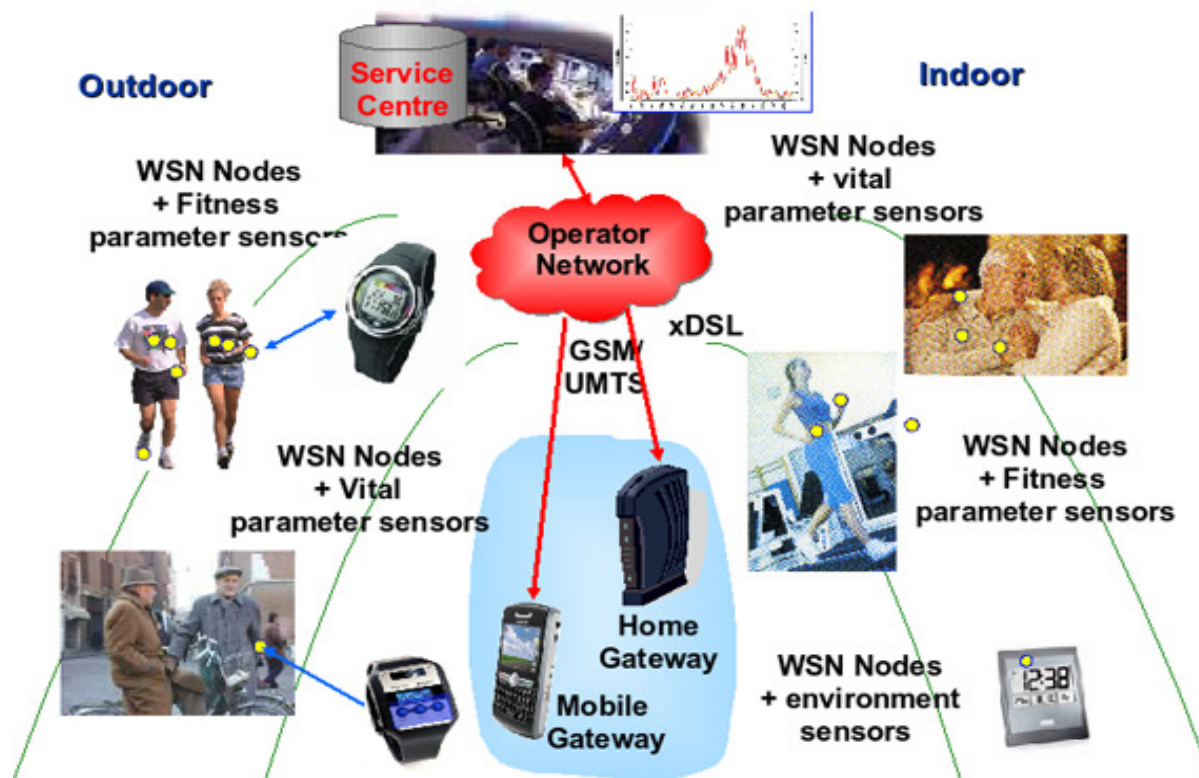




Wireless Sensor Network

- Caratteristiche principali:
 - consumo energetico ridotto;
 - potenze di trasmissione ridotte;
 - throughput ridotto;
 - raggio di operazione ridotto;
 - costi ridotti;
 - complessità progettuale ridotta (componentistica economica);
 - densità di posizionamento a volte elevata;
 - auto-configurabilità della rete.

Applicazioni



- medicina (stato paziente)
- sistemi di allarmi intelligenti
- monitoraggio del territorio
- applicazioni militari
- monitoraggio processi di produzione
- rilevamento in zone difficilmente accessibili

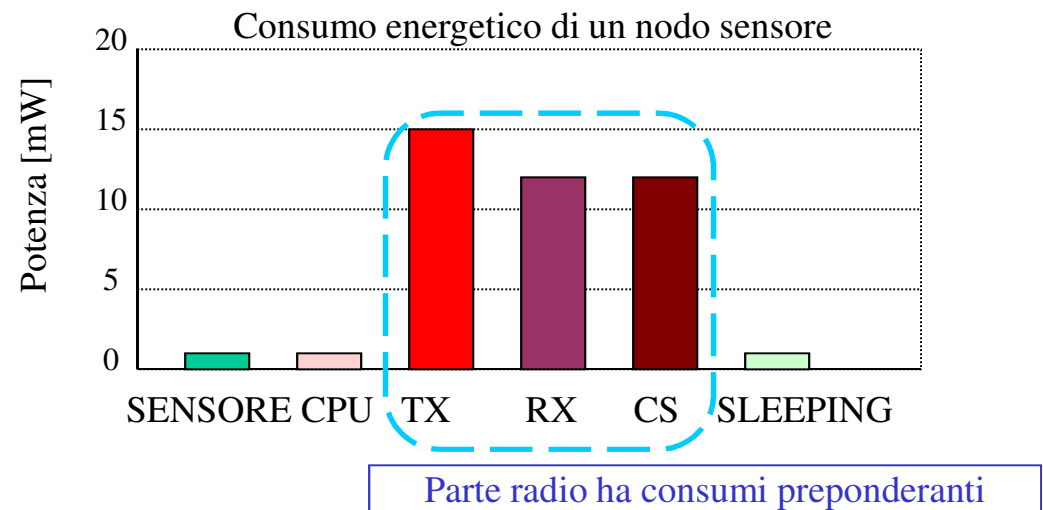


Parametri

- Tempo di vita (dato che spesso i nodi sono alimentati a batterie).
- Tolleranza ai guasti (probabilità di non avere guasti nell'intervallo $(0,t)$ di solito descritta da una legge esponenziale di parametro λ : per il nodo k -mo, $R_k(t)=\exp(-\lambda_k t)$).
- Consumo energetico.
- Latenza (ritardo).
- Integrità (consegna accurata dei dati).
- Ridondanza (affidabilità, resistenza ai guasti).
- Sicurezza.
- Throughput.
- Probabilità di perdita.
- Scalabilità (descritta dalla densità $\mu(r)$: numero di nodi N , con raggio di copertura r , in una regione di area A : $\mu(r)=N\pi r^2/A$).

IEEE 802.15.4 - ZigBee

- Motivazione: estensione nata per gestire l'accesso in una Wireless Sensor Network (WSN) in scenari caratterizzati dall'assenza di una rete di alimentazione fissa e dall'impossibilità di cambiare la batteria (monitoraggio ambientale, applicazioni industriali o militari). L'obiettivo fondamentale diventa **minimizzare il consumo energetico**, anche accettando forti riduzioni di throughput.
- **Nodo sensore**: nodo estremamente semplice e di basso costo, costituito dal sensore fisico, dall'unità di elaborazione (CPU), e dalla parte radio. I **consumi principali** sono dovuti alla parte radio (CS, ricezione e trasmissione **hanno consumi simili**). Il risparmio energetico viene raggiunto tenendo la parte **radio spenta per più tempo possibile** (i nodi sono attivi solo per brevi periodi di tempo).
- Supportato sia l'accesso **centralizzato** che quello **distribuito** (CSMA/CA).
- La tecnologia **ZigBee** (più economica di Bluetooth) deve soddisfare le specifiche 802.15.4, ma può avere funzionalità in più, come ad esempio il **routing**.





Zig Bee

- Il nome deriva dalla "Waggle dance", movimenti che l'ape utilizza per informare le compagne sulla posizione dei fiori
- Un insieme di aziende fondano il gruppo ZigBee Alliance con l'obiettivo di creare uno standard per dispositivi wireless a basso rate e consumo energetico
- I primi due livelli (fisico (PHY) e Medium Access Control (MAC)) adottano lo standard IEEE 802.15.4
- Il protocol stack prevede anche il livello network (NWT) e il livello applicazione (APL)



Livello fisico (1)

- Lo standard 802.15.4 specifica l'uso della tecnica Direct Sequence Spread Spectrum (DSSS) suddivisa nelle seguenti frequenze:
 - ISM 868/915 MHz europea e 902 - 928 MHz americana
 - ISM 2450 MHz internazionale.In questa banda si adotta la O-QPSK. I bit vengono associati ai chip in gruppi di 4. A 4 bit corrispondono 32 chip (SF=8). I chip di posto dispari sono trasportati dalla parte in fase, quelli di posto pari dalla parte in quadratura.

PHY (MHz)	Band (MHz)	Parameters		Data parameters
		Chip rate (kchip/s)	Modulation	Bit rate (kbit/s)
868/915	868-868.6	300	BPSK	20
	902-928	600	BPSK	40
2450	2400-2483.5	2000	O-QPSK	250

