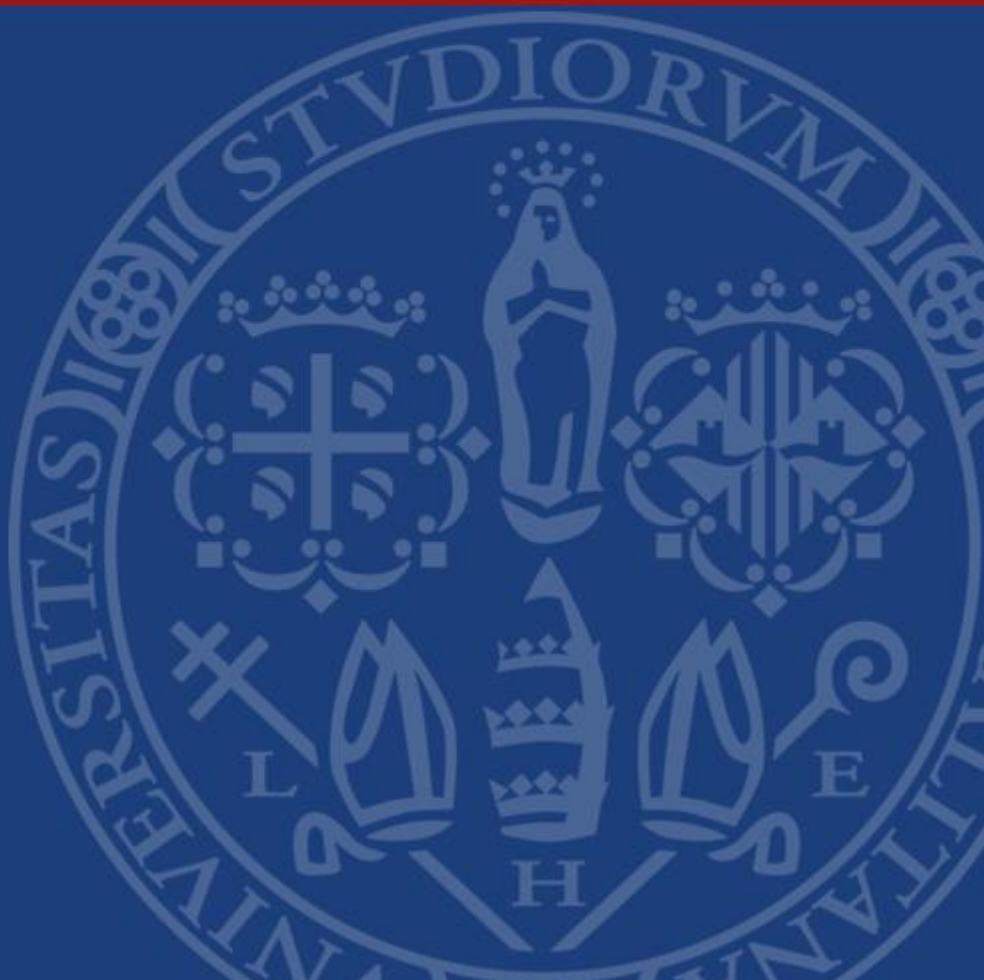
CORSO DI TECNOLOGIE D'ACCESSO



ZigBee

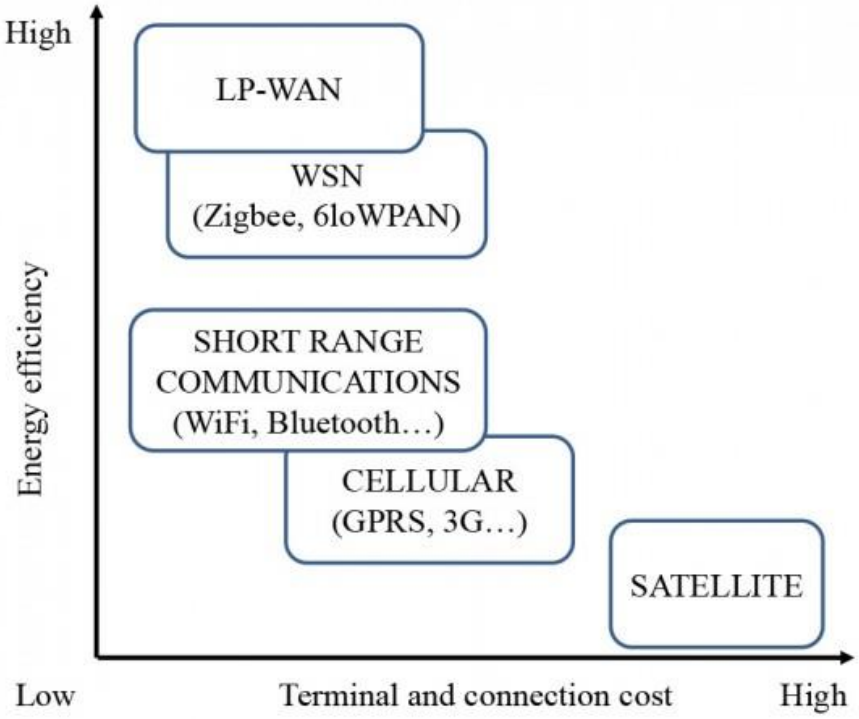
Introduzione

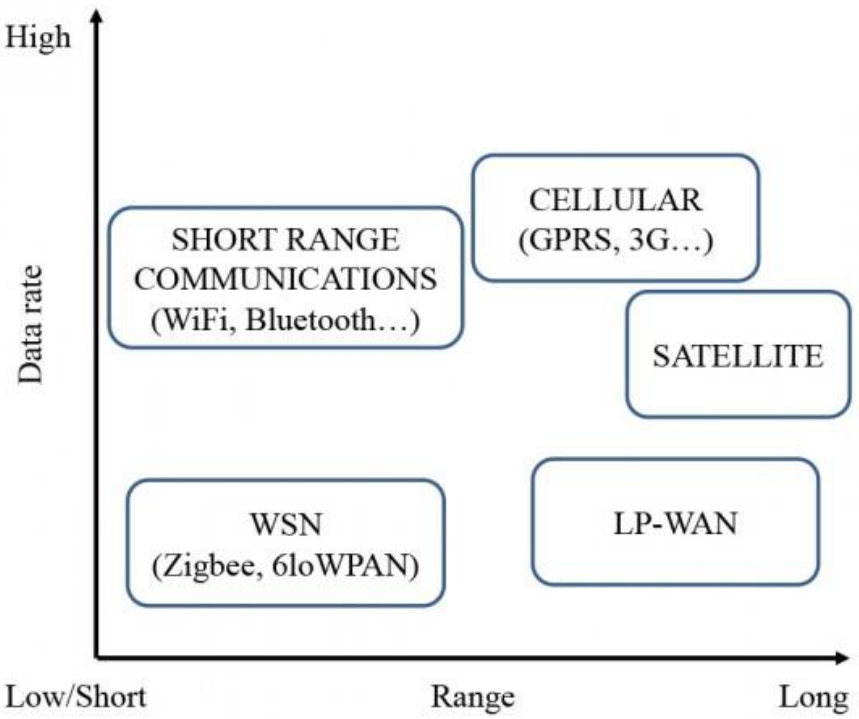
- ✓ Siamo in un'epoca in cui il settore del networking senza fili punta a capacità trasmissive pari a quelle dei tradizionali cavi Ethernet ed a coperture dell'ordine dei chilometri

- ✓ Può quindi sembrare strana la scommessa di lanciare uno standard che punti ad avere una copertura a corto raggio e una ridotta capacità trasmissiva

- ✓ Tale standard può trovare applicazione in settori dove prima era impensabile ed economicamente sconveniente usare dispositivi senza fili

Introduzione





ZigBee Alliance

- ✓ La ZigBee Alliance è un'associazione di più di 200 aziende che lavorano assieme per realizzare dispositivi affidabili, con costi contenuti, basse potenze e senza fili, basati su uno standard aperto a livello globale
- ✓ L'obiettivo principale della ZigBee Alliance è fornire all'utente flessibilità, mobilità e facilità d'uso
- ✓ Vengono integrate l'intelligenza e le potenzialità delle reti wireless nei dispositivi comunemente usati ogni giorno

ZigBee Alliance

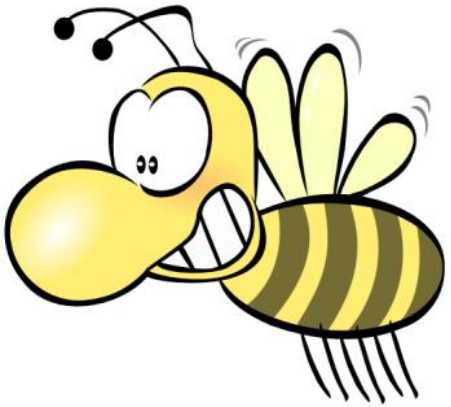
- ✓ La ZigBee Alliance si focalizza sulla:
  - ➢ definizione delle reti, della sicurezza e dei livelli d'accesso per le applicazioni
  - ➢ realizzazione dell'interoperabilità e definizione delle specifiche per i test di conformità
  - ➢ promozione del marchio ZigBee nel mercato
  - ➢ gestione dell'evoluzione della tecnologia

Significato del nome ZigBee (1/2)

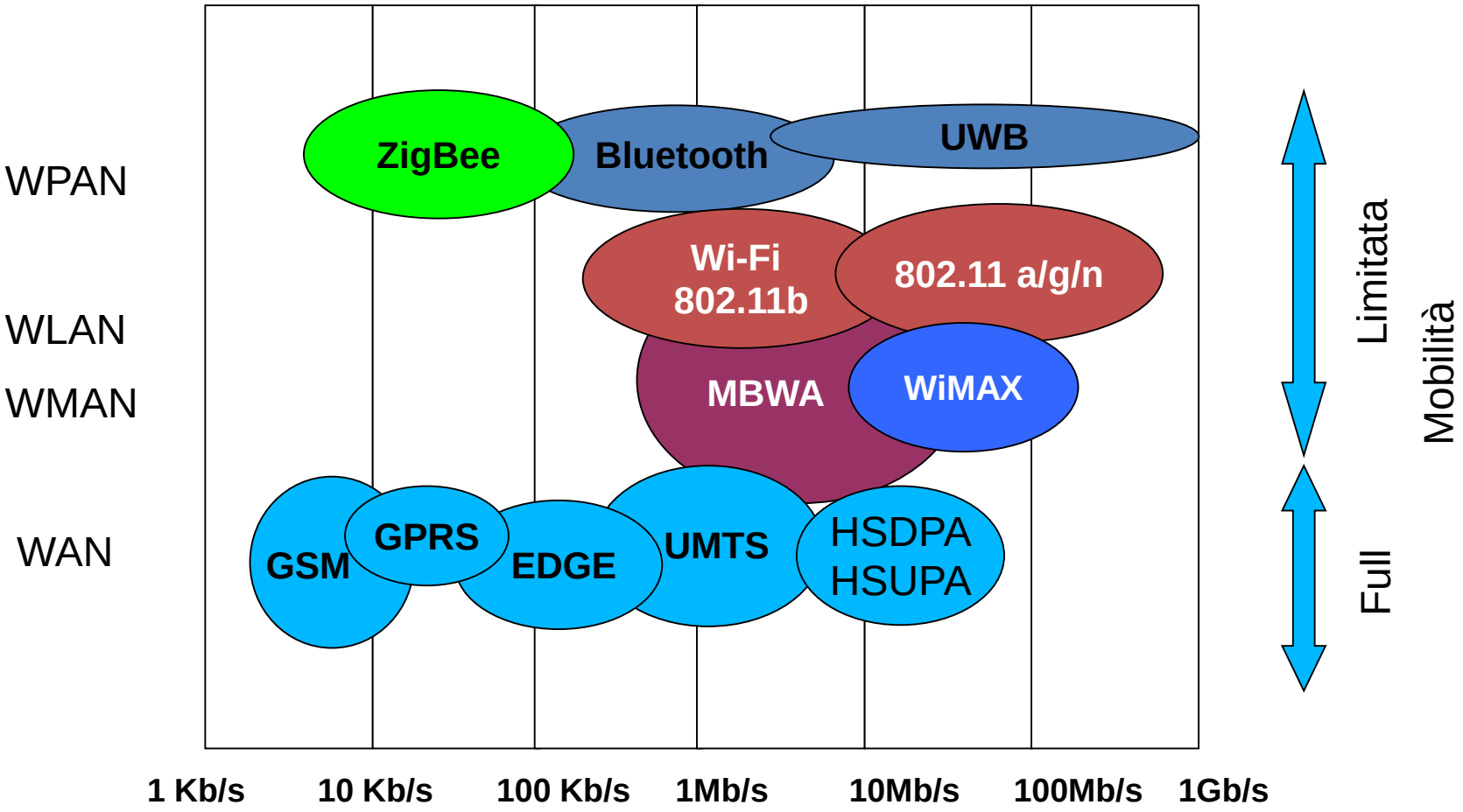
- ✓ Il nome ZigBee è ispirato al comportamento delle api domestiche (honeybee)
- ✓ Le api vivono in moltitudini che contengono una regina, pochi fuchi (i maschi) e migliaia di api lavoratrici
- ✓ La sopravvivenza e quindi il futuro della colonia dipende dalla continua comunicazione di informazioni vitali tra tutti i membri. Usando questo sistema di comunicazione dove le api “danzano” a zig-zag possono essere condivise informazioni vitali come per esempio la direzione ed il luogo di nuove fonti di cibo