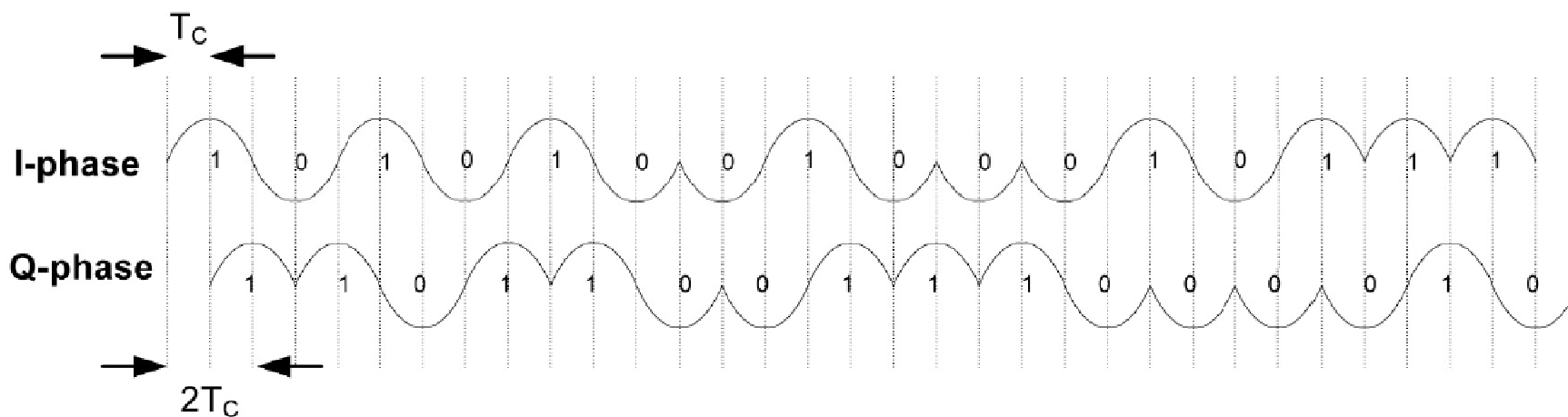


Mapping a 2.45 GHz

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

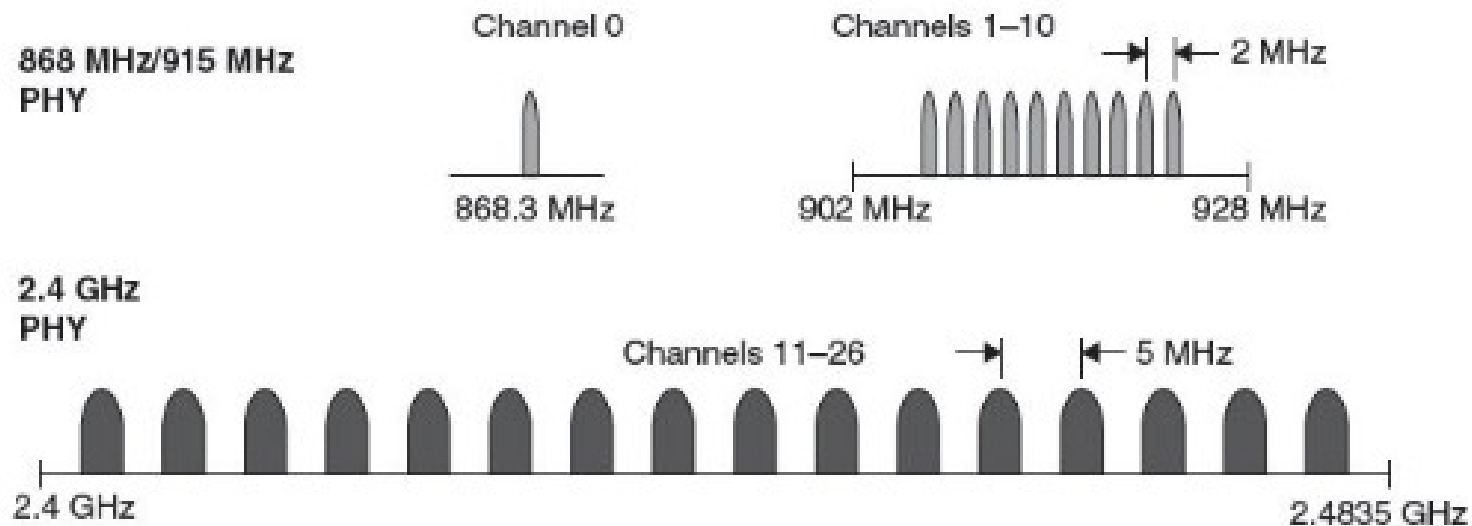
Esempio

- Trasmissione chip associati a $0000 T_c = 0.5 \mu\text{s}$.



Canali

- Un canale nella banda 868 MHz, con data rate 20 kbps
- 10 canali nella banda 915 MHz spazati di 2 MHz con data rate 40 kbps
- 16 canali nella banda 2.450 GHz spazati di 5MHz a 250 kbps





Tipologia nodi

- Full Function Device (FFD)
 - svolge il ruolo di coordinatore o nodo
 - parla con altri nodi o coordinatori
 - inoltra pacchetti (PAN coordinator)
 - Alimentazione a batterie o linea elettrica
- Reduced Function Device (RFD)
 - parla con altri nodi RFD o FFD
 - non può diventare coordinatore
 - alimentato a batterie



Ulteriore classificazione

- **ZigBee Coordinator (ZC)**
 - startup della rete e decisione del relativo PAN-ID
 - permettere l'entrata e l'uscita (join/leave) dalla rete
 - Ruolo di Trust Center in una rete con supporto della sicurezza
- **ZigBee Router (ZR)**
 - Instradare dati per altri dispositivi
 - Permette l'entrata e l'uscita (join/leave) dalla rete
 - Conservare i messaggi destinati ai suoi ZED
- **ZigBee End Device (ZED)**
 - modalità risparmio energetico e polling
 - Costo e complessità limitati, niente supporto rete



Packet Format

4 bytes	1 byte	1 byte		Variable
Preamble	SFD	Frame length (7 bits)	Reserved (1 bit)	Payload (PSU)
SHR		PHR		PHY Payload

- L'LSB è trasmesso e ricevuto per primo.
- La dimensione del pacchetto può raggiungere al massimo 127 byte.



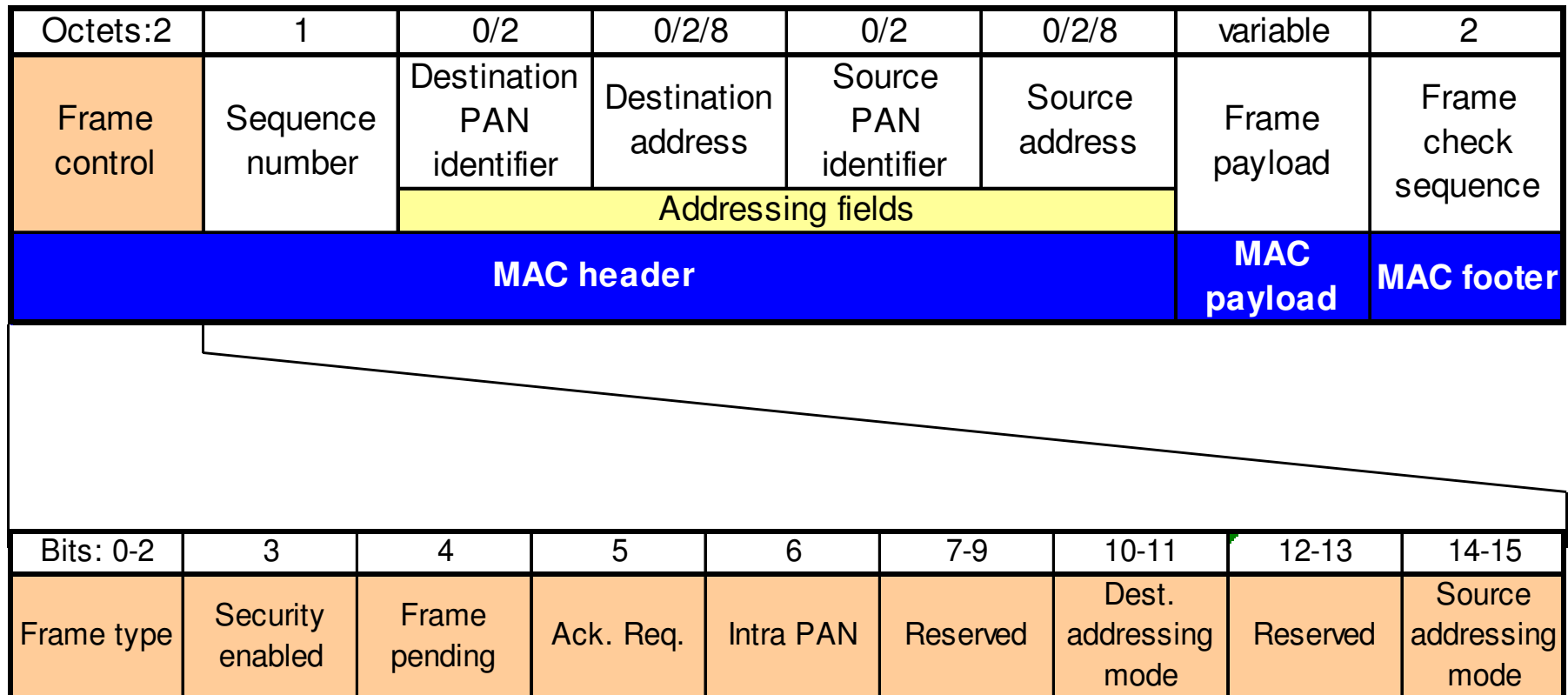
MAC Layer

- Il MAC data service gestisce la trasmissione e la ricezione di MPDU utilizzando i servizi del livello PHY.
- Il MAC management service del coordinatore gestisce i network beacon. È inoltre responsabile di associazione e dissociazione alla PAN, validazione frame, e acknowledgment, fornendo un link affidabile fra due entità MAC.
- Utilizza CSMA/CA per l'accesso e gestisce il Guaranteed Time Slot (GTS) mechanism (rete beacon enabled).
- Fornisce strumenti di supporto alla sicurezza del dispositivo.



MAC Layer Frame Format

- Lo standard IEEE 802.15.4 definisce quattro formati diversi: beacon, data, acknowledgment, e MAC command frame.
- Tutti i formati si basano sul formato MAC generico.



Frame control field



Beacon frame format

Octets:2	1	4 or 10	2	variable	variable	variable	2
Frame control	Beacon sequence number	Source address information	Superframe specification	GTS fields	Pending address fields	Beacon payload	Frame check sequence
MAC header			MAC payload				MAC footer

Bits: 0-3	4-7	8-11	12	13	14	15
Beacon order	Superframe order	Final CAP slot	Battery life extension	Reserved	PAN coordinator	Association permit

- Il beacon frame è trasmesso periodicamente dal coordinatore PAN.
- Fornisce informazioni sulla gestione di rete tramite i campi super frame e GTS (CAP: Contention Access Period).
- Sincronizza i dispositivi di rete, indicando il periodo di comunicazione opportuno.



Altri frame format

- Data frame.

Octets :2	1		Variable	2
Frame Control	Sequence Number	Addressing Field	Data Payload	FCS
MHR			MAC Payload	MFR

- Acknowledgment frame (facoltativo).

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

- Command frame.

Octets:2	1		1	Variable	2
Frame Control	Sequence Number	Addressing Fields	Command Frame Identifier	Command Payload	FCS
MHR			MAC Payload		MFR

- Il *command identifier* specifica l'azione quale *association*, *disassociation*, e la richiesta dati, GTS o *beacon*.



Modalità *Low power*

- Controllo di *Duty-cycle* utilizzando la struttura *superframe*.
- Estensione della durata della batteria del coordinatore.
- Trasmissione indiretta dei dati.
- I dispositivi possono dormire per un periodo prolungato pari ad alcuni *beacon*.
- Permette il controllo dello stato del ricevitore dagli strati superiori.

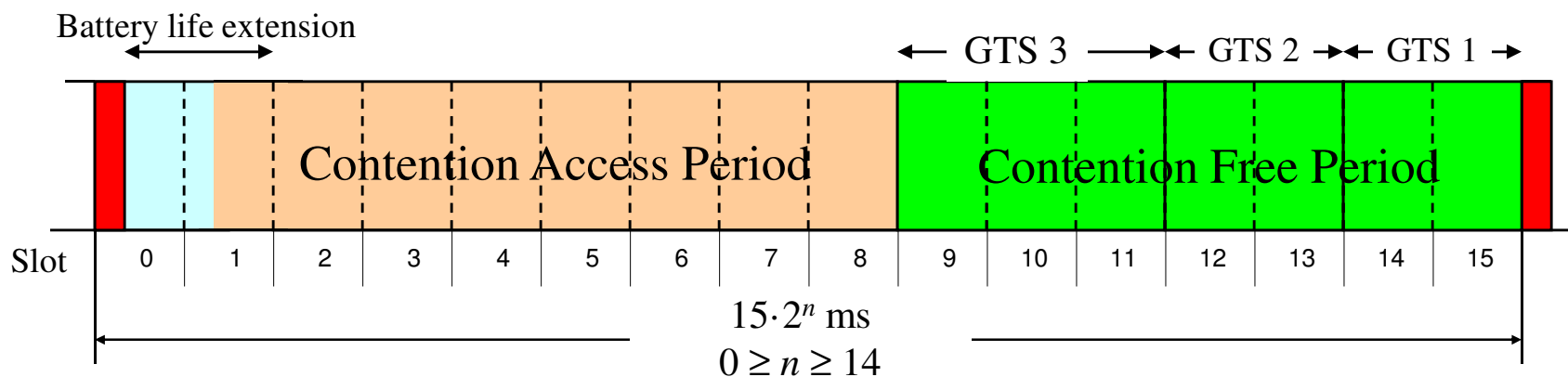


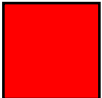
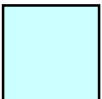
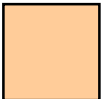
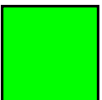
Superframe (1)

- Ogni PAN ha il proprio coordinatore che può decidere se usare la struttura *superframe*. La *superframe* utilizza i *beacon* di rete. Se il coordinatore non desidera utilizzare una struttura *superframe*, sospende la trasmissione *beacon*.
- Se il coordinatore desidera mantenere uno stretto controllo della comunicazione nella PAN e supportare dispositivi a bassa latenza, di solito utilizza la *superframe*.
- Una *superframe* determina un periodo di tempo specifico, limitato da *beacon*.



Superframe (2)

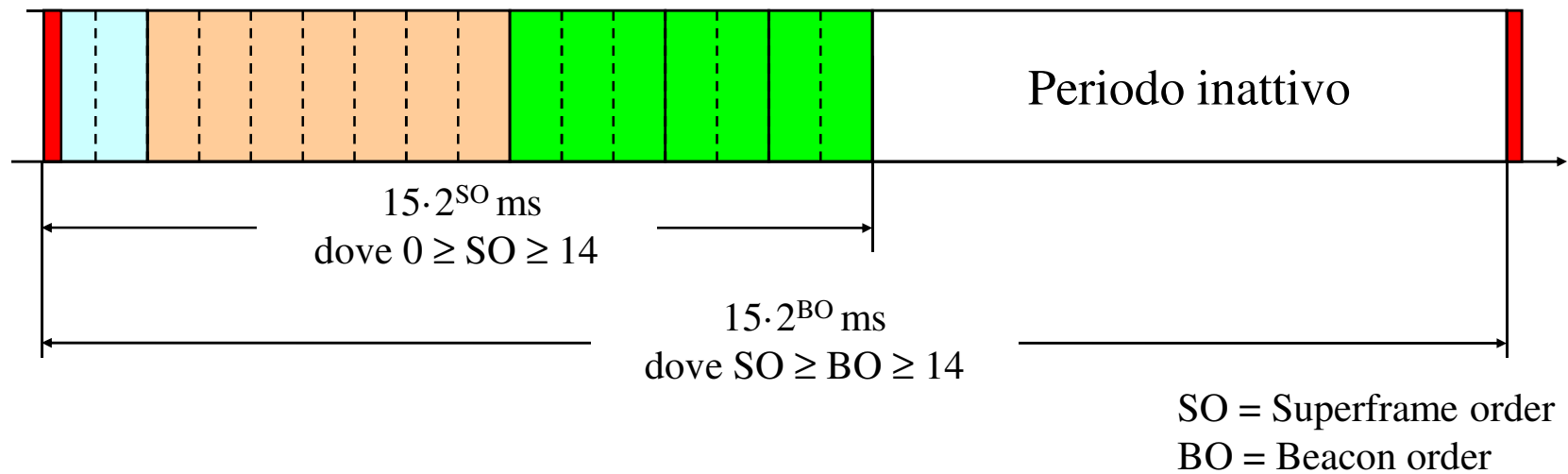


- Network beacon  Trasmesso dal coordinatore PAN. Contiene informazioni di rete, struttura del frame e notifica dei messaggi di nodo in sospenso.
- Beacon extension period  Spazio riservato all'estensione dei beacon a causa dei messaggi di nodo in sospenso.
- Contention period  Accesso libero mediante CSMA-CA.
- Guaranteed Time Slot  Accesso riservato per servizi con garanzia di banda.



Superframe (3)

- Una superframe può avere periodi di inattività.



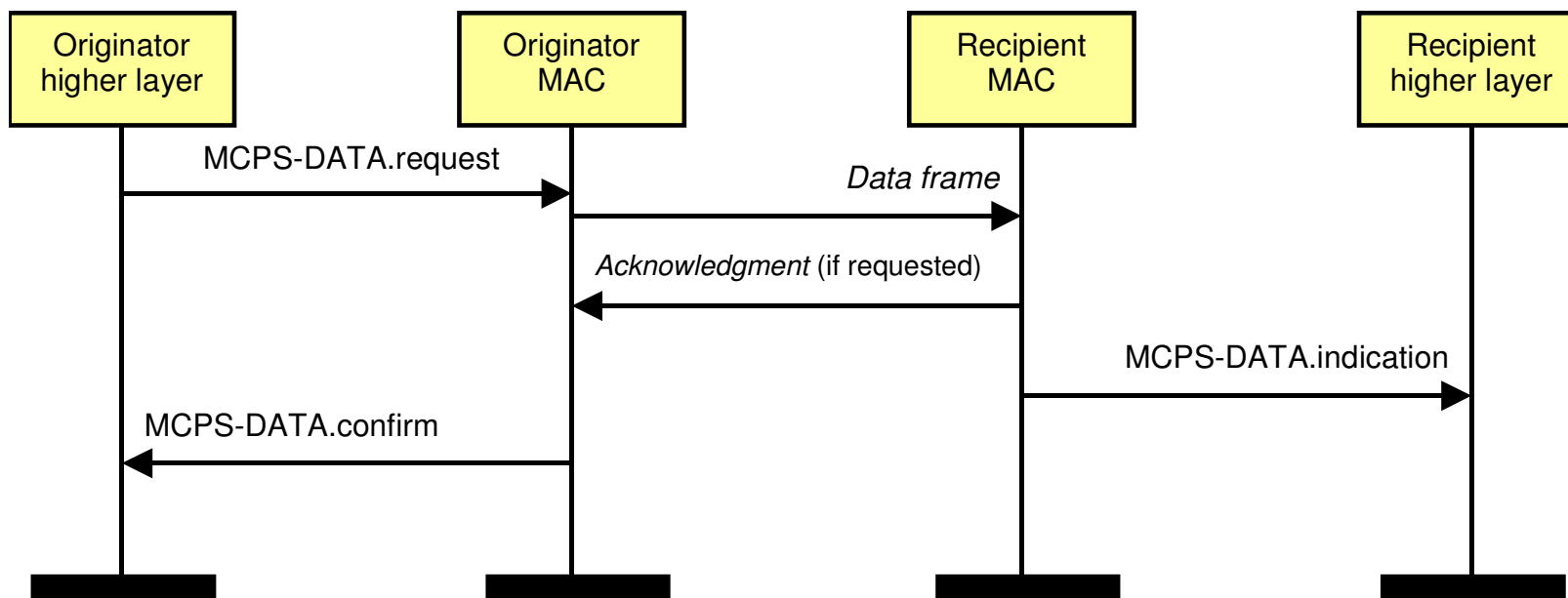


Data transfer

- Tre tipi di data transfer.
 - Data transfer da un dispositivo a un coordinatore di PAN.
 - Data transfer da un coordinatore di PAN a un dispositivo.
 - Peer-to-peer Data Transfer
 - I dispositivi sono liberi di comunicare con qualsiasi altro dispositivo all'interno del loro raggio di comunicazione.
 - In una peer-to-peer PAN i dispositivi possono ricevere costantemente o sincronizzarsi tra loro.
 - Se ricevono costantemente, per trasmettere dati usano la tecnica *un-slotted* CSMA-CA. Nel secondo caso, la sincronizzazione deve essere ottenuta per prima.