Significato del nome ZigBee(2/2)

- ✓ I dispositivi ZigBee imitano la vita collaborativa delle api ed il loro continuo scambio di informazioni
- ✓ Da questo nasce il nome composto da zig-, relativo al movimento a zig-zag e -bee che significa ape



Mobilità vs Rate



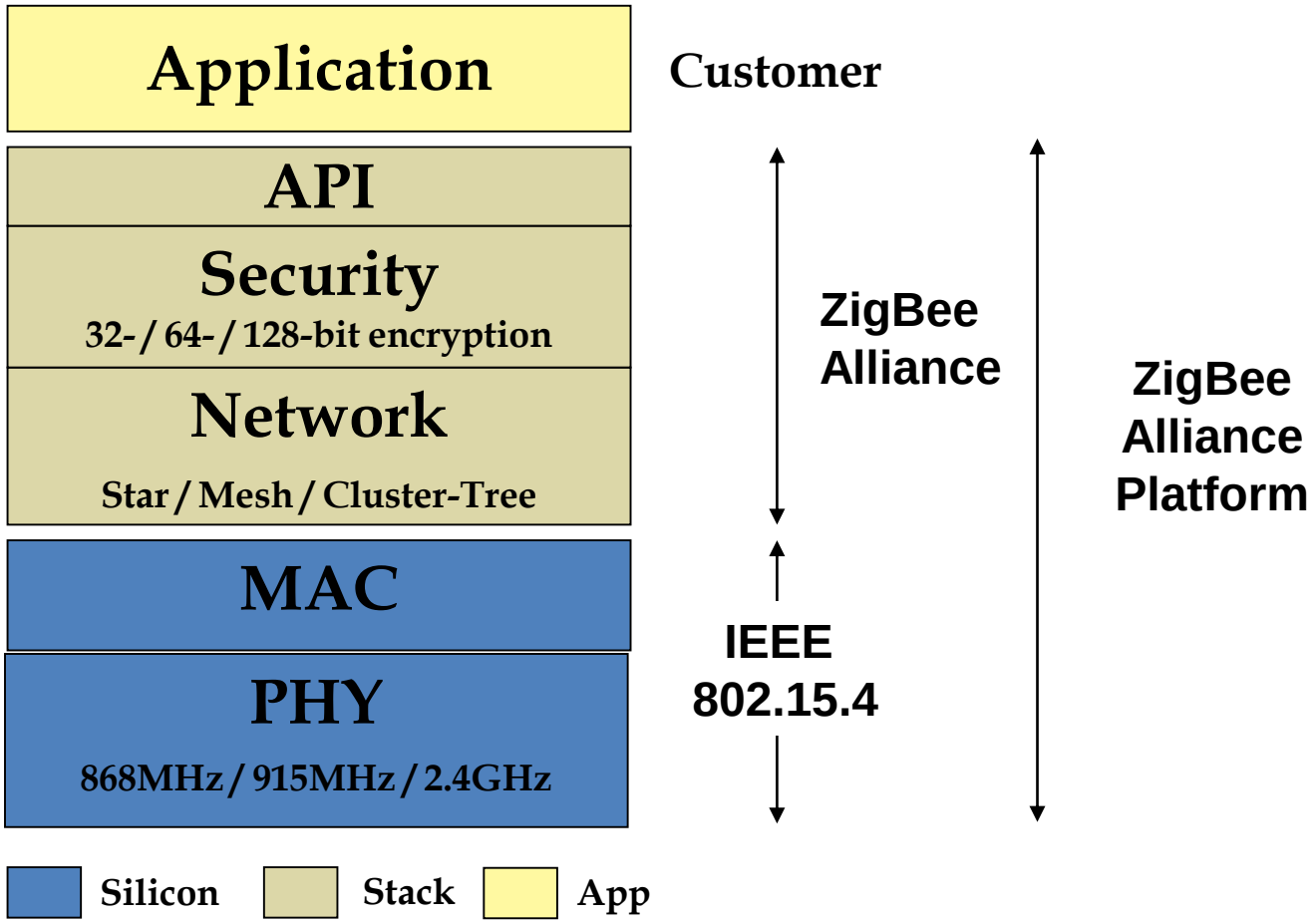
Architettura 1/2

- La ZigBee Alliance definisce i livelli superiori della pila protocollare:
  - logical network
  - security
  - software application

- I livelli inferiori, cioè il livello fisico ed il MAC, sono definiti dallo standard IEEE 802.15.4

- I livelli fisico PHY e MAC definiscono i protocolli e le interconnessioni fra i dispositivi che comunicano via radio in una WPAN

Architettura 2/2



Livello fisico

- ✓ Crea un interfaccia tra il livello MAC ed il canale radio ed è responsabile di:
  - attivare/disattivare l'interfaccia radio
  - indicare il livello di qualità del link per i pacchetti ricevuti (LQI - Link Quality Indicator)
  - effettuare una stima del canale per CSMA-CA (ED - Energy Detection)
  - selezionare la frequenza del canale
- ✓ Lo standard definisce due interfacce radio:
  - una alle frequenze di lavoro nell'intorno di 868 e 915 MHz
  - una per la banda ISM 2.4 GHz

Livello MAC

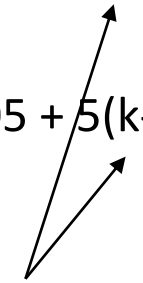
- ✓ Il livello MAC si occupa di tutti gli accessi al canale radio ed è inoltre responsabile delle seguenti funzioni:
  - ➢ gestire gli accessi multipli al canale (CSMA-CA)
  - ➢ realizzare un link logico tra 2 dispositivi
- ✓ Ha un ruolo secondario nella sicurezza dei dispositivi

Bande e canali 1/3

- ✓ Lo standard definisce 3 diverse bande per un totale di 27 canali disponibili per la comunicazione:
  - la banda a 868.3 MHz che definisce 1 canale (0)
  - la banda da 902 a 928 MHz che definisce 10 canali (1-10)
  - la banda ISM a 2.4 GHz che definisce 16 canali (11-26)

Bande e canali 2/3

- ✓ Le frequenze centrali per i 27 canali vengono così definite:
  - F_c = 863.2 MHz per k=0
  - F_c = 906 + 2(k-1) MHz per k=1,2,…,10
  - F_c = 2405 + 5(k-11) MHz per k=11,12,….,26

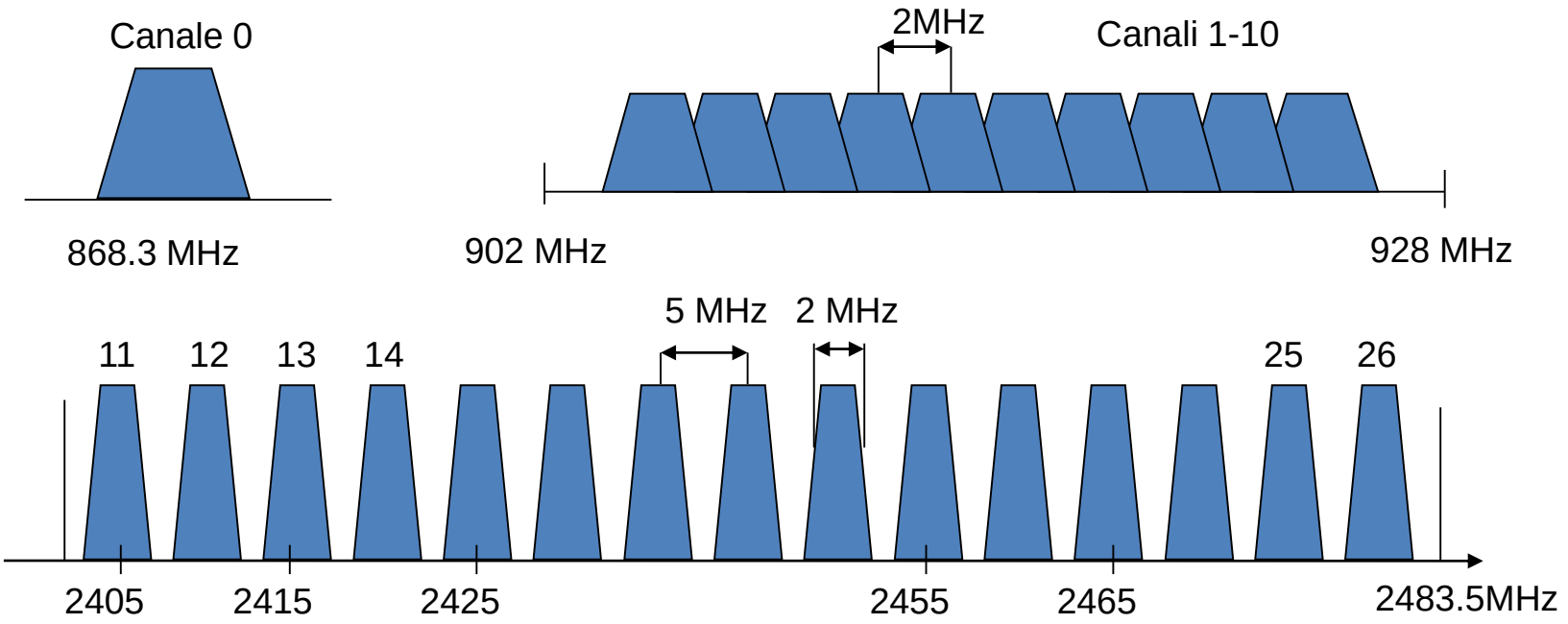


sono gli intervalli di guardia

- ✓ La tolleranza massima per la F_c è di 40ppm

Bande e canali 3/3

- ✓ Banda a 868 MHz ⇒ larghezza di 600 KHz
- ✓ Bande 915 MHz e 2.4 GHz ⇒ larghezza di 2 MHz



Modulazioni utilizzate

- ✓ L'obiettivo principale di questi dispositivi è avere bassi consumi e dimensioni ridotte -> È richiesta perciò la minima complessità
- ✓ Le modulazioni utilizzate sono la BPSK, l'ASK e la O-QPSK con 16 simboli (4+4+4+4)
- ✓ L'accesso al canale è realizzato tramite diverse tecniche di spread spectrum, a seconda delle frequenze di lavoro:
  - a 868 e 915 MHz è utilizzata la DSSS e la PSSS
  - a 2450 MHz è utilizzata la DSSS