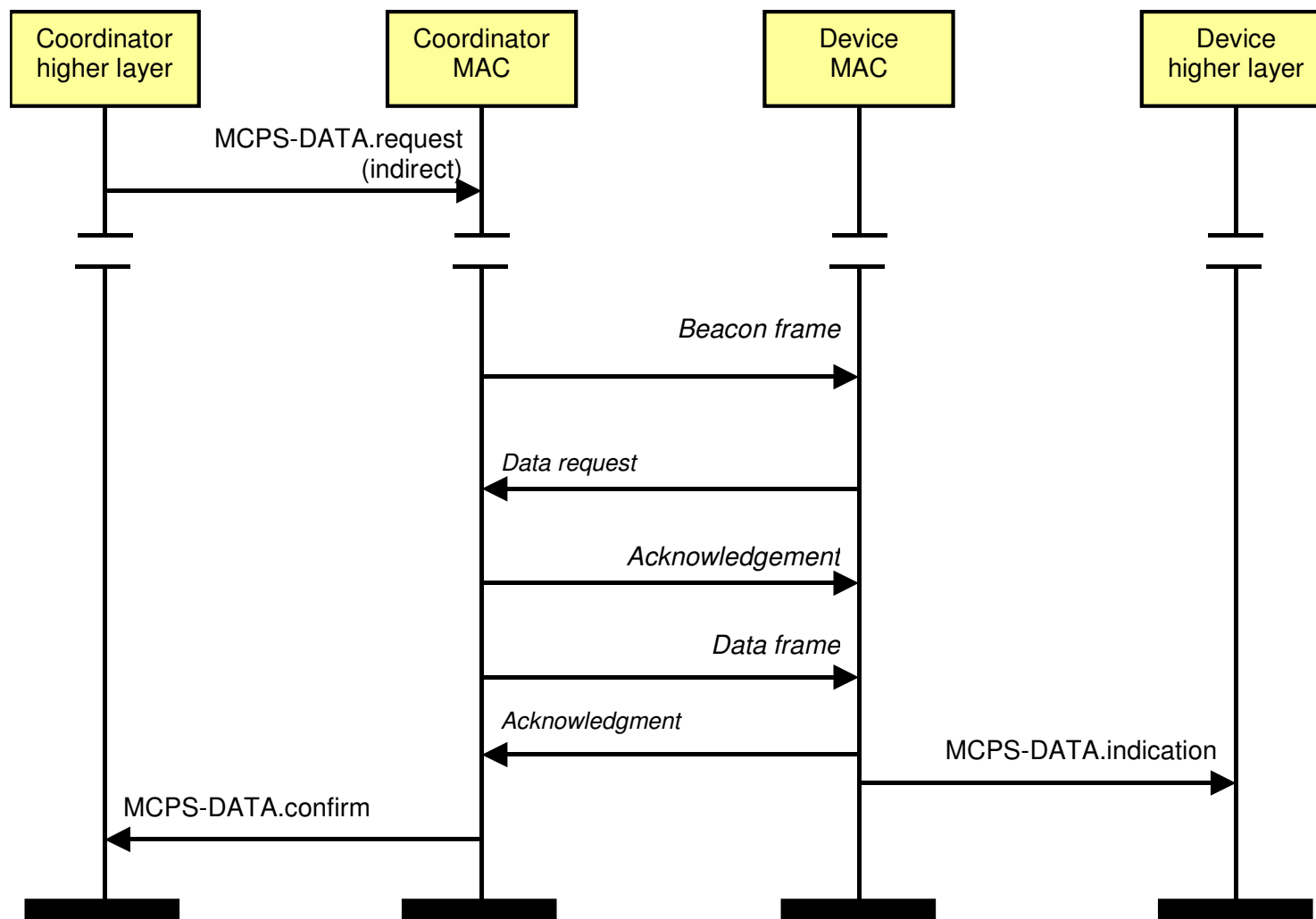
Peer-to-peer data transfer

- Sequenza messaggi



Indirect data transfer

- Sequenza messaggi



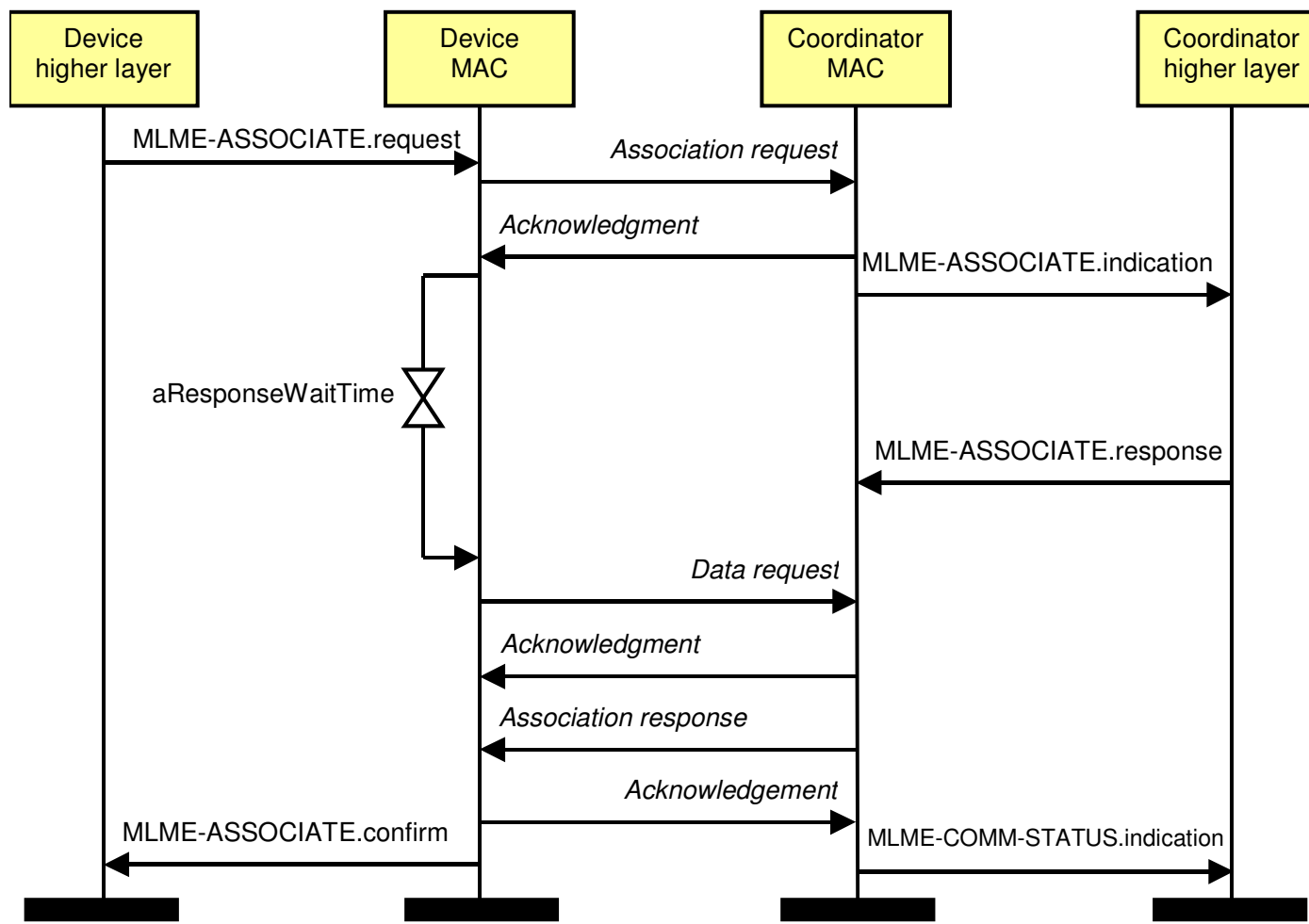


Management Service

- Accesso alle informazioni di base PHY PAN (PIB).
- Association / disassociation.
- Allocazione GTS.
- Message pending
- Node notification
- Network scanning/start
- Network synchronization/search

Association

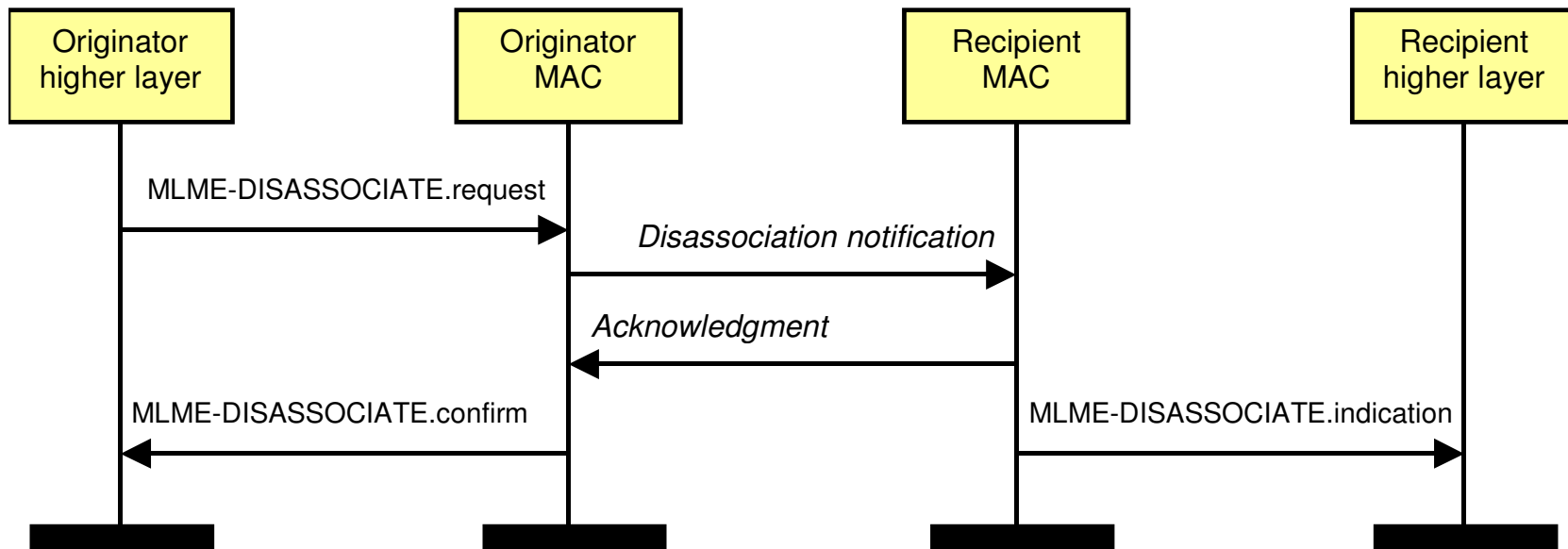
- Sequenza messaggi





Disassociation

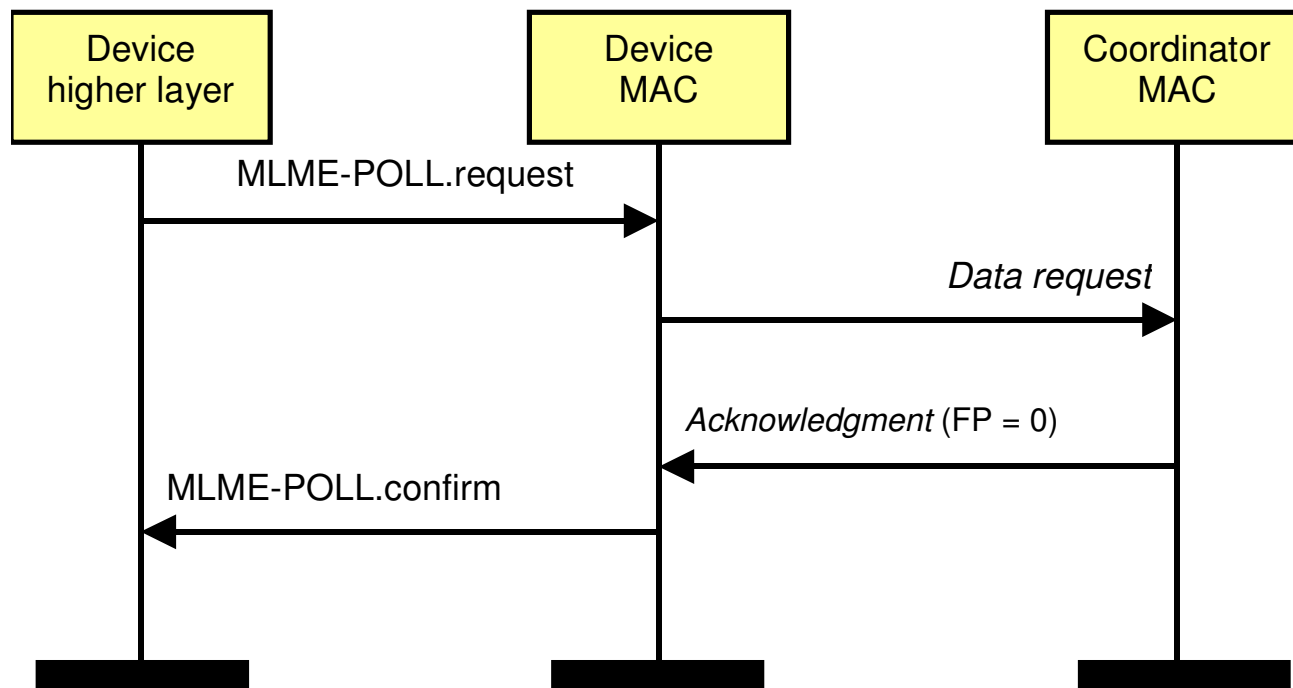
- Sequenza messaggi





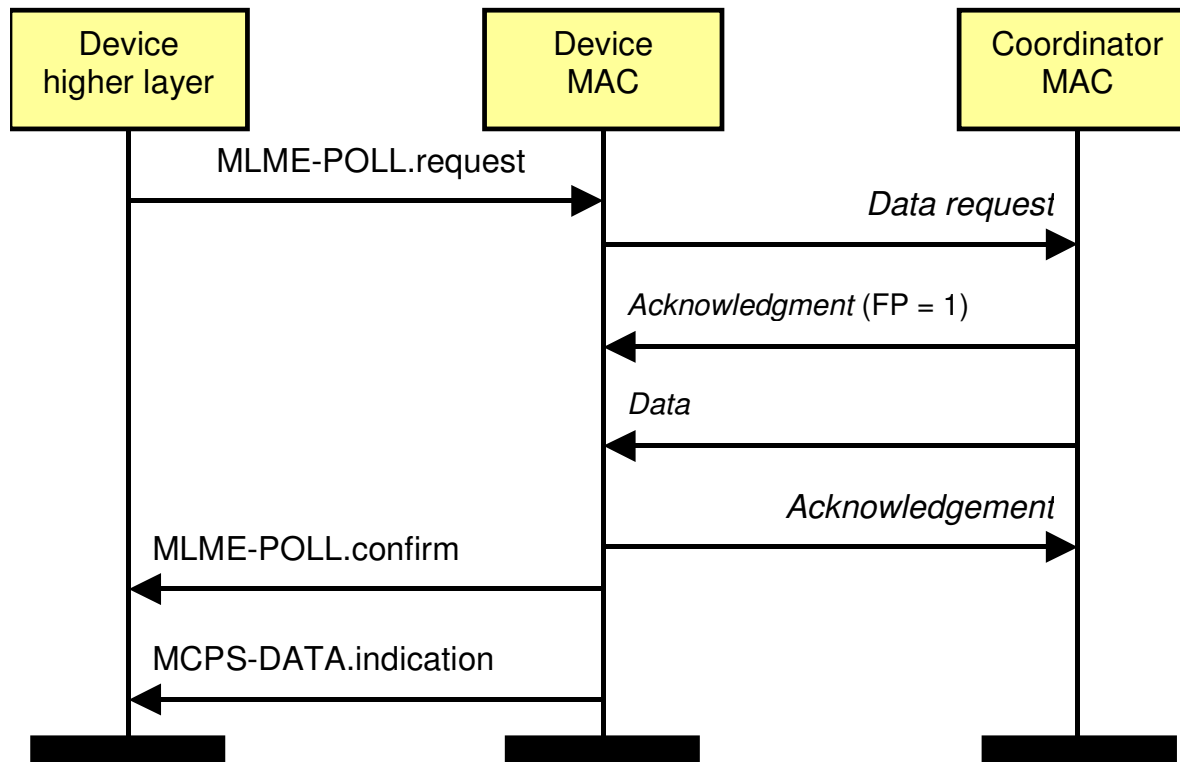
Data Polling

- Sequenza messaggi (No data pending at the coordinator)



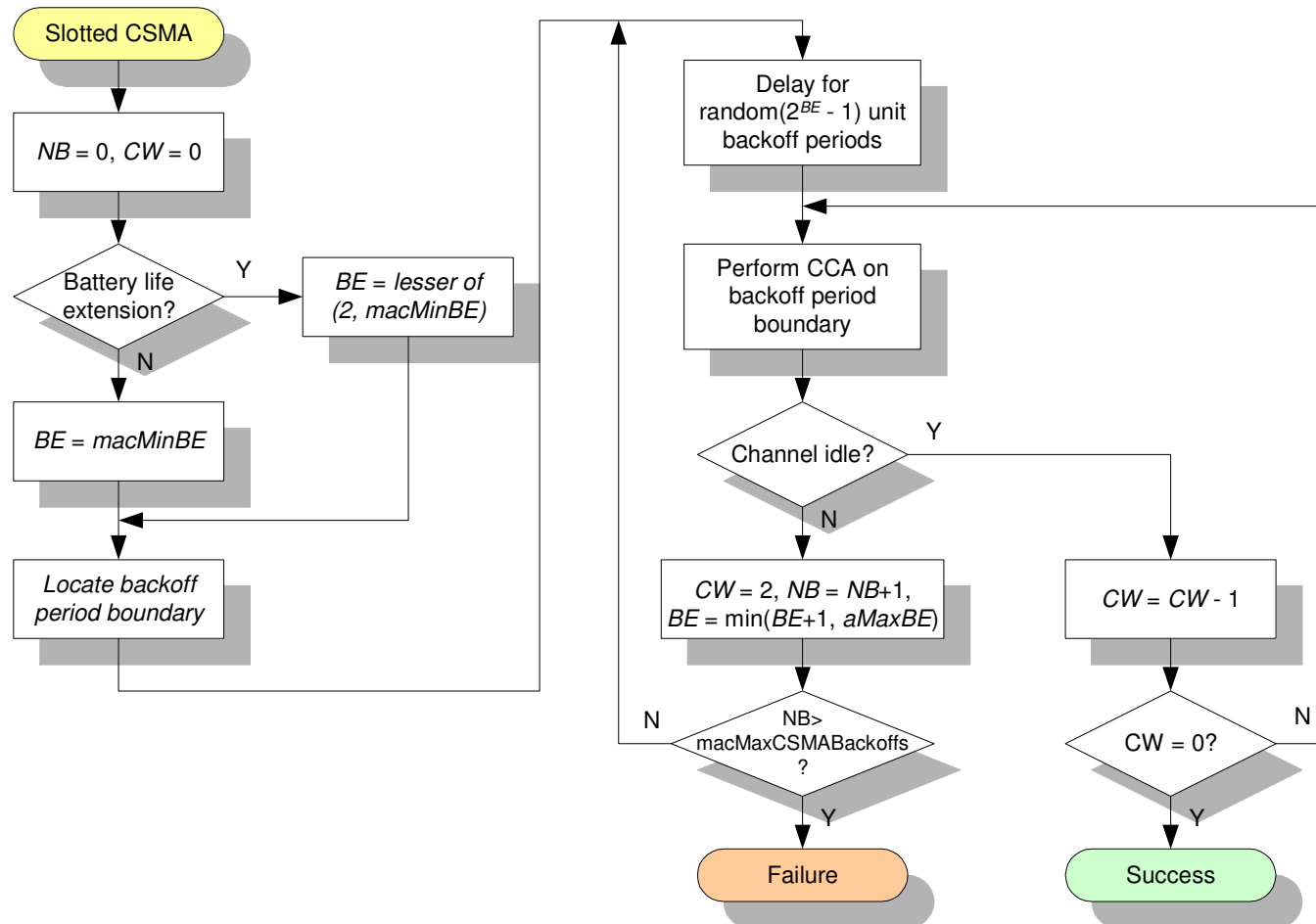
Data Polling

- Sequenza messaggi (Data pending at the coordinator)



Slotted CSMA Procedure

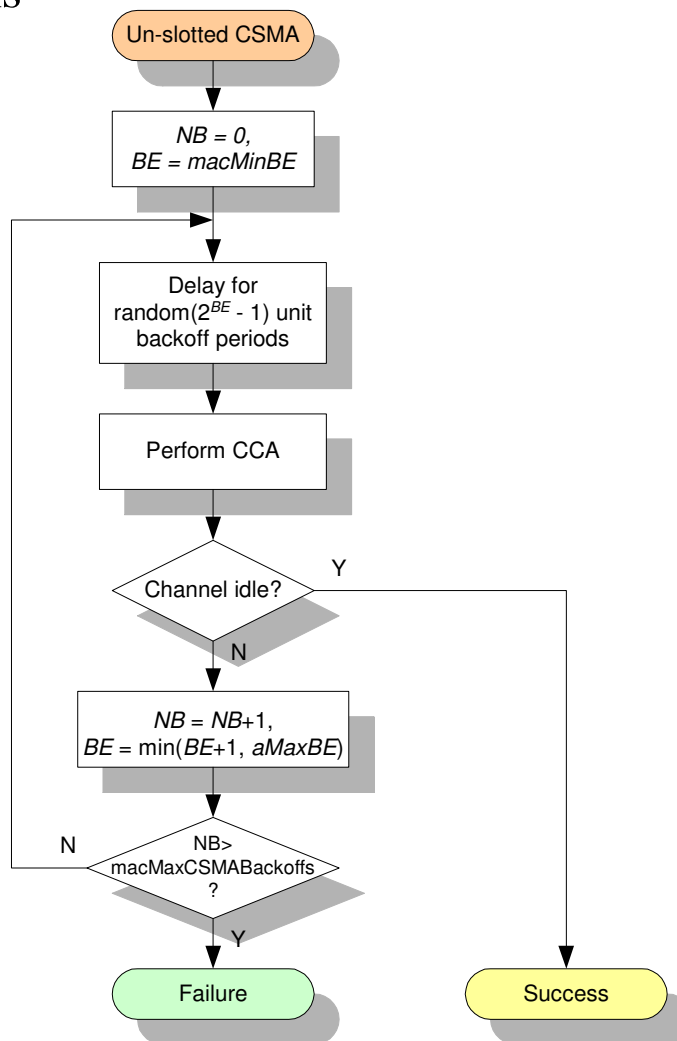
- Beacon enabled networks





Un-slotted CSMA procedure

- Non- beacon networks





Security

- The wireless networks may be used in critical monitoring and control applications all over the world. Any weakness in these systems can have real and direct consequences on efficiency and safety.
- The main safety objectives in WSN are based on the provision of three elements:
 - **Confidentiality**: data carried on the network can not be read by anyone except the intended recipient.
 - **Integrity**: any message received is known to be exactly the message that was sent, without additions, deletions or changes to the content.
 - **Authenticity**: a message that claims to come from a given source actually comes from that source. If time is used as part of the authentication scheme, authenticity also protects the message from being recorded and reproduced later.



Security in IEEE 802.15.4 (1)

- Fornisce una base di sicurezza, inclusa la possibilità di utilizzare la crittografia simmetrica per la crittografia dei dati.
- L'algoritmo utilizzato per la crittografia è AES con una chiave a 128 bit (16 byte) per:
 - **Data security** – eseguita crittografando il data payload.
 - **Data Integrity** – ottenuta mediante un *Message Integrity Code* (MIC) o un *Message Authentication Code* (MAC) che viene aggiunto al messaggio da inviare. Questo codice garantisce l'integrità del MAC header e dei dati del payload. Viene ottenuto cifrando l'IEEE MAC frame mediante la chiave a 128-bit.
- I livelli superiori decidono quando la sicurezza è necessaria.
- I livelli superiori sono generalmente responsabili dell'autenticazione del dispositivo e della gestione delle chiavi.
- ZigBee estende lo standard IEEE 802.15.4 aggiungendo il framework per i servizi di definizione della rete, di sicurezza e di livello applicativo.



Security in IEEE 802.15.4 (2)

- Nel frame IEEE 802.15.4 MAC, l'*Auxiliary Security Header* è abilitato solo se è settato il valore *Security Enabled* del *Frame Control Field*. Questo header speciale ha 3 campi:
- **Security Control** specifica il tipo di protezione fornito dalla rete. È il luogo in cui è impostata la modalità globale di sicurezza. La scelta del livello di sicurezza determina la lunghezza della chiave e ciò che deve essere crittografato. Ciascun livello di sicurezza fornisce un certo grado di crittografia dei frame e controlli di integrità. ZigBee definisce 8 diversi livelli di sicurezza disponibili per Network Layer (NWK) e APS Layer.
- **Frame Counter** è un contatore fornito dalla sorgente del frame corrente al fine di ripetere esattamente lo stesso messaggio.
- **Key Identifier** specifica le informazioni necessarie per determinare il tipo di chiave utilizzata dal nodo per la comunicazione.