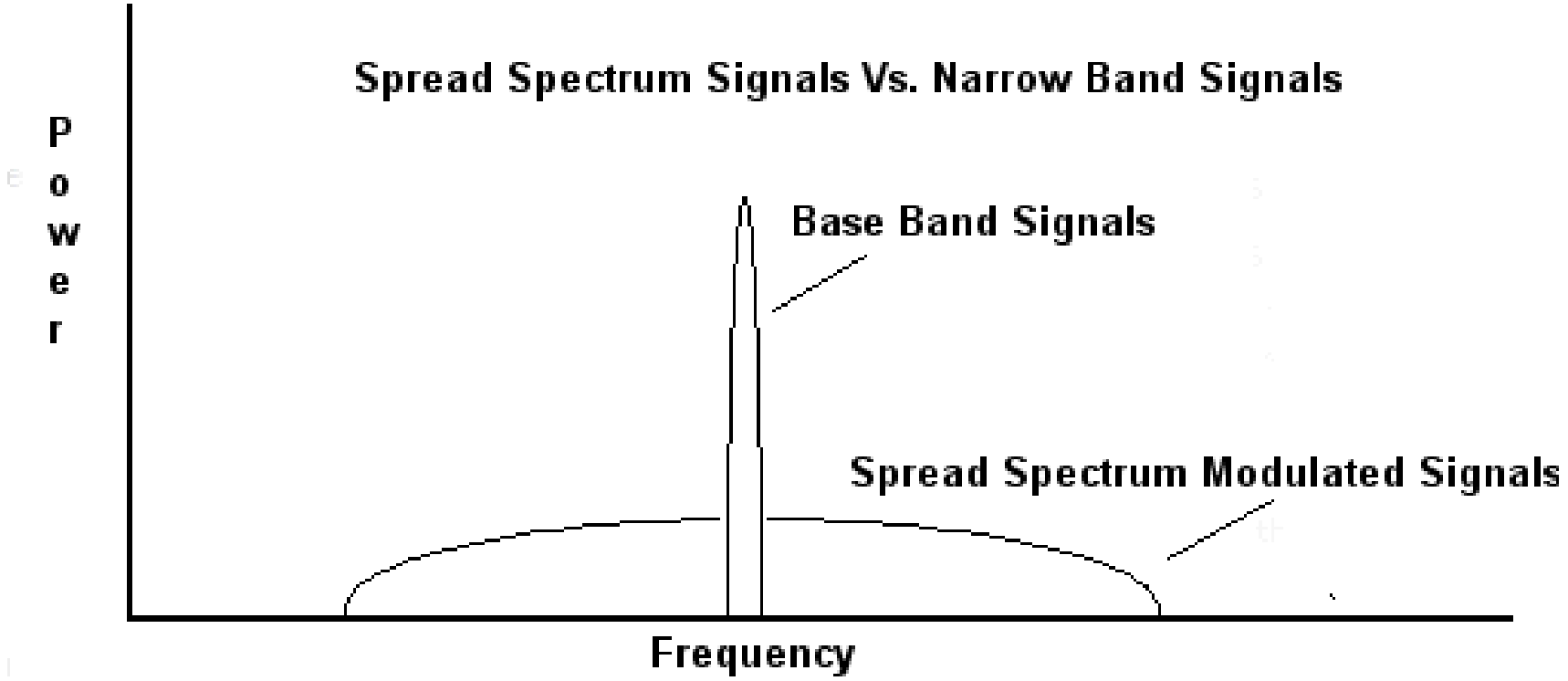
Tabella riassuntiva delle modulazioni

PHY (MHz)	Frequency Band (MHz)	Chip rate (Kchip/s)	Modulation	Bit rate (Kb/s)	Symbol rate (Ksymb/s)
868/915	868-868.6	300	BPSK	20	20
	902-928	600	BPSK	40	40
868/915 (optional)	868-868.6	400	ASK	250	12.5
	902-928	1600	ASK	250	50
868/915 (optional)	868-868.6	400	O-QPSK	100	25
	902-928	1000	O-QPSK	250	62.5
2450	2400-2483.5	2000	O-QPSK	250	62.5

Spread Spectrum 1/2

- ✓ Trasmissione “tradizionale”: Più potenza possibile nello spettro più stretto possibile
- ✓ Uso di “trasformazioni matematiche” per disperdere lo spettro originale del segnale da trasmettere in uno spettro molto più largo
- ✓ L’operazione inversa deve essere svolta in ricezione

Spread Spectrum 2/2



FHSS

- ✓ La tecnica ***Frequency Hopping Spread Spectrum*** ottiene la dispersione dello spettro mediante la variazione rapidissima della frequenza di trasmissione con andamento pseudo-casuale
- ✓ TX e RX devono essere perfettamente sincronizzati e conoscere la sequenza pseudo-casuale delle frequenza di trasmissione
- ✓ Non è più utilizzate nelle apparecchiature Wireless fidelity in commercio
- ✓ Esiste anche una tecnica Time hopping (THSS) analoga alla FHSS che trasmette in slot temporali in maniera pseudo-casuale

DSSS 1/6

- ✓ La dispersione dello spettro avviene moltiplicando il bit-rate del segnale per un codice pseudo-casuale a media nulla, lo stream così ottenuto (tipicamente il chip-rate è 10÷100 volte superiore al bit-rate) viene inserito in un modulatore e trasmesso a radio frequenza (RF)

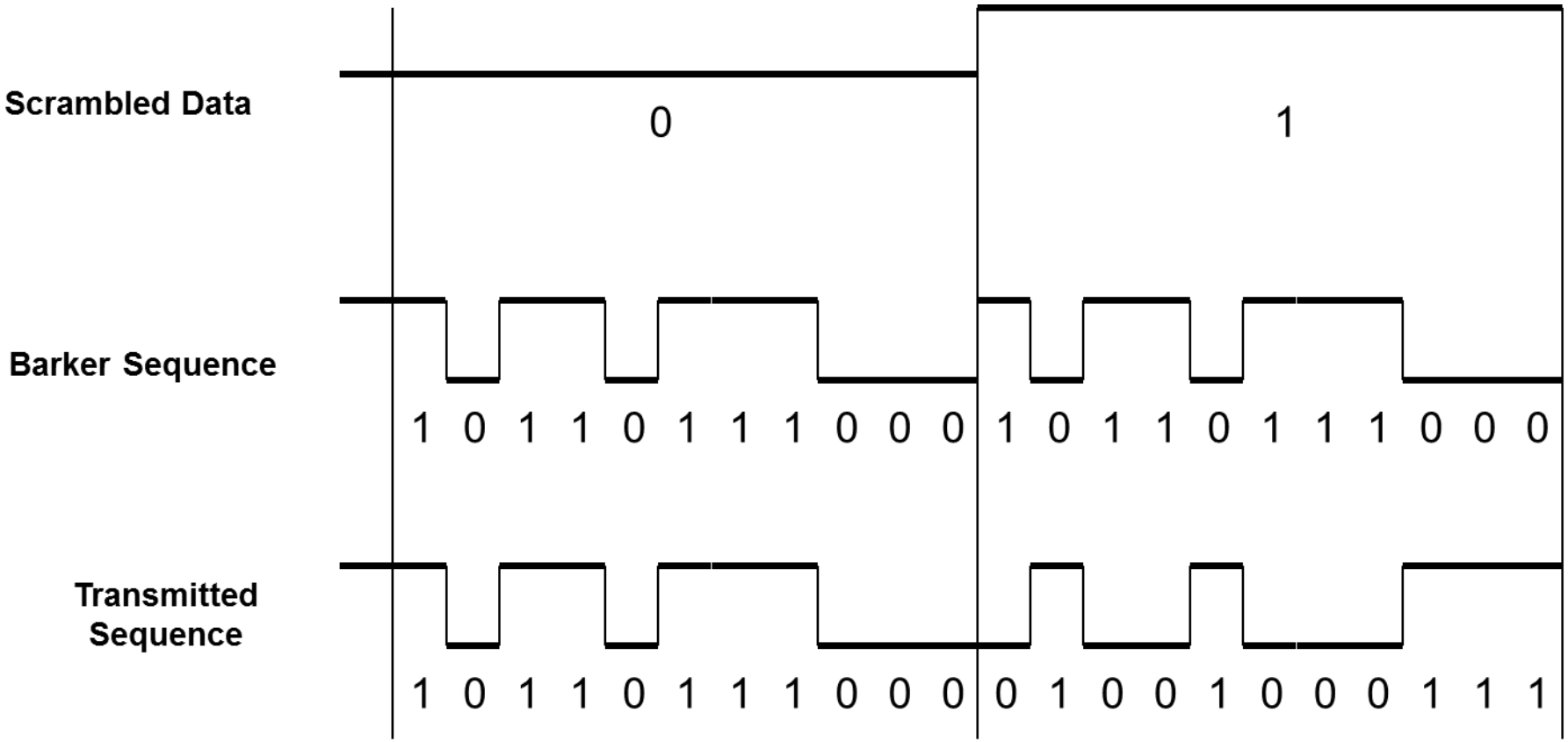
- ✓ ***Direct Sequence Spread Spectrum*** tollera un rapporto segnale rumore (SNR) più basso rispetto al frequency hopping

- ✓ Tecnologicamente si presta per velocità più elevate rispetto a FHSS

DSSS 2/6

- ✓ Il ***chip*** è una cifra binaria usata nel processo di dispersione
- ✓ Ogni bit trasmesso viene disperso su una sequenza a 11 chip detta sequenza Barker
- ✓ Il segnale trasmesso occuperà una maggior larghezza di banda consentendo la ricezione di segnali deboli
- ✓ I bit sono i dati di informazione, mentre i chip sono solo una parte della codifica e non portano alcuna informazione
- ✓ I flussi di chipping sono anche detti codici di rumore pseudo-casuale (Pseudo-Noise)

DSSS 3/6


Scrambled Data
0
1
Barker Sequence
1 0 1 1 0 1 1 1 0 0 0 1 0 1 1 0 1 1 1 0 0 0
Transmitted Sequence
1 0 1 1 0 1 1 1 0 0 0 0 1 0 0 1 0 0 0 1 1 1

DSSS 4/6

- ✓ In ricezione un correlatore mette a confronto la sequenza pseudo-casuale (che deve essere nota) con il segnale ricevuto, determinando se il bit trasmesso era un “1” oppure uno “0”

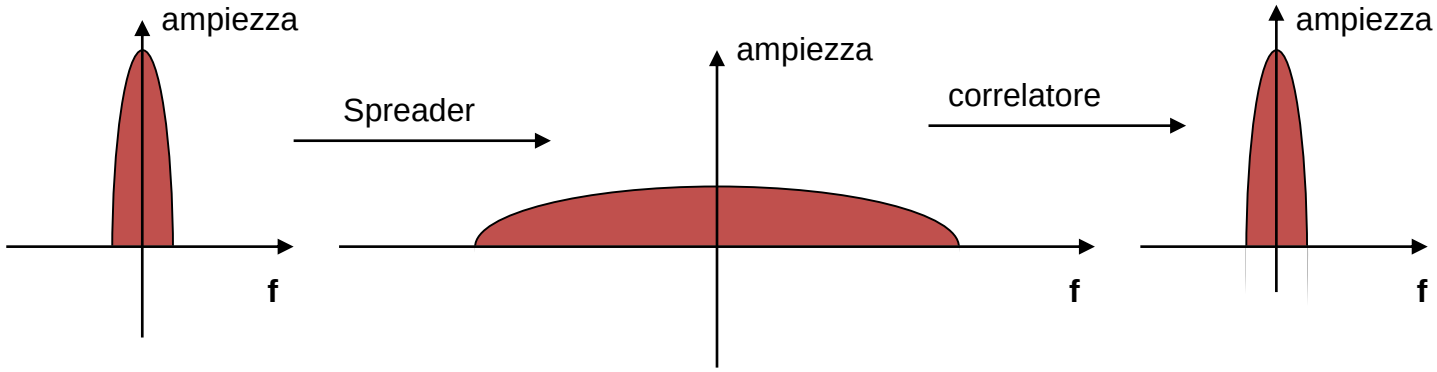
- ✓ Grazie alla ridondanza dei flusso di chipping (vengono trasmessi molti chip per codificare uno solo bit), in questa tecnica è presente un “***Guadagno di Codifica***” tanto maggiore quanti più sono i chip rispetto ai bit di informazione