Security in IEEE 802.15.4 (3)

802.15.4 Security levels

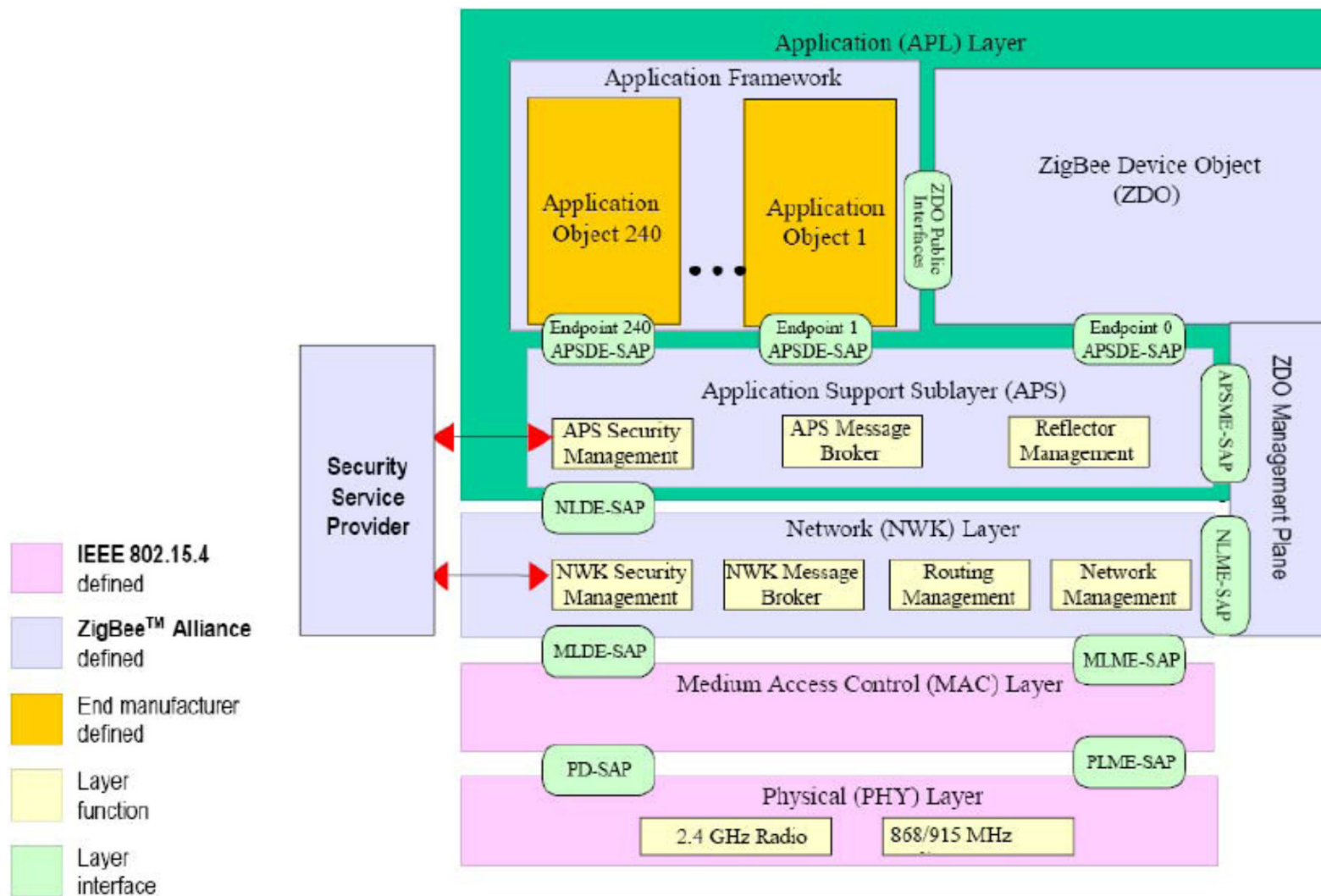
Security Level Identifier	Security Attributes	Data Encryption	Frame Integrity (length of MIC)
0x00	None	OFF	NO (M = 0)
0x01	MIC-32	OFF	YES (M=4)
0x02	MIC-64	OFF	YES (M=8)
0x03	MIC-128	OFF	YES (M=16)
0x04	ENC	ON	NO (M = 0)
0x05	ENC-MIC-32	ON	YES (M=4)
0x06	ENC-MIC-64	ON	YES (M=8)
0x07	ENC-MIC-128	ON	YES (M=16)



Security in IEEE 802.15.4 (4)

- Gli elementi di sicurezza IEEE 802.15.4, quali chiavi, numero di frame e livello di sicurezza, sono archiviati in un file **Access Control List (ACL)**.
- L'ACL viene utilizzato per impedire la partecipazione alla rete di dispositivi non autorizzati. L'ACL è memorizzato nella MAC PAN Information Base (PIB) ed è accessibile e modificato in modo simile ad altri attributi MAC.
- Ogni ACL memorizza l'indirizzo del nodo con cui comunicare, la Security Suite (AEC-CTR, AES-CCM-64, AES-CCM-128, etc), le chiavi:
 - la chiave 128b utilizzata nell'algoritmo AES, il Last Initial Vector (IV) e il Replay Counter (utilizzati dal destinatario come ID messaggio per evitare attacchi di risposta).
- Nonostante le misure di sicurezza fornite da IEEE 802.15.4, la gestione delle chiavi o il tipo di criteri di autenticazione da applicare è demandato a ZigBee.

ZigBee Protocol Stack





ZigBee Application Layer (1)

- È formato dagli ZigBee device objects (ZDOs), dall'Application support sub-layer (APS) e dall'Application Framework.
- **ZigBee Device Objects (ZDO)**
 - Responsabile dell'inizializzazione di APS, Network Layer (NWK) e provider di servizi di sicurezza. Riunisce le informazioni di configurazione dalle applicazioni finali per determinare e implementare l'individuazione di dispositivi e servizi, la gestione della sicurezza (caricamento delle chiavi, creazione delle chiavi, trasporto e autenticazione delle chiavi), la gestione della rete (individuazione della rete, uscire / unirsi a una rete, ripristinare una connessione di rete e creare una rete), associazione, nodo e gestione dei gruppi.
 - ZDO gestisce le politiche di sicurezza e la configurazione di sicurezza di un dispositivo.
 - Gli oggetti elencati come obbligatori nel documento delle specifiche sono implementati in tutti i dispositivi ZigBee.



ZigBee Application Layer (2)

- **Application support sub-layer (APS)**
 - Fornisce un'interfaccia tra NWK e APL. Fornisce servizi per la creazione e il mantenimento di relazioni di sicurezza. I servizi sono forniti tramite l'entità dati APS (APSD: fornisce servizi di trasmissione dati tra entità dell'applicazione) e l'entità di gestione APS (APMSE: fornisce servizi di sicurezza, associazione di dispositivi e gestione dei gruppi).
 - Il livello APS consente alla sicurezza dei frame di basarsi sulle chiavi di collegamento o sulla chiave di rete. Il livello APS è responsabile delle fasi di elaborazione necessarie per trasmettere in modo sicuro i frame in uscita, ricevere in modo sicuro i frame in entrata e stabilire e gestire in modo sicuro le chiavi crittografiche. I livelli superiori controllano la gestione delle chiavi crittografiche emettendo primitive al livello APS.
- **Application Framework**
 - Oggetti applicazione definiti dal produttore. Definisce i profili dell'applicazione (tipo di messaggi, formati dei messaggi e azioni di elaborazione che consentono agli sviluppatori di creare un'applicazione distribuita interoperabile che impiega entità dell'applicazione che risiedono su dispositivi distinti).



ZigBee Network Layer (NWK)

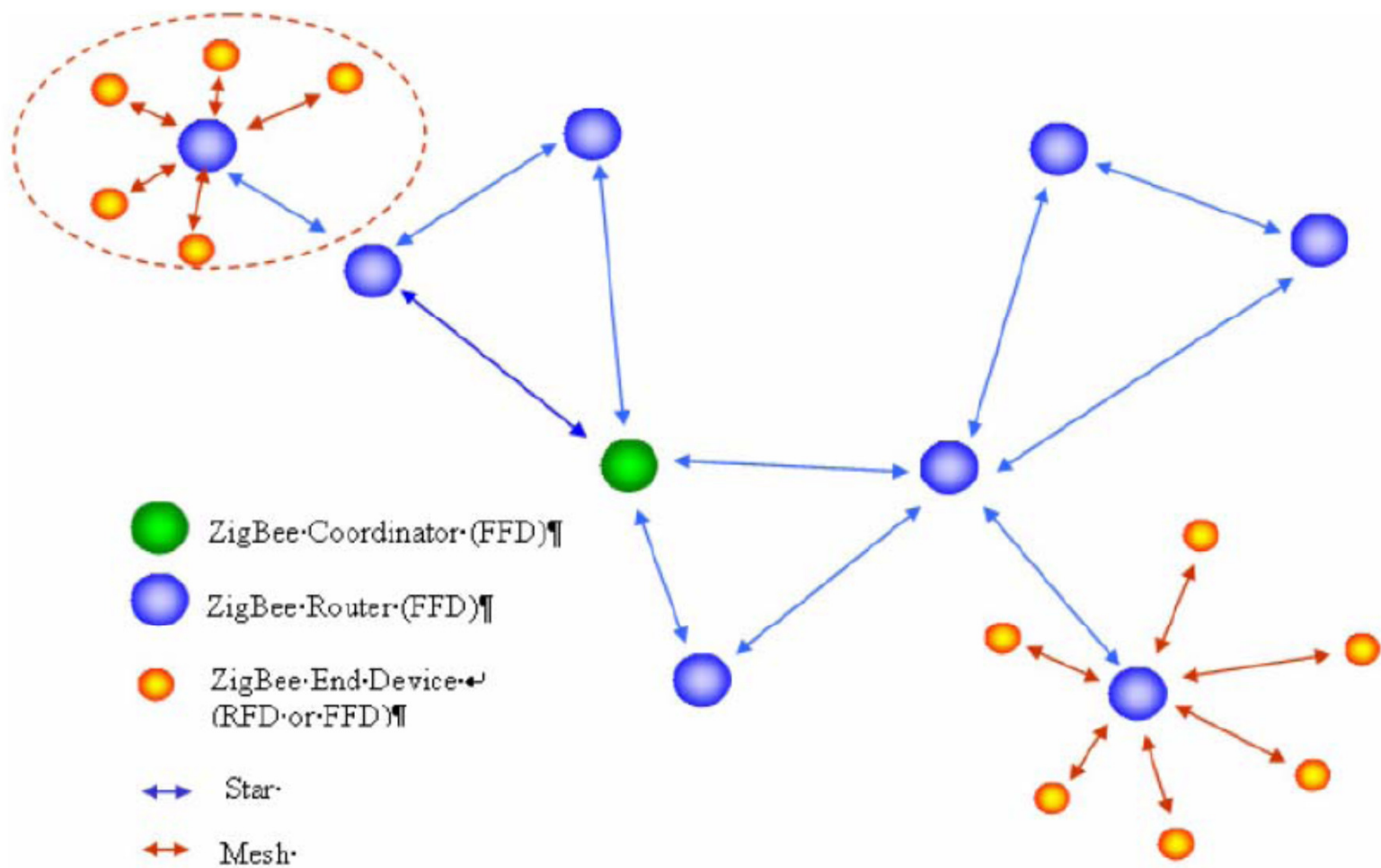
- Lo standard ZigBee utilizza lo schema di indirizzamento di IEEE 802.15.4, adoperando indirizzi standard a 64 bit e indirizzi brevi a 16 bit.
- Compiti del Network layer.
 - Attivazione di una nuova rete.
 - Configurazione di dispositivi nuovi per la rete, assegnazione degli indirizzi, sincronizzazione della rete
 - Sicurezza di frame
 - Il livello NWK è responsabile delle fasi di elaborazione necessarie per trasmettere in modo sicuro i frame in uscita e ricevere in modo sicuro i frame in arrivo. Il meccanismo di protezione del frame del livello NWK utilizza Advanced Encryption Standard (AES) e CCM * (contatore avanzato con modalità operativa CBC-MAC) per autenticazione e riservatezza
 - Intradamento



Topologie Zig Bee

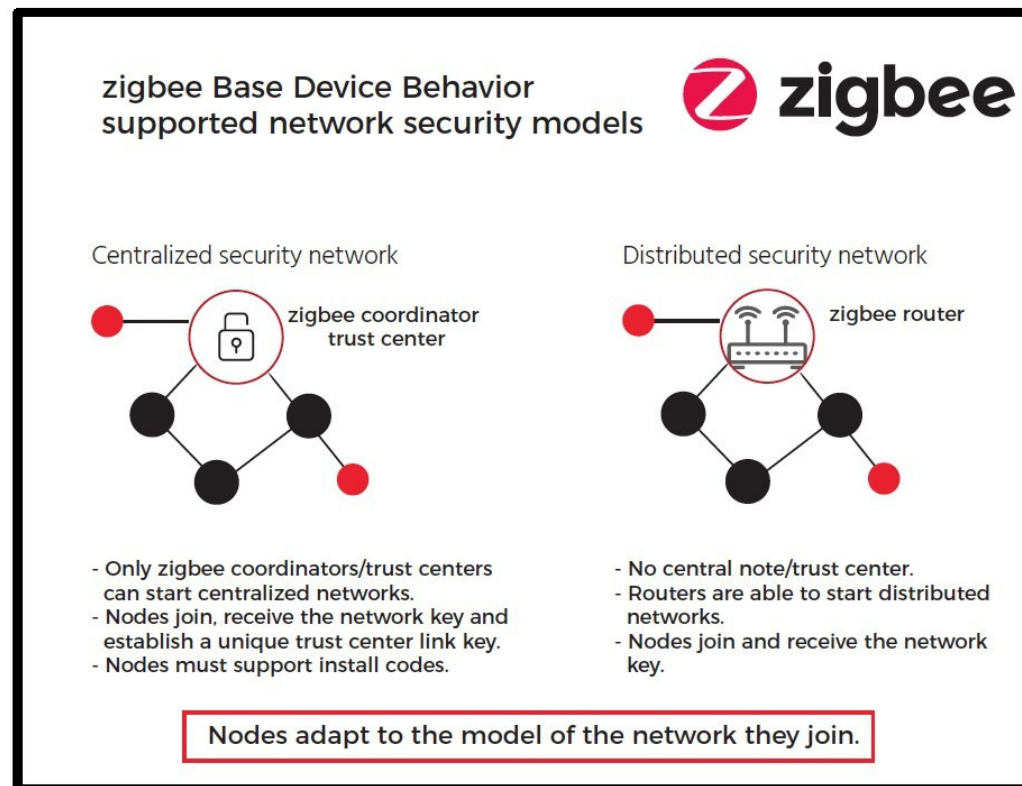
- Zig Bee adotta una topologia a stella o di tipo peer-to-peer.
- La topologia peer-to-peer opera in modalità mesh, multi-hop networking.
- Qualsiasi dispositivo nella topologia peer-to-peer può comunicare con qualsiasi altro dispositivo nel suo raggio di comunicazione; tuttavia, questa topologia ha anche un coordinatore PAN.
- Tutti i dispositivi in una LR-WPAN (Low-Rate Wireless Personal Area Network) hanno un indirizzo univoco a 64 bit. Questo o un indirizzo breve, assegnato dal coordinatore PAN, può essere utilizzato all'interno di una PAN.
- Ogni PAN ha un identificatore univoco. La combinazione dell'identificatore PAN e degli indirizzi brevi consente la comunicazione tra diverse PAN.

Topologie ZigBee



ZigBee Security

- Lo standard ZigBee supporta due tipi di modelli di sicurezza, come mostrato in figura. Tali modelli differiscono per il modo in cui ammettono nuovi dispositivi nella rete e per come proteggono i messaggi sulla rete.





ZigBee Centralized Security

- **Trust Center:** è un'applicazione che viene eseguita sul dispositivo considerato affidabile da altri dispositivi all'interno della rete ZigBee per distribuire chiavi ai fini della gestione della configurazione della rete e dell'applicazione.
- Tutti i membri della rete riconoscono un solo Trust Center e esiste un solo Trust Center in ciascuna rete protetta.
- ZigBee CS è configurato per funzionare in modalità di sicurezza standard o elevata, e può essere utilizzato per aiutare a stabilire chiavi di applicazione end-to-end inviando direttamente le chiavi di collegamento (ovvero la funzionalità di deposito delle chiavi) o inviando le chiavi master. Queste chiavi sono generate in modo casuale.



Standard Mode

- Progettato per applicazioni residenziali.
- Il Trust Center mantiene un elenco di dispositivi, chiavi master, chiavi di collegamento e chiavi di rete con tutti i dispositivi della rete.
- Mantiene una chiave di rete standard e controlla le politiche di accesso alla rete.
- Ogni dispositivo che si unisce alla rete in modo sicuro deve disporre di una chiave di collegamento globale o di una chiave di collegamento univoca a seconda dell'applicazione in uso. È necessario che il Trust Center abbia una conoscenza preliminare del valore della chiave di collegamento e del tipo (globale o unico) al fine di unire in modo sicuro il dispositivo alla rete.
 - Una chiave di collegamento globale ha il vantaggio che la memoria richiesta dal Trust Center non aumenta con il numero di dispositivi nella rete.
 - Una chiave di collegamento univoca ha il vantaggio di essere unica per ciascun dispositivo sulla rete e le comunicazioni delle applicazioni possono essere protette da altri dispositivi sulla rete.
- Entrambi i tipi di chiavi possono essere utilizzati sulla rete, ma un dispositivo deve avere un solo tipo in uso.



High Security Mode

- Progettato per applicazioni commerciali ad alta sicurezza.
- Il Trust Center mantiene un elenco di dispositivi, chiavi master, chiavi di collegamento e chiavi di rete necessarie per controllare e applicare le politiche di aggiornamento delle chiavi di rete e accesso alla rete.
- Richiede inoltre l'implementazione della inizializzazione delle chiavi mediante SKKE (*Symmetric-Key Key Exchange*) e l'autenticazione dell'entità.



ZigBee Distributed Security

- È semplice, ma meno sicuro.
- Questo modello supporta solo router ed end-device.
- I router formano la rete distribuita e sono responsabili della registrazione di altri router ed end-device.
- I router rilasciano le chiavi di rete (utilizzate per crittografare i messaggi) ai router e agli end-device appena aggiunti.
- Tutti i nodi della rete utilizzano la stessa chiave di rete per crittografare i messaggi.
- Inoltre, tutti i nodi sono preconfigurati con una chiave di collegamento (utilizzata per crittografare la chiave di rete) prima di essere registrati nella rete.

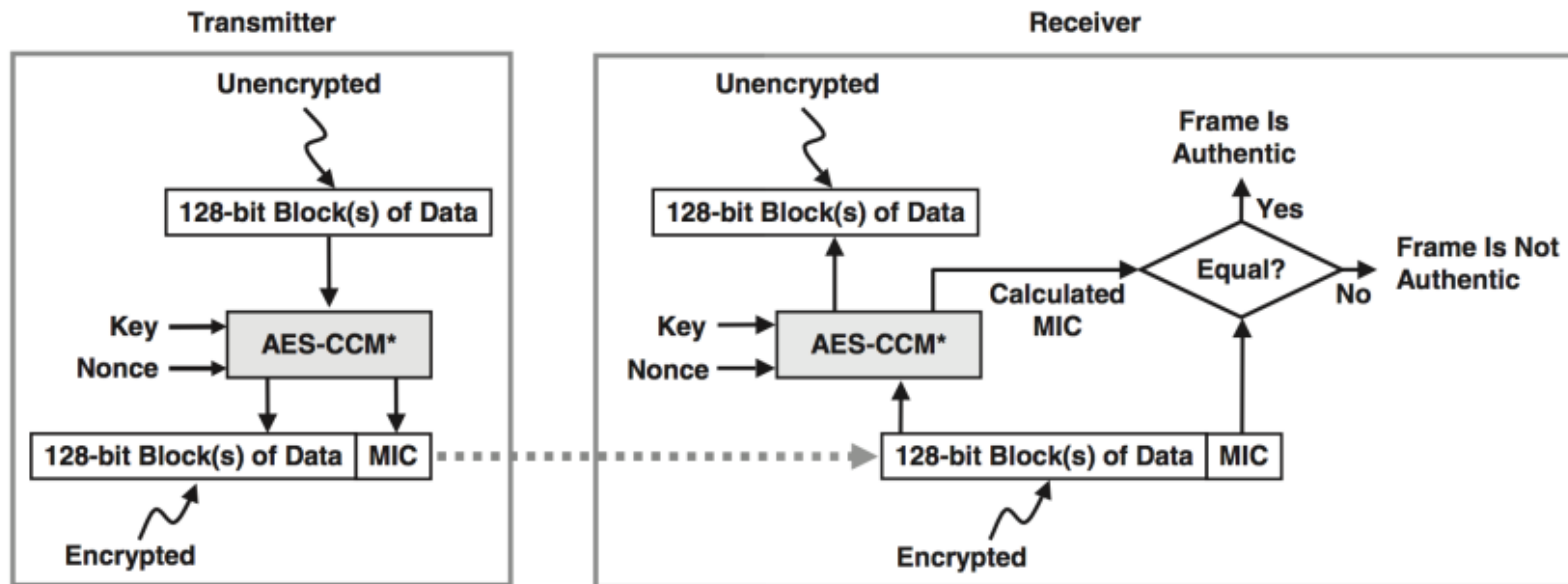


ZigBee Encryption/Decryption

- I frame ZigBee possono essere opzionalmente protetti con la suite di sicurezza AES-CCM * per garantire la riservatezza, l'autenticazione e l'integrità dei dati. AES-CCM * è una variante minore di AES (Advanced Encryption Standard) con una modalità CCM modificata (Counter con CBC-MAC).
 - Sul lato del trasmettitore, il testo in chiaro sotto forma di blocchi di dati a 128 bit entra nell'AES-CCM *. La responsabilità di AES-CCM * è di crittografare i dati e generare un MIC (*Message Integrity Code*) associato, che viene inviato al ricevitore insieme al frame.
 - Il ricevitore utilizza AES-CCM * per decifrare i dati e generare il proprio MIC dal frame ricevuto da confrontare con il MIC ricevuto (integrità dei dati).
 - Un MIC offre una maggiore garanzia di autenticità rispetto al CRC. Il MIC generato da CCM * rileva modifiche intenzionali e non autorizzate dei dati nonché errori accidentali.