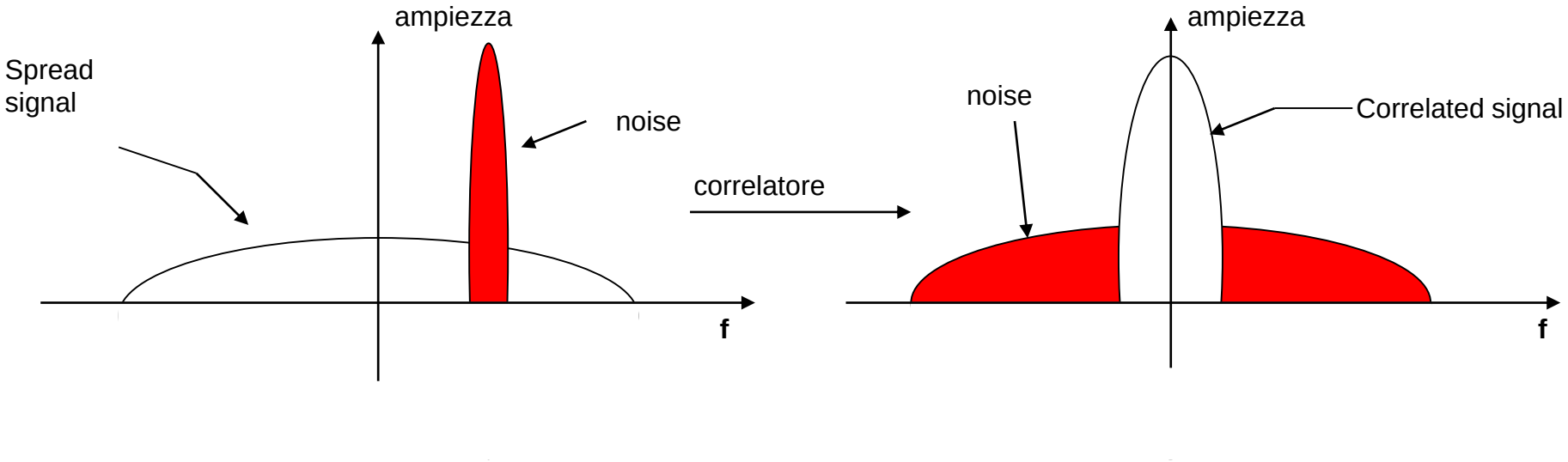
$$\text{Spreading Factor} = \frac{chipRate}{bitRate}$$

DSSS 5/6

- ✓ Poiché lo spettro è più largo il livello della densità spettrale di potenza del segnale è molto basso (anche inferiore alla potenza del rumore termico)
  - ➢ Conseguenza:
    - E' difficilmente individuabile
    - Non disturba altre trasmissioni
- ✓ La decodifica è possibile solo se il ricevitore conosce la sequenza pseudo-casuale usata in trasmissione:
  - ➢ Conseguenza:
    - È garantita la protezione dei dati
    - Tolleranza al rumore impulsivo

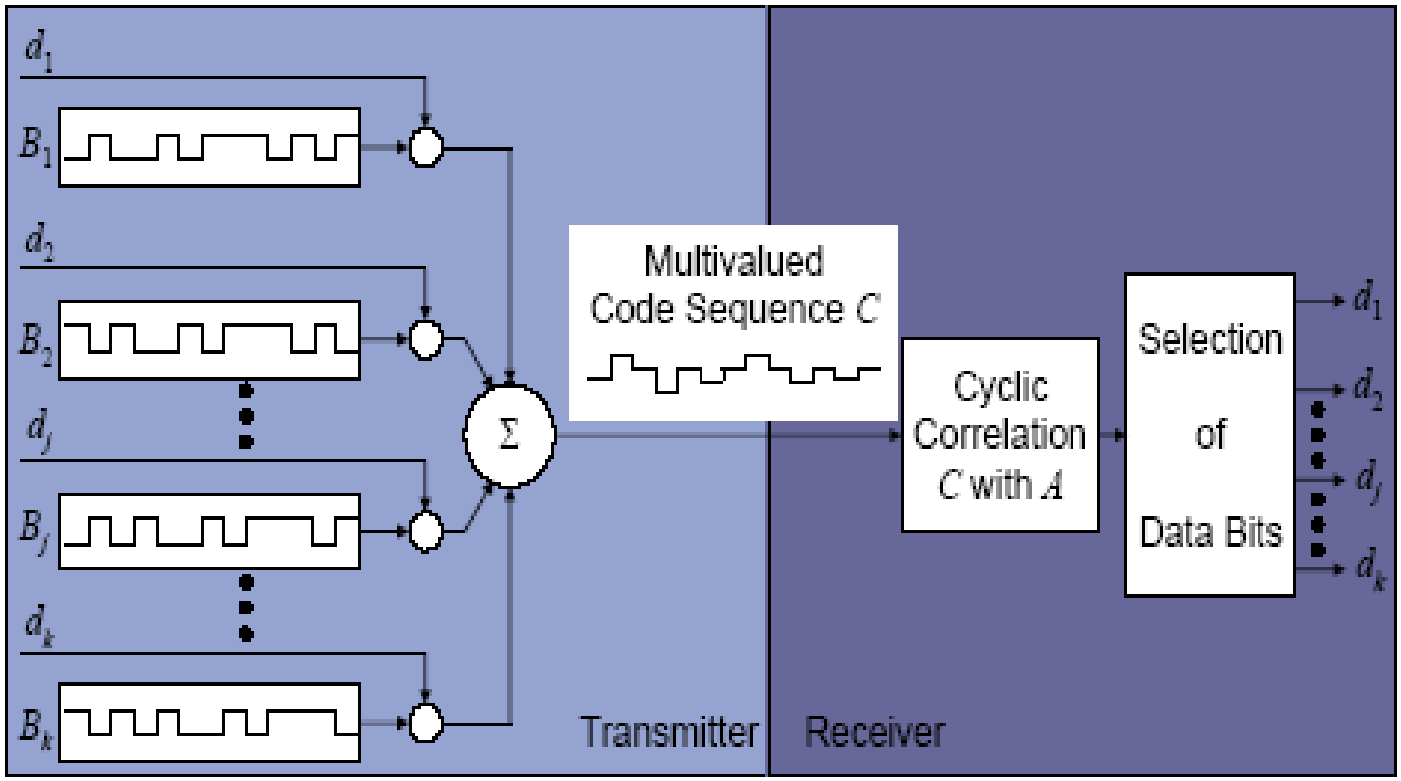
DSSS 6/6


ampiezza
f
Spreader
ampiezza
f
correlatore
ampiezza
f


Spread
signal
ampiezza
noise
f
correlatore
ampiezza
noise
Correlated signal
f

Parallel Sequence Spread Spectrum (PSSS) 1/4

- ✓ La PSSS invia “in parallelo” sul canale una sovrapposizione di sequenze ortogonali (fino a 20)



PSSS 2/4

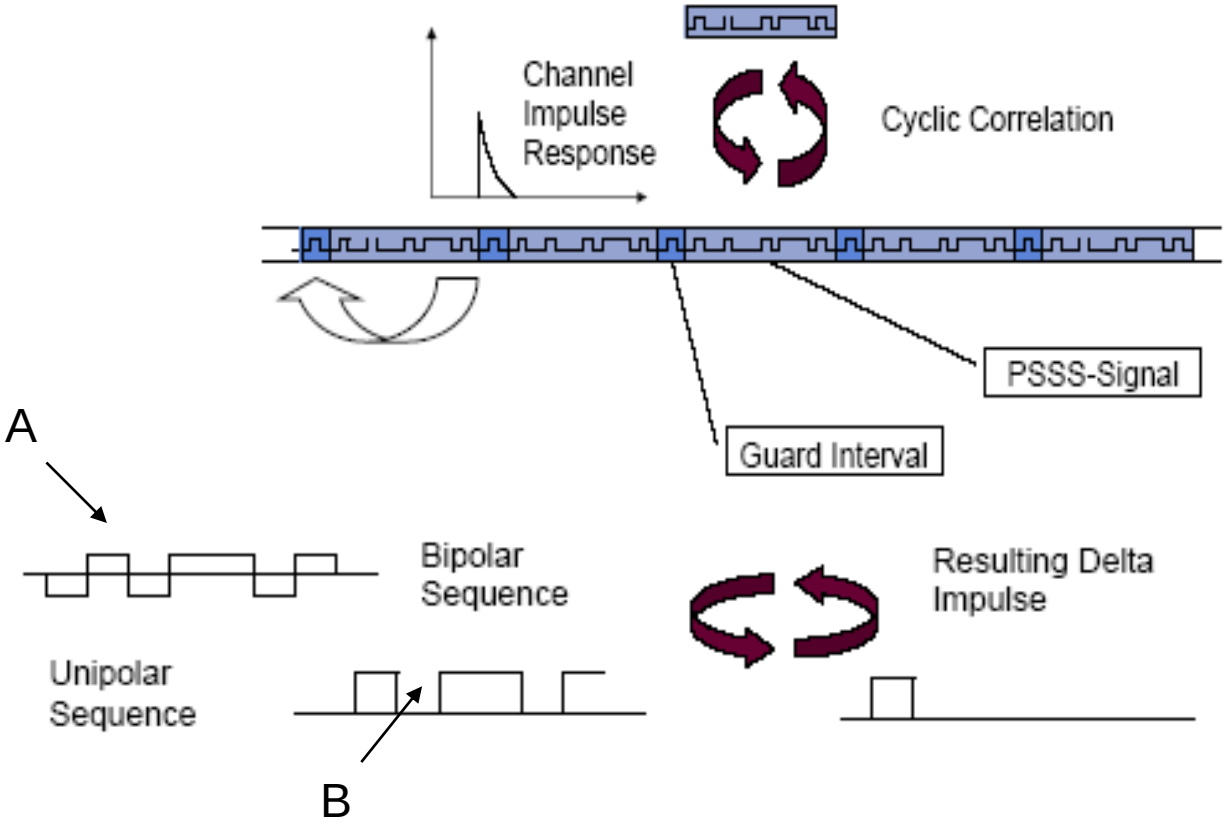
- ✓ Data una sequenza madre A (bipolare), è costruita la sequenza B (unipolare), utilizzata per la costruzione del codice. Le sequenze B_i sono generate con uno shift ciclico della sequenza B per ogni bit d'informazione
- ✓ Ogni bit d'informazione d_i viene moltiplicato per la sequenza B_i
- ✓ La sequenza codificata d_i viene sommata alle altre sequenze per formare la sequenza PSSS. Il segnale è quindi trasmesso con opportuna modulazione

$$c_i = d_i * B_i$$

- ✓ In ricezione la correlazione tra la sequenza ricevuta e la sequenza madre A permette la ricostruzione dell'informazione

PSSS 3/4

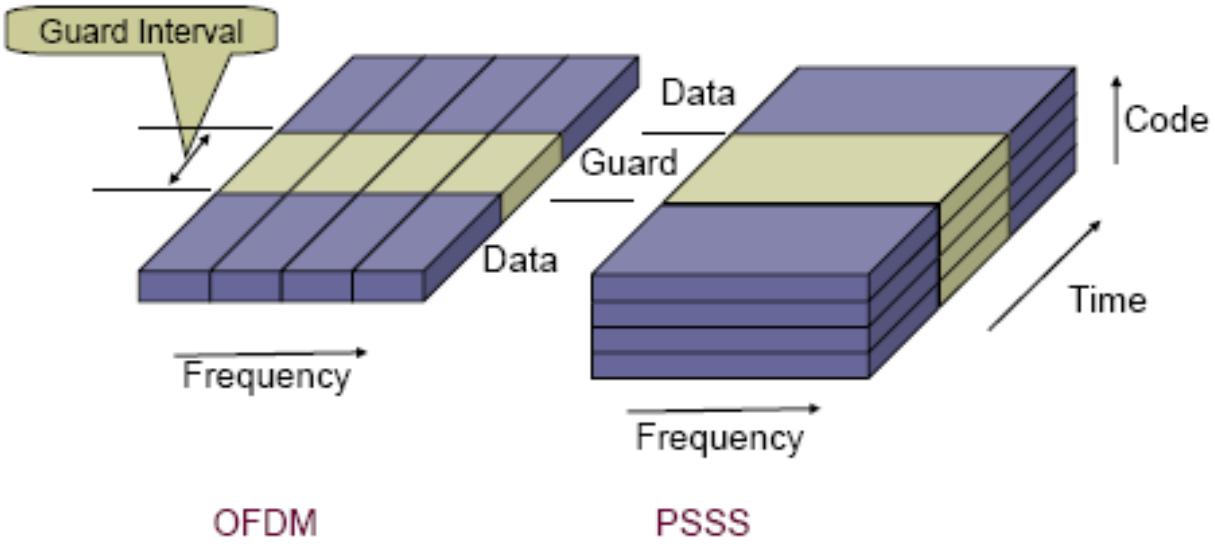
- ✓ La correlazione ciclica di una sequenza bipolare con una versione unipolare della stessa sequenza origina un impulso discreto



$$d_k = \begin{cases} +1 \Rightarrow '1' \\ -1 \Rightarrow '0' \end{cases}$$

PSSS 4/4

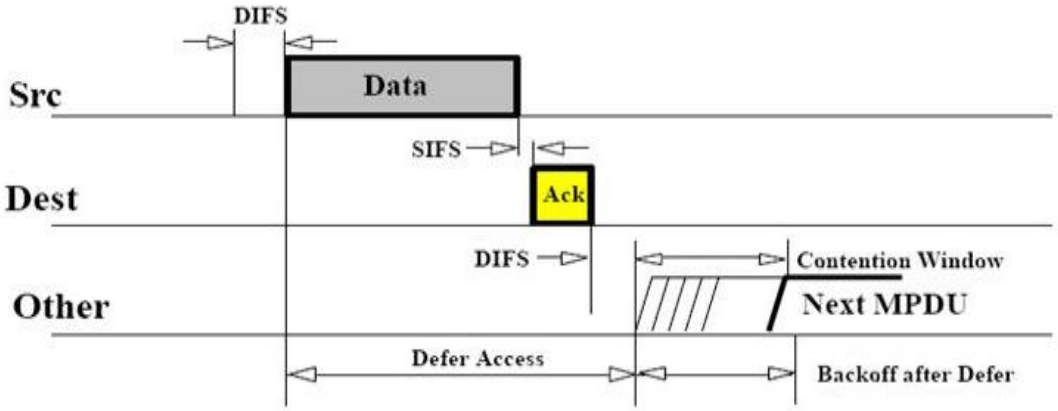
- ✓ E’ importante avere una sincronizzazione fine
- ✓ Confronto con l’ OFDM



Accesso al canale 1/3

- ✓ L' accesso al canale può essere libero o conteso
  - ➢ Nel primo caso l'accesso è controllato dal Coordinator tramite messaggi di sincronizzazione (beacon frame) inviati a tutti i dispositivi da lui gestiti
    - bassa latenza e banda dedicata
    - ideale per dispositivi che stanno sempre in ascolto
  - ➢ Nel secondo caso si basa sul noto algoritmo CSMA-CA. Questo prende le informazioni necessarie per gestire gli accessi dalla funzione ED (Energy Detection)
    - è un semplice e tradizionale sistema di accesso multiplo
    - usato nelle reti peer-to-peer

Accesso al canale 2/3



✓Nel momento in cui una stazione vuole tentare una trasmissione ascolta il canale (*Listen-before-Transmit*)

✓Se il canale risulta libero (*idle*) la stazione attende per un certo lasso di tempo identificato come DIFS (*Distribuited Inter Frame Space*)

✓A trasmissione completata il nodo di trasmissione attende per un tempo detto SIFS (*Short Inter Frame Space*) la ricezione di un ACK

Accesso al canale 3/3

- ✓ Inoltre vengono introdotte le definizioni di canale adiacente e canale alternato
  - ➢ Canale adiacente:
    - se il canale desiderato per la comunicazione è ad esempio il 5°, i canali adiacenti saranno il 4° e il 6°.
  - ➢ Canale alternato:
    - se il canale utilizzato è il 5°, i canali alternati saranno il 3° e il 7°

- ✓ Questi dovranno ovviamente rispettare dei vincoli in termini di potenza per non interferire nella comunicazione

Low rate – Wireless Personal Area Network 1/2

- ✓ Una LR-WPAN è una semplice rete a costi relativamente bassi che consente di ottenere connettività con potenza e throughput limitati

- ✓ Una rete di questo tipo deve
  - ➢ essere facile da installare
  - ➢ garantire un trasferimento dati affidabile
  - ➢ consentire operazioni a corto raggio con una ragionevole durata della batteria
  - ➢ utilizzare un protocollo semplice e flessibile

Low rate – Wireless Personal Area Network 2/2

- ✓ Le caratteristiche tecniche definite delle reti ZigBee sono:
  - data rate di 250Kb/s, 40Kb/s e 20Kb/s
  - accesso al canale con CSMA-CA
  - 16 canali nella banda 2450MHz, 10 canali nella banda 915MHz, 1 canale a 868MHz
  - il raggio di copertura va da 10 a 70 metri

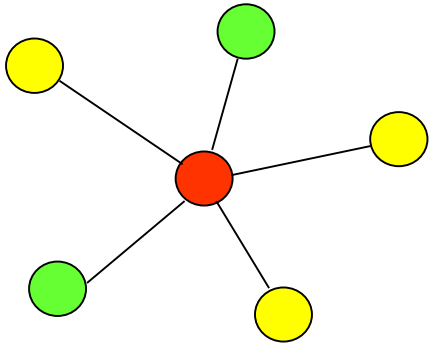
Tipologie di dispositivi

- ✓ I dispositivi ZigBee possono essere configurati in modo da realizzare diverse topologie di reti

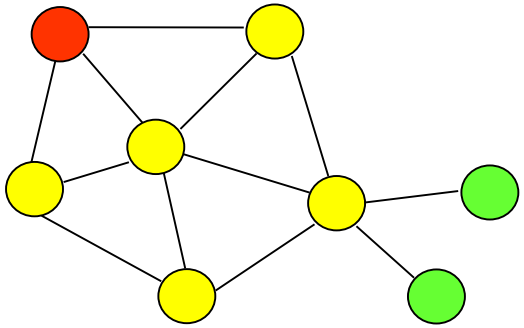
- ✓ Le specifiche dello standard distinguono 3 tipi di dispositivi:
  - **Il coordinatore**, che ha il compito di organizzare la rete e conservare le tabelle di routing
  - **I router**, che possono parlare con tutti gli altri dispositivi
  - **I dispositivi finali** (Reduced devices), che hanno funzionalità ridotte e che possono parlare con in router e il coordinatore, ma non tra di loro

- ✓ Una topologia largamente usata è quella mesh

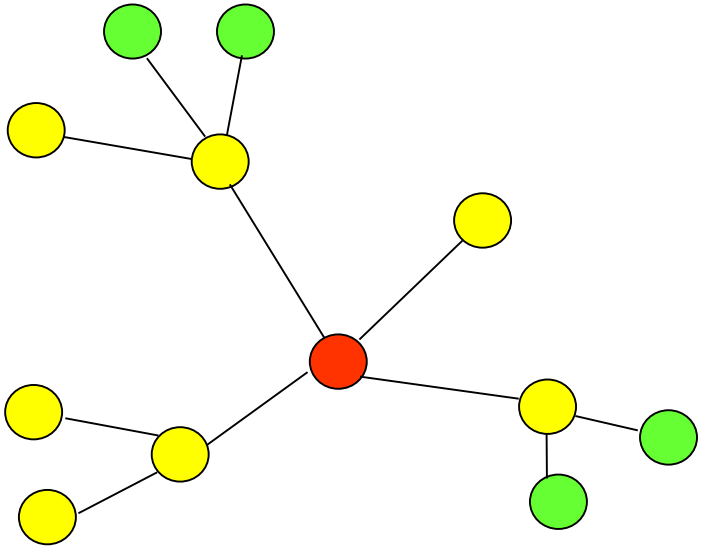
Topologie di rete



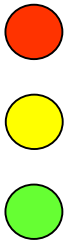
Stella



Mesh



Cluster



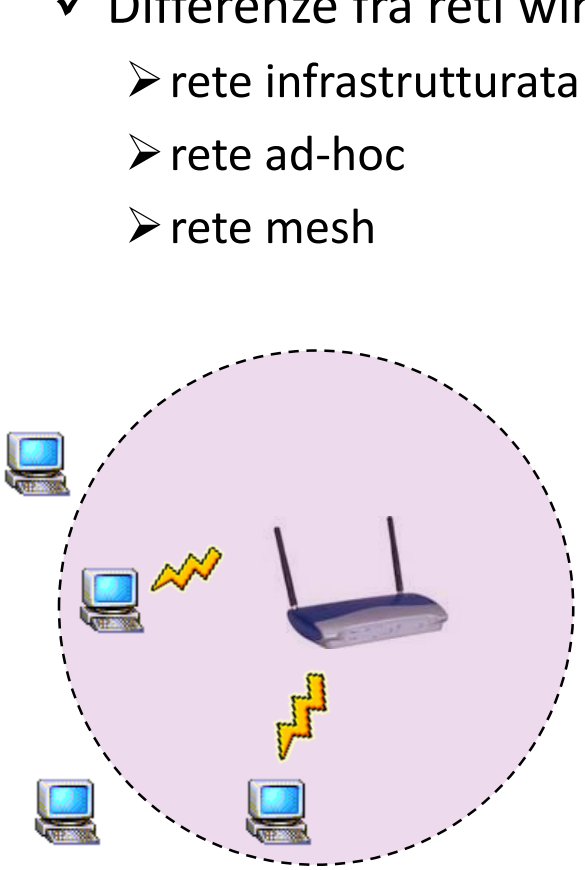
Coordinatore

Router

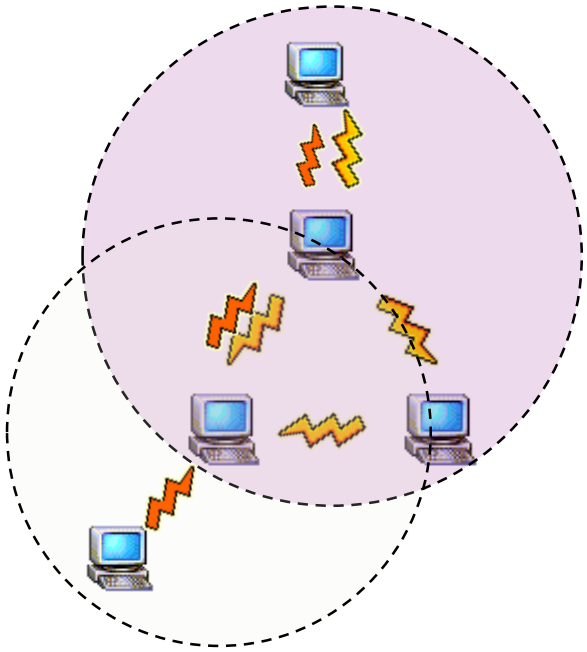
Reduced device

Reti mesh 1/2

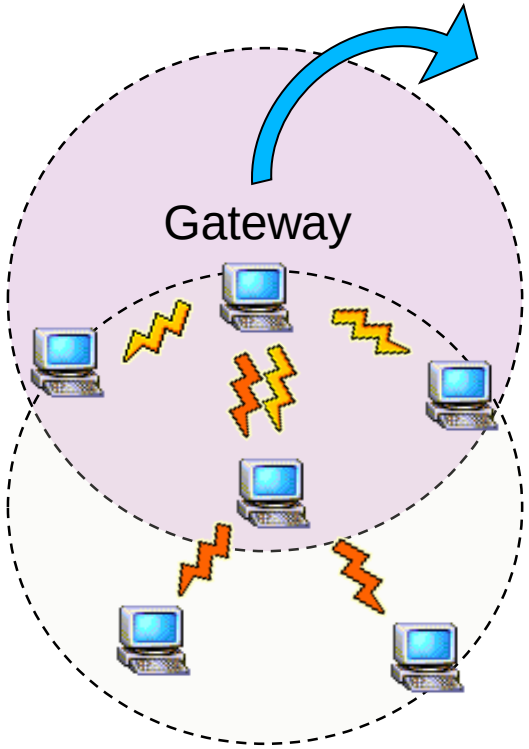
- ✓ Differenze fra reti wireless a corto raggio
  - ➢ rete infrastrutturata
  - ➢ rete ad-hoc
  - ➢ rete mesh



Rete infrastrutturata



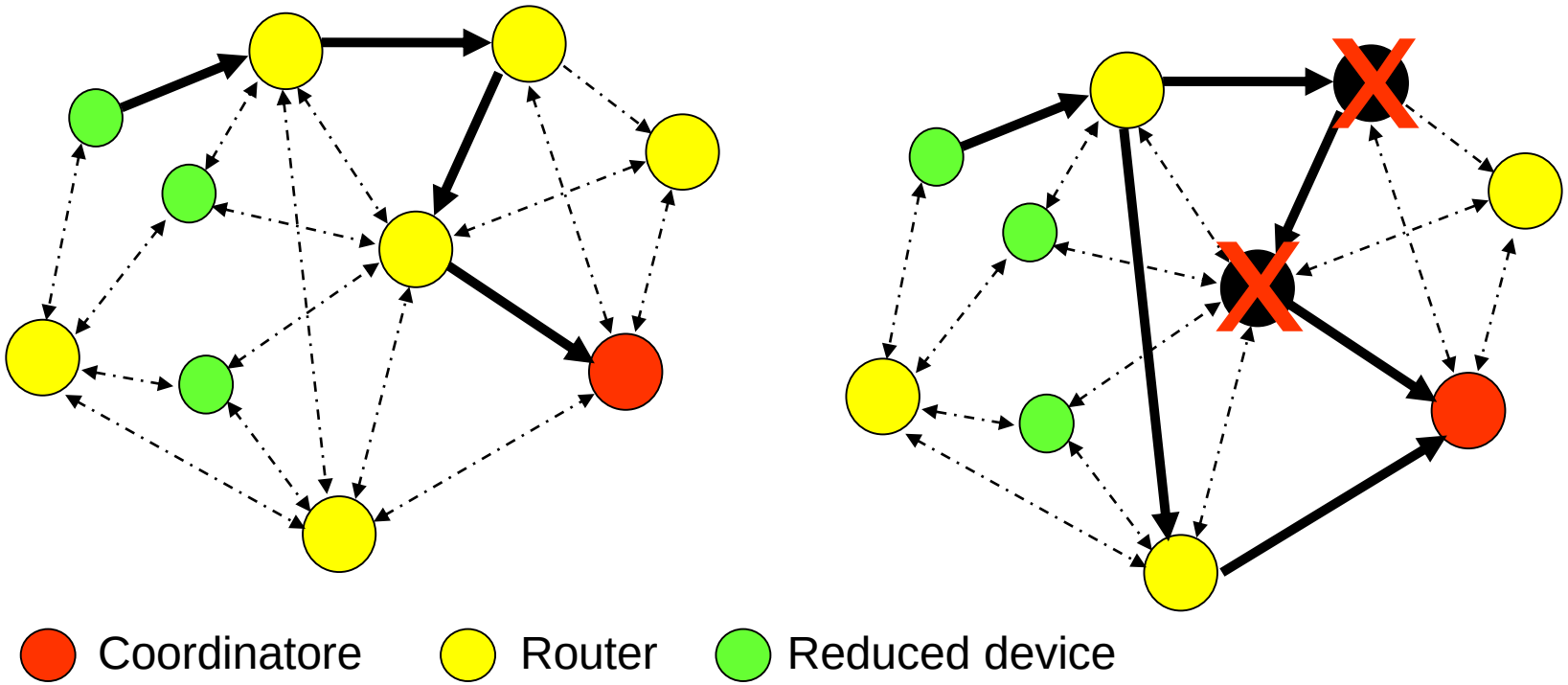
Rete ad-hoc



Rete mesh

Reti mesh 2/2

- ✓ Il percorso possibile fra un end-device ed un altro non è unico



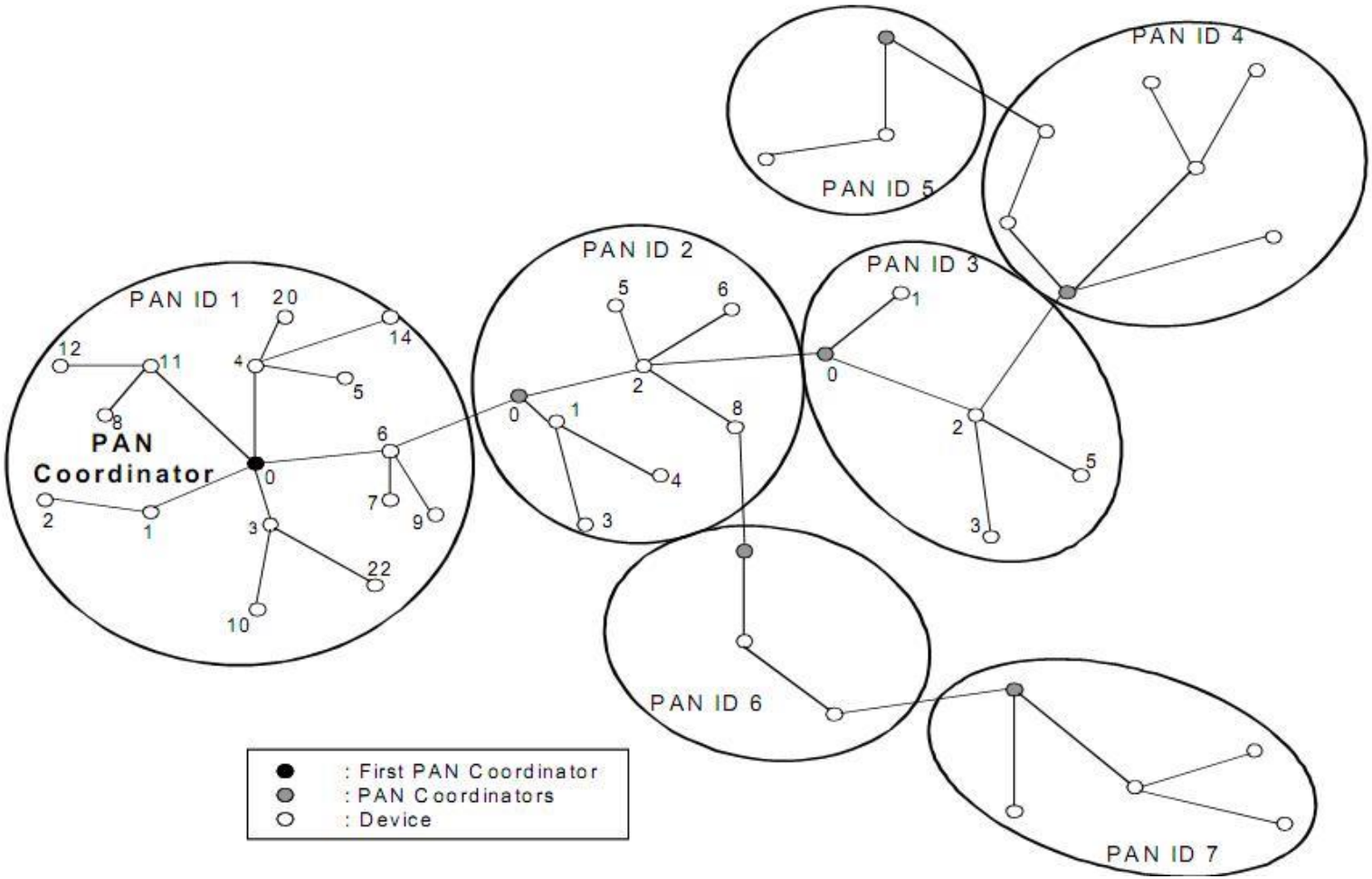
- ✓ Questo è un grande vantaggio per quanto riguarda la flessibilità e la realizzabilità della rete

Cluster tree networks 1/2

- ✓ Più reti possono organizzarsi in cluster con una struttura ad albero. Viene così realizzata una rete peer-to-peer con un minimo overhead di routing

- ✓ Il sistema ha un alta tolleranza intrinseca alle interferenze
  - ➢ può utilizzare canali multipli
  - ➢ può facilmente cambiare canale (usare altre frequenze)
  - ➢ usa una modulazione robusta

Cluster tree networks 2/2



Consumo di potenza

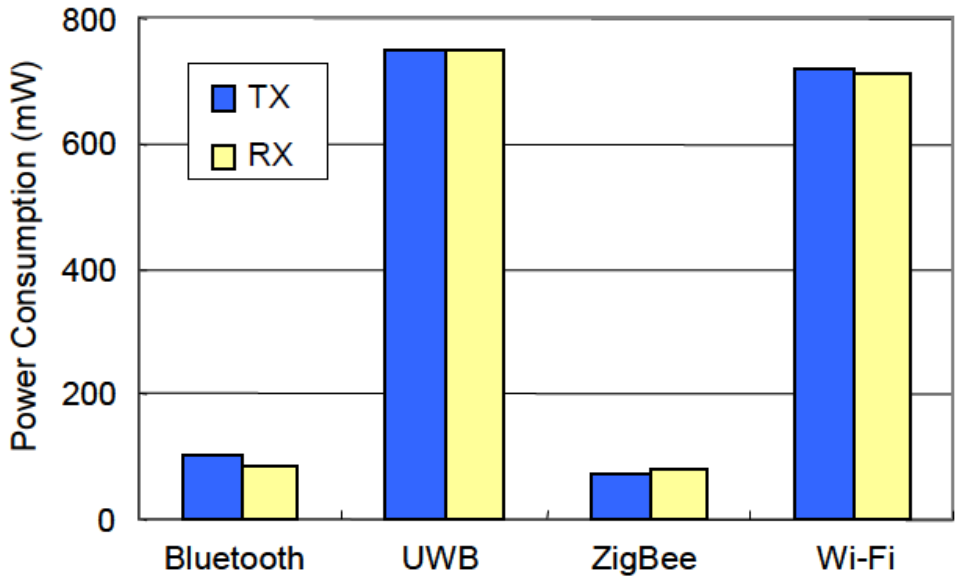
- ✓ Per minimizzare il consumo di potenza e quindi massimizzare la durata delle batterie i dispositivi finali passano la maggior parte del loro tempo “addormentati”
- ✓ Si svegliano soltanto quando hanno bisogno di comunicare e poi si riaddormentano immediatamente
- ✓ Lo standard prevede invece che i router ed il coordinatore siano collegati alla rete elettrica e siano sempre attivi non avendo quindi dei vincoli sul consumo di potenza

Potenze in trasmissione

- ✓ La potenza in trasmissione usata nella banda a 2.4GHz è compresa tra -3dBm e 10dBm con valore tipico 0dBm
- ✓ Nella banda 915MHz il limite massimo è di 1000 mW (30dBm) tuttavia i terminali costruiti secondo la tecnologia “system-on-chip” limitano la potenza intorno ai 10dBm
- ✓ Nella banda 868MHz il limite massimo è di circa 14dBm (25mW) e la potenza minima deve essere almeno di -3dBm

Potenze

Standard	Bluetooth	UWB	ZigBee	Wi-Fi
Chipset	BlueCore2	XS110	CC2430	CX53111
VDD (volt)	1.8	3.3	3.0	3.3
TX (mA)	57	~227.3	24.7	219
RX (mA)	47	~227.3	27	215
Bit rate (Mb/s)	0.72	114	0.25	54



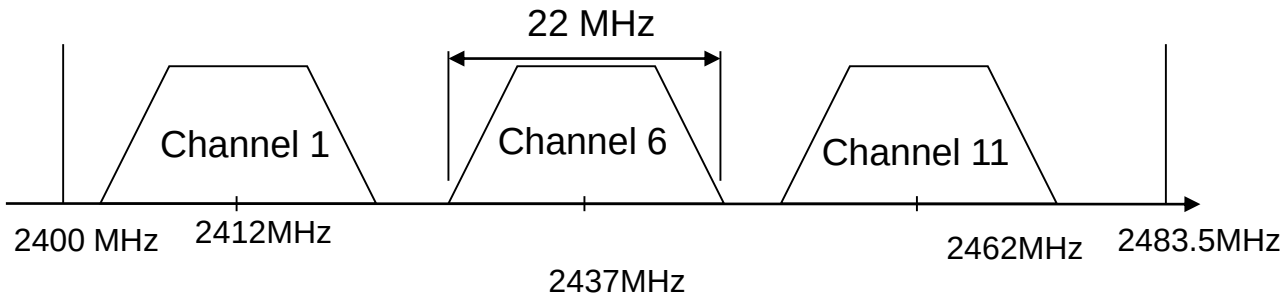
Interferenze con i dispositivi esistenti 1/2

- ✓ Nella banda 868/915 MHz, si utilizzano le modulazioni BPSK, O-QPSK e ASK
  - ➢ la modulazione ASK usa soltanto 2 simboli con una codifica polare
  - ➢ sono usate tecniche DSSS, che permettono di trasmettere con bassi SNR e SIR (Signal to Interference Ratio)
  - ➢ oltre alla DSSS viene usata anche la PSSS (Parallel Sequence Spread Spectrum)

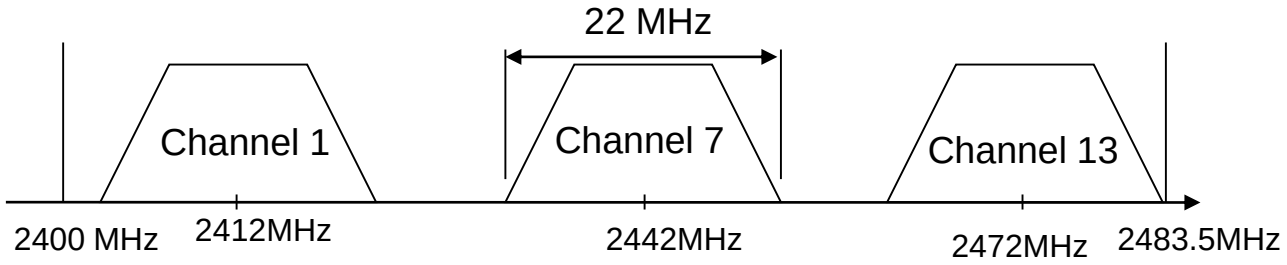
Interferenze con i dispositivi esistenti 2/2

- ✓ Nella banda a 2400MHz si usa soltanto la O-QPSK
- ✓ L'uso di sequenze PN (Pseudo Noise) per rappresentare ciascun simbolo garantisce prestazioni simili alla modulazione DSSS
  - ➢ i dispositivi conformi alle specifiche 802.11b (WiFi - DSSS) e 802.15.3(UWB) sono visti dai ricevitori ZigBee come rumore bianco
  - ➢ nel caso di un dispositivo che trasmette con una modulazione FHSS (es. Bluetooth) il trasmettitore ZigBee va ad interferire soltanto su 3 dei 79 hop (circa il 4%)

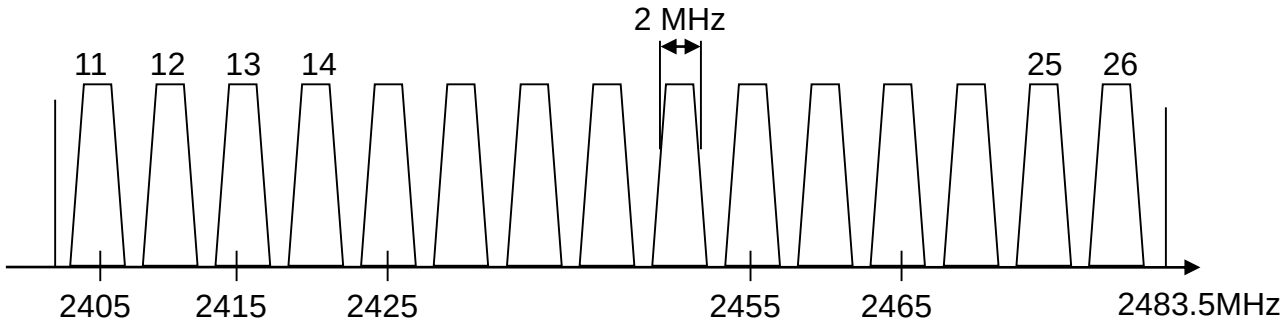
Interferenza con il WiFi nella banda ISM



WiFi (802.11b)
Nord America



WiFi (802.11b)
Europa



IEEE
802.15.4

Sicurezza 1/4

- ✓ IEEE 802.15.4 imposta l'algoritmo di crittografia da utilizzare quando codifica i dati da trasmettere tuttavia lo standard non specifica come devono essere gestite le chiavi o che tipo di criteri di autenticazione devono essere applicati

- ✓ Questi problemi vengono trattati negli strati superiori gestiti da ZigBee

- ✓ Il primo step per abilitare la sicurezza a livello 802.15.4 è impostare una chiave detta **link key** da 128 bit che deve essere la stessa su tutti i nodi per renderli capaci di comunicare all'interno della rete.

Sicurezza 2/4

- ✓ Abilitare la sicurezza diminuisce il Payload ma garantisce la privacy nella rete

	Unicast	Broadcast
Criptato	**98 Bytes**	**95 98 Bytes**
Non Criptato	**100 Bytes**	**100 Bytes**

- ✓ Lo Zigbee implementa 2 livelli di sicurezza aggiuntivi sopra lo standard 802.15.4:
  - ➢ Sicurezza nel Network layer
  - ➢ Sicurezza nell'Application layer

Sicurezza 3/4

- ✓ Abilitare la sicurezza nel Network layer aggiunge uno step di autenticazione nel processo di join alla rete

- ✓ Dopo che un router si aggiunge alla rete deve ottenere la **network security key** per diventare autenticato e se non la ottiene l'autenticazione fallisce e il dispositivo lascia la rete dal momento che non è in grado di comunicare con nessun altro nodo nella rete

- ✓ La distribuzione della network security key avviene ad opera del **Trusted Center** utilizzando la link key

Sicurezza 4/4

- ✓ La application key è usata per cifrare i dati del livello applicazione
- ✓ È unica per ogni coppia di nodi
- ✓ La chiave non è configurabile e quindi deve essere specificato se un nodo ha intenzione di usarla

Trusted center 1/2

- ✓ Lo standard ZigBee definisce il ruolo di Trusted center ovvero di dispositivo “fidato” che all’interno della rete distribuisce le chiavi allo scopo di gestire le connessioni
- ✓ Tutti i membri della rete devono riconoscere esattamente solo un trusted center ed all’interno di ogni rete ce ne deve essere solo uno
- ✓ Di default è il coordinatore della PAN

Trusted center(2/2)

- ✓ Il trusted center svolge fondamentalmente 3 ruoli
  - trust manager: identifica i dispositivi appartenenti alla sua rete
  - network manager: è il responsabile della rete. Distribuisce e gestisce la network-key
  - configuration manager: permette di instaurare una connessione end-to-end sicura a livello applicazione

Applicazioni ¼

- ✓ Lo standard è stato principalmente pensato per la creazione di reti di sensori wireless, e più in generale per prodotti di monitoraggio e controllo

- ✓ Domotica
  - ➢ in una casa, per esempio, è possibile integrare un host su ogni interruttore della luce ed acquisire la capacità di monitorare e controllare in maniera centralizzata lo stato dell'illuminazione di un ambiente
  - ➢ automatizzazione garage
    - ▪ un dispositivo installato sull'auto permette l'apertura automatica del garage senza l'uso del telecomando

Applicazioni 2/4

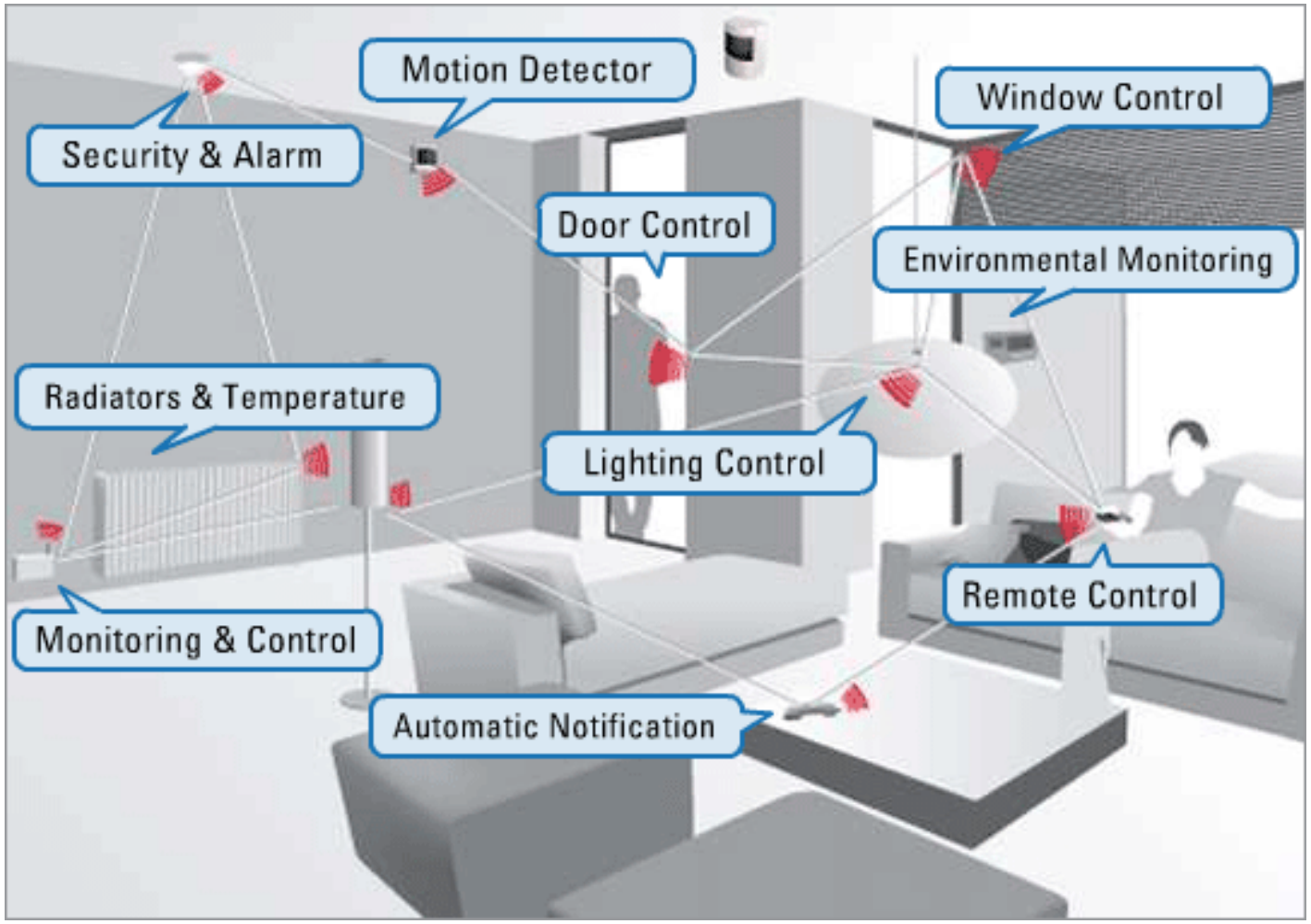
- ✓ Controllo granulare di un ambiente civile o industriale
  - monitoraggio dei consumi energetici (gas, elettrici) per impostare piani di risparmio
  - accounting dei consumi per la certificazione energetica
  - conteggio dei consumi di singole aree (dipartimenti, negozi, appartamenti...) e fatturazione relativa
  - monitoraggio delle condizioni ambientali (temperatura, umidità, luce) di aree sensibili
- ✓ Periferiche del PC
  - joystick, tastiera, mouse

Applicazioni 3/4

- ✓ Monitoraggio dei pazienti
  - ➢ il paziente è tenuto sotto osservazione direttamente a casa sua. Le informazioni sono inviate via Internet alla clinica medica dove il dottore può modificare il settaggio del dispositivo

- ✓ Sistemi di tracciabilità
  - ➢ determinare la posizione di un nodo non fisso della rete. Il nodo non fisso, identificato con l'oggetto da monitorare, si muove nell'area controllata e dialoga con i nodi fissi della rete
  - ➢ questo consente al sistema di stabilire con ragionevole approssimazione la sua posizione

Applicazioni 4/4



Vantaggi dello standard ZigBee

- ✓ Rispetto alle soluzioni proprietarie una soluzione standardizzata ha sicuramente dei vantaggi:
  - ➢ interoperabilità dei prodotti certificati
  - ➢ indipendenza dei vendor
  - ➢ l'utilizzo di una piattaforma comune è più efficiente rispetto ad una piattaforma proprietaria per quanto riguarda i costi
  - ➢ le aziende possono concentrare le loro energie per realizzare prodotti specifici che richiede il mercato

Confronto ZigBee-Bluetooth 1/3

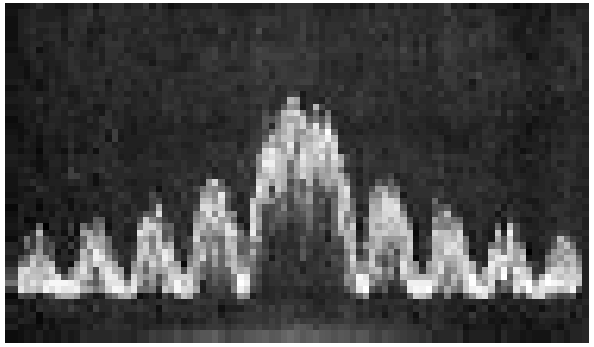
- ✓ Le due tecnologie hanno caratteristiche fisiche molto simili, mentre i protocolli che utilizzano sono diversi perché gli scenari d'uso sono nettamente distinti

- ✓ I dispositivi Zigbee saranno usati nei contesti in cui è scomodo o difficile cambiare le batterie: sensori antifurto, comandi per porte/finestre/illuminazione, sensori di pressione nei pneumatici…

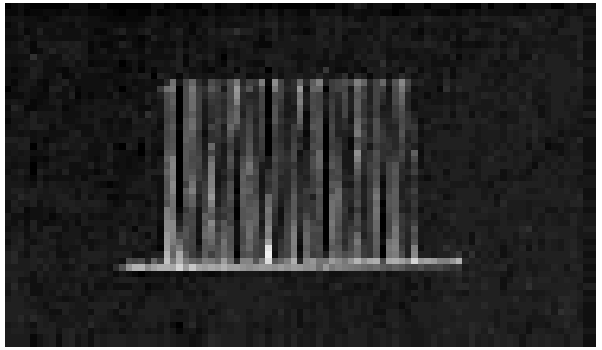
- ✓ I dispositivi Bluetooth sono più utilizzati dove è necessaria una maggior velocità di trasmissione e parametri di QoS stringenti, per esempio negli auricolari

Confronto ZigBee-Bluetooth 2/3

- ✓ Bluetooth ha una struttura di rete quasi statica, mentre quella dello ZigBee è dinamica, con possibilità di estensione piuttosto semplice
- ✓ ZigBee e Bluetooth sono due tecnologie complementari

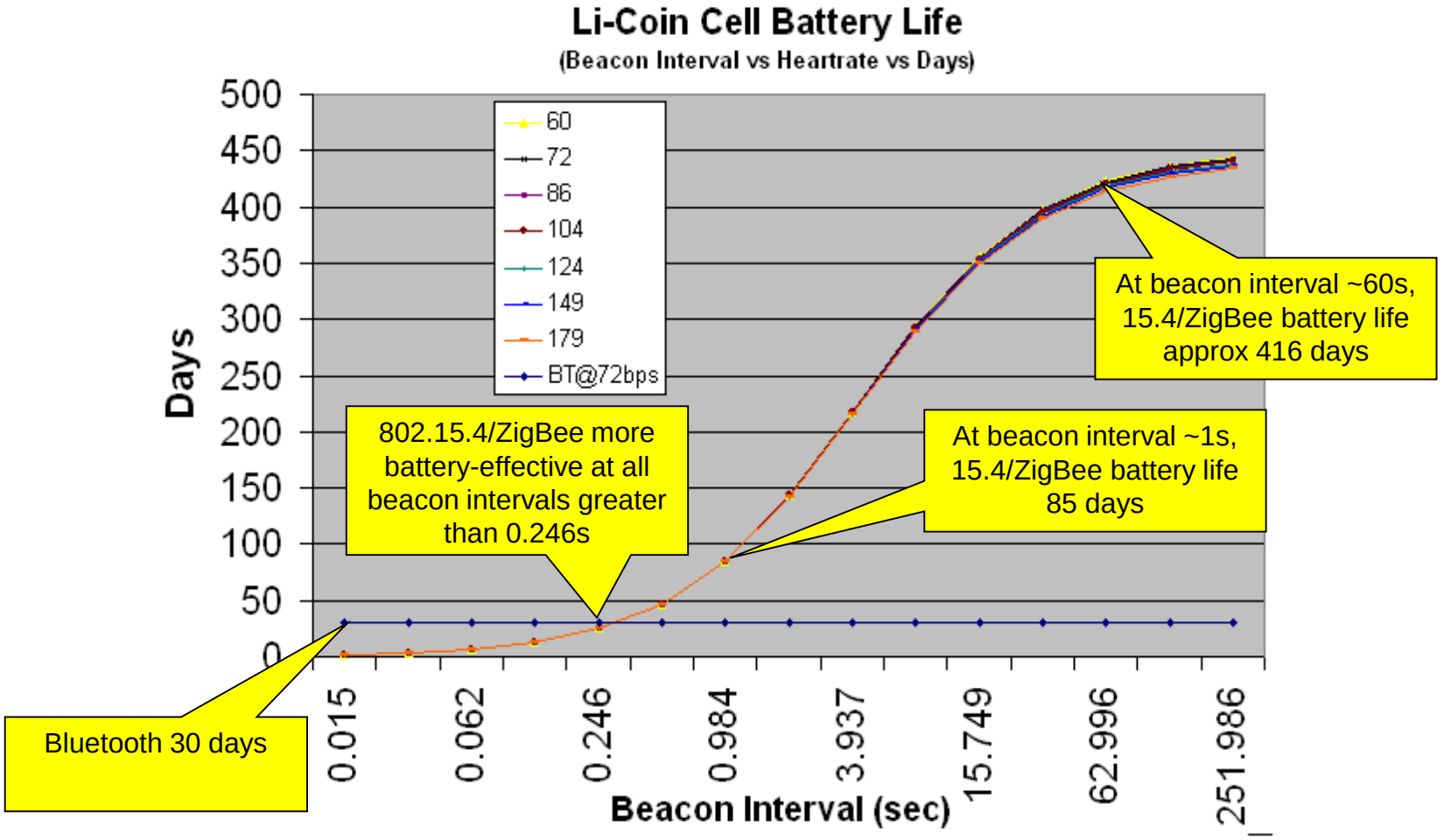


DSSS



FHSS

Confronto ZigBee-Bluetooth 3/3

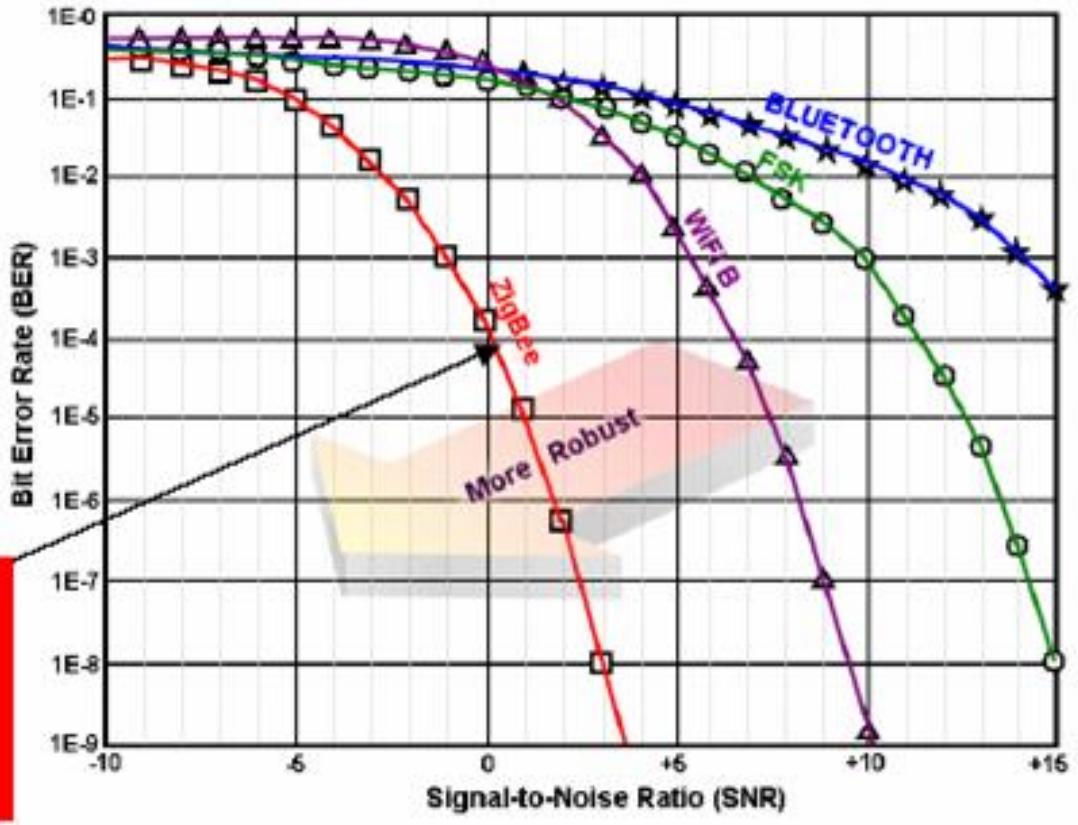


Standard reti wireless

	IEEE 802.11b	Bluetooth	IEEE 802.15.4
Profilo di durata	Ore	1 settimana	Più di un anno
Costo di produzione	9€	6€	3€
Complessità	Complessa	Molto complessa	Semplice
Nodi/Master	32	7	65K
Latenza	Fino a 3 secondi	Fino a 10 s	30ms
Distanza	100m	10m	70m
Estensibilità	Roaming	NO	SI
Data rate(max)	11 Mbps	1 Mbps	250 kbps
Sicurezza	Autenticazione Service Set ID (SSID)	64 bit, 128 bit	128 bit AES e layer applicazione definito dall'utente

Confronto con altri standard

✓La capacità richiesta è molto bassa in confronto alle altre tecnologie wireless



La tecnologia ZigBee è costruita sullo standard IEEE 802.15.4, che offre prestazioni eccellenti in condizioni di basso SNR

Conclusioni

- ✓ Lo standard aperto ZigBee va a coprire un campo applicativo dove non esistono tecnologie in grado di fornire un servizio equivalente

- ✓ La caratteristica principale è il bassissimo consumo energetico. Si stima che un dispositivo ZigBee con semplici batterie alcaline abbia un'autonomia di 2 anni

- ✓ Grazie all'autonomia di organizzazione in reti mesh, non è richiesto nessun intervento dall'esterno se non quello della sostituzione delle batterie

Altri standard

- ✓ Esiste un'altra associazione, la Z-Wave, guidata da aziende come la Panasonic e la Intel, che ha sviluppato una piattaforma proprietaria in netto contrasto con la ZigBee Alliance
- ✓ Le due alliances non sono riuscite a trovare un intesa. Sarà perciò il mercato a stabilire quale sarà la tecnologia vincente

Products that speak Z-Wave work together better™