ZigBee Encryption/Decryption (2)





Relay protection

- Ogni nodo nella rete ZigBee contiene un contatore di frame a 32 bit che viene incrementato ad ogni trasmissione di pacchetti.
- Ciascun nodo tiene inoltre traccia del precedente contatore di frame a 32 bit di ciascun dispositivo (nodo) a cui è collegato.
- Se un nodo riceve un pacchetto da un nodo vicino con lo stesso valore o un valore minore del contatore di frame rispetto a quello precedentemente ricevuto, il pacchetto viene eliminato.
- Il valore massimo che un contatore di frame può avere è pari a 0xFFFFFFFF. Se viene raggiunto il valore massimo, non è possibile effettuare alcuna trasmissione.
- L'unica volta che il contatore dei frame viene reimpostato su 0 è quando la chiave di rete viene aggiornata.
 - Periodicamente o quando richiesto, il Trust Center genera una nuova chiave di rete e la distribuisce in tutta la rete crittografandola con la vecchia chiave di rete. Tutti i dispositivi continuano a conservare la vecchia chiave di rete per un breve periodo di tempo dopo l'aggiornamento fino a quando tutti i dispositivi sulla rete non passano alla nuova chiave di rete. Inoltre, i dispositivi, alla ricezione della nuova chiave di rete, inizializzano il contatore dei frame a zero.



Autenticazione del dispositivo

- È l'atto di confermare un nuovo dispositivo che si unisce alla rete come autentico. Il nuovo dispositivo deve essere in grado di ricevere una chiave di rete e impostare gli attributi corretti entro un determinato periodo per essere considerato autentificato.
- L'autenticazione del dispositivo viene eseguita dal Trust Center.
 - In **modalità residenziale** il Trust Center invia la chiave di rete su un collegamento non protetto, causando un momento di vulnerabilità.
 - Il nuovo dispositivo utilizza l'indirizzo di origine del messaggio ricevuto per impostare l'indirizzo del Trust Center. Il nuovo dispositivo viene quindi considerato autentificato per la modalità residenziale.
 - In **modalità commerciale**, una chiave master viene inviata non protetta.
 - Dopo che il nuovo dispositivo riceve la chiave master, il Trust Center e il nuovo dispositivo avviano il *key establishment protocol* (SKKE).
 - Il nuovo dispositivo ha un tempo limitato per stabilire una chiave di collegamento con il Trust Center, altrimenti il nuovo dispositivo deve lasciare la rete e riprovare l'associazione e la procedura di autenticazione.
 - Quando la nuova chiave di collegamento viene confermata, il Trust Center invierà la chiave di rete al nuovo dispositivo tramite una connessione protetta. Il dispositivo di giunzione ora è considerato autentificato per la modalità commerciale.



Ulteriori considerazioni: affidabilità (1)

- Per aumentare l'affidabilità, è necessario fornire alcuni livelli di ridondanza, come la ridondanza spaziale (in modo che i dispositivi siano in grado di comunicare con più di un partner, in modo da evitare interruzioni di rete in caso di guasto di un singolo sensore).
- Lo standard IEEE 802.15.4e è stato definito per utilizzare bassi livelli di potenza ricevuta o gestire perdita di segnale nelle reti industriali di dispositivi connessi a Internet (IPv6) con risorse protette, in base allo standard IEEE 802.15.4, dove il MAC opera in modalità Time Slotted Channel Hopping (TSCH).
- Il nuovo MAC è stato progettato per soddisfare i requisiti delle applicazioni industriali, riducendo l'ascolto inattivo e migliorando l'affidabilità in presenza di interferenze a banda stretta e fading multi-percorso.



Ulteriori considerazioni: affidabilità (2)

- Inoltre, Internet Engineering Task Force (IETF) ha formato un gruppo di lavoro chiamato "IPv6 sulla modalità TSCH di IEEE 802.15.4e" (6TiSCH) [1, 2], per definire un protocollo sicuro per applicazioni industriali basato su IEEE 802.15.4.
- Il gruppo di lavoro IETF 6TiSCH mira a consentire un'interazione efficace tra IEEE 802.15.4, uno standard a livello di collegamento che offre prestazioni industriali in termini di affidabilità e consumo di energia, e Internet.
- L'obiettivo è consentire un corretto equilibrio tra throughput (quantità di dati scambiati), latenza e consumo di energia, in base ai requisiti dell'applicazione, mantenendo un'altissima affidabilità.

[1] D. Dujovne, T. Watteyne, X. Vilajosana, and P. Thubert, "6TiSCH: Deterministic IP-Enabled Industrial Internet (of Things)", IEEE Communications Magazine, Communications Standards Supplement, December 2014, pp. 36-41.

[2] P. Thubert, M. R. Palattella, and T. Engel, "6TiSCH Centralized Scheduling: when SDN Meet IoT", 2015 IEEE Conference on Standards for Communications and Networking (CSCN), pp. 42-47.



Ulteriori considerazioni: safety e security

- È essenziale disporre di un esperto del sistema di sicurezza durante la progettazione e la fase di gestione della rete, assicurandosi che la progettazione e l'uso sicuro della rete e dei dispositivi siano una priorità.
- È necessario rendere aggiornabile il software dei dispositivi collegati in rete e assicurarsi che l'aggiornamento avvenga in condizioni che non creino problemi al funzionamento del dispositivo (evitare gli aggiornamenti quando il dispositivo esegue operazioni critiche). L'aggiornamento può essere essenziale per rimediare alle falle di sicurezza rilevate quando il sistema è già stato installato.
- Alcuni esempi di protocolli di sicurezza ben progettati in una WN basata su IEEE 802.15.4 includono il protocollo di automazione industriale Wireless HART [1], che è stato sottoposto a una revisione approfondita da parte di esperti di sicurezza.

[1] M. Nixon, “A Comparison of WirelessHART™ and ISA100.11a, White Paper, Sept 23, 2012.



UWB (IEEE802.15.3 – WiMedia Alliance)

Definizione: tecnica di trasmissione che utilizza una banda di almeno 500 MHz oppure non inferiore al 20% della frequenza di centro banda.

Caratteristiche:

- segnali di durata ridotta (ordine dei nano e dei pico secondi)
 - densità spettrale bassa (non interferiscono con altri segnali)
- sensibilità alle interferenze
 - bassa per il multipath
 - alta per l'interferenza intersimbolica
- utilizzo :
 - data rate alti, range ridotti – trasferimento dati multimediali
 - data rate bassi, range estesi – radar, localizzazione (*)



Tabella comparativa (I)

	Bluetooth	UWB	ZigBee	Wi-Fi
IEEE standard	802.15.1	803.15.3	802.15.4	802.11
Frequenze	2.4 GHz	3.1-10.6 GHz	869/915 MHz 2.4 GHz	2.4 GHz 5 GHz
Applicazioni	Connessione fra dispositivi	Multimedia W-PAN	Monitoraggio Automazione Rete di sensori	LAN Accesso a Internet
Tasso massimo	3 Mbit/s	110 Mbit/s	250 kbit/s	54 Mbit/s 7 Gbit/s
Distanza nominale	10 m	10 m	10-100 m	100 m
Potenza trasmissione	0-10 dBm	-41.3 dBm/MHz	(-25)-0 dBm	15-20 dBm
Banda canale	1-2 MHz	500 MHz 7.5 GHz	0.3, 0.6, 2 MHz	20 MHz 160 MHz



Tabella comparativa (II)

	Bluetooth	UWB	ZigBee	Wi-Fi
Modulazione	GFSK	BPSK, QPSK	BPSK, O-QPSK	BPSK M-QAM
Topologia elementare	Piconet	Piconet	Stella	BSS
Estensioni	Scatternet	Peer to peer	Albero, mesh	ESS
Nodi	8 attivi, 255 in park mode	8	migliaia	Non limitato
Cifratura	E0	AES	AES	RC4. AES
Integrità	16 bit CRC	32 bit CRC	16 bit CRC MIC	32 bit CRC



Radio Frequency Identification (RFID)

- La tecnologia RFID consente di identificare in modo univoco i dispositivi utilizzando le comunicazioni wireless.
- Un sistema RFID comprende un'etichetta (tag), un lettore, e un'antenna.
- Il lettore invia un segnale di interrogazione al tag attraverso l'antenna, e il tag risponde con le sue informazioni uniche.
- Le etichette RFID possono essere attive o passive.
- Le etichette attive contengono una sorgente di energia e possono trasmettere fino a 100 metri.
- Le etichette passive vengono alimentate dal segnale interrogante e possono trasmettere fino a 25 m.
- Frequenze utilizzate
 - Low Frequency (LF) 125 -134 kHz (range: 10 cm).
 - High Frequency (HF) 13.56 MHz (range: 30 cm).
 - Ultra High Frequency (UHF) 856 MHz to 960 MHz (range: 100 m).



Near-Field communication (NFC)

- Dispositivi di tipo RFID, che operano nell'intervallo di frequenze HF(13.56 MHz), e possono svolgere sia il ruolo di etichetta che di lettore (scambio bi-direzionale, peer to peer, di informazioni).
- Tecnologia gestita dall'NFC Forum.
- Basata sugli standard ISO 15693, 18092.
- Opera a brevissima distanza (alcuni centimetri).
- Velocità di trasmissione sino a 424 kbit/s.

ANT



- Sistema proprietario, opera su brevi distanze (fino a 30 m).
<http://www.thisisant.com/developer/resources/downloads>
- Il transceiver ANT lavora alla frequenza di 2.4 GHz all'interno della banda ISM, con la possibilità di diverse modalità di comunicazione
- Esistono diverse modalità di comunicazione (Broadcast , Acknowledged e Burst).
- Parametri di configurazione del canale:
 - Channel Type: Bidirectional slave, Bidirectional master, Shared bidirectional slave, Slave receive only, Master transmit only.
 - RF Frequency: 78 canali da 1 MHz, da 2403 a 2480 MHz.
 - Channel Period: accesso TDMA. All'interno di un Channel period possono essere presenti 100 o più time-slot, così da dare la possibilità ad un canale di essere condiviso da più trasmettitori .
 - Network: specifica la topologia di rete (broadcast, Peer to peer, Secure authenticated, Star, Shared uni-directional, Shared bi-directional, Ad-hoc, Scanning node, Mesh).

LoRa

- LoRa (Long Range) Wan è una tecnologia proprietaria, definita e controllata da LoRa Alliance.
- Adotta una tecnica di modulazione a spettro espanso derivata dalla tecnologia chirp spread spectrum (CSS).
- Particolarmente adatto per comunicazioni a lungo raggio, LoRa utilizza bande di radiofrequenza sub-gigahertz senza licenza come 169 MHz, 433 MHz, 868 MHz (Europa) e 915 MHz (Nord America). Le bande basse consentono velocità dati da 0.3 kbps a 50 kbps.
- Altre caratteristiche:
 - Low Power WAN con topologia a stella.
 - Distanza: 2-5 km in area urbana / 15 km in area sub-urbana o in campo aperto.
 - Potenza di trasmissione: da -2dBm a 20 dBm.
 - Sicurezza: AES 128-bit.

