



**UNIVERSITA' POLITECNICA DELLE MARCHE**  
**FACOLTA' DI INGEGNERIA**

---

Corso di Laurea magistrale in Ingegneria Elettronica

**Studio e implementazione di un sistema di localizzazione indoor per il  
tracciamento di oggetti per il cambio formato all'interno di reparti di  
produzione**

**Study and implementation of an indoor localization system for tracking  
objects for changeover within production departments**

Relatore:  
Prof.ssa Paola Pierleoni

Tesi di Laurea di:  
Gianmarco Martella

Correlatore:  
Dott.ssa Sara Raggiunto

A.A. 2021/ 2022

*Alla mia famiglia che mi ha sempre supportato ed aiutato, sia moralmente che economicamente, alla mia ragazza Silvia che c'è sempre per me e soprattutto per calmare le mie preoccupazioni, ai miei amici, chi lontano, chi vicino mi hanno fatto passare momenti di spensieratezza e felicità in questi anni.*

*Un ringraziamento speciale ai miei genitori Giacomo ed Elena e ai miei nonni Rocco, Ilda, Bruno ed Anna, perché senza il loro aiuto non avrei mai potuto raggiungere questo traguardo.*

## Sommario

<b>1</b>	<b>Introduzione</b>	<b>5</b>
1.1	Abstract	5
1.2	Internet of Things (IoT)	6
1.3	Industria 4.0	14
1.3.1	Tecnologie principali dell'industria 4.0	22
1.4	Industria 5.0	26
1.4.1	Nuovi argomenti di studio nell'industria 5.0	28
1.4.2	Applicazioni dell'industria 5.0	30
1.4.3	Nuove tecnologie abilitanti nell'industria 5.0	32
<b>2</b>	<b>Indoor Positioning Systems</b>	<b>33</b>
2.1	Parametri e tecniche per il calcolo della posizione	36
2.1.1	Received Signal Strength Indicator (RSSI)	36
2.1.2	Channel State Information (CSI)	38
2.1.3	Fingerprinting/ Scene Analysis	39
2.1.4	Angle of Arrival (AoA)	41
2.1.5	Time of Flight (ToF)	41
2.1.6	Time Difference of Arrival (TDoA)	43
2.1.7	Return Time of Flight (RToF)	46
2.1.8	Phase of Arrival (PoA)	46
2.2	Tecnologie per l'IPS	48
2.2.1	Sistemi di visione	48
2.2.2	Infrarossi	49
2.2.3	Visible Light Communication (VLC)	50
2.2.4	Ultrasuoni	50
2.2.5	Wi-Fi	51
2.2.6	RFID	53
2.2.7	Bluetooth (IEEE 802.15.1)	61
2.2.8	Ultra-Wide Band (UWB, IEEE 802.15.4a)	61
2.2.9	ZigBee	65
2.3	Metriche di valutazione per un sistema IPS	65
2.4	Sfide per un sistema di localizzazione	68
<b>3</b>	<b>Bluetooth Low Energy</b>	<b>69</b>
3.1	Controller	72
3.1.1	Physical Layer	72
3.1.2	Link Layer (LL)	73
3.1.3	Link Layer (Struttura dei pacchetti)	78
3.1.4	Host Controller Interface	83
3.2	Host	84
3.2.1	L2CAP	84
3.2.2	ATT	84

3.2.3	GATT	86
3.2.4	SMP	94
3.2.5	GAP	95
<b>3.3</b>	<b>Beacons</b>	<b>99</b>
3.3.1	Protocollo iBeacon	100
3.3.2	Protocollo Eddystone	102
3.3.3	Protocollo AltBeacon	103
<b>4</b>	<b>Algoritmi di localizzazione e stato dell'arte</b>	<b>104</b>
4.1	Articoli del BLE	105
4.2	Articoli UWB	121
<b>5</b>	<b>Progetto: Conteggio pezzi e localizzazione</b>	<b>125</b>
5.1	Attività di cambio formato e tipologie di oggetti da tracciare	126
5.2	Oggetti del cambio formato	129
5.2.1	Unità di produzione	129
5.2.2	Minuteria	131
5.3	Tecnologia utilizzata	132
5.4	Database per cambio formato	133
5.5	Primo caso d'uso: Conteggio pezzi	136
5.5.1	MQTT	136
5.5.2	Calcolo della distanza tra gateway e beacons	137
5.5.3	Architettura dell'applicazione	138
5.5.4	Step del conteggio pezzi	139
5.6	Secondo caso d'uso: Localizzazione	140
5.6.1	Mappa	141
5.6.2	Acquisizione e organizzazione dei dati	143
5.6.3	Algoritmo sperimentale	144
<b>6</b>	<b>Conclusioni</b>	<b>146</b>

## Indice delle immagini

Figura 1: Panorama dell'IoT .....	7
Figura 2: Stack dell'IoT .....	9
Figura 3: Architettura IoT.....	10
Figura 4: Evoluzione industriale.....	15
Figura 5: Introduzione dell'industria 5.0 .....	26
Figura 6: Trilaterazione e Triangolazione attraverso segnali RSSI.....	37
Figura 7: Rappresentazione grafica del ToF.....	42
Figura 8: Rappresentazione grafia del TDoA.....	44
Figura 9: Rappresentazione di PoA .....	47
Figura 10: Differenze tra segnale NB e UWB.....	62
Figura 11: Modalità del Bluetooth.....	70
Figura 12: Tipi di pacchetto nel Bluetooth 5.0.....	71
Figura 13: Spettro di frequenze del BLE e del WiFi.....	72
Figura 14: Stati del Link Layer.....	74
Figura 15: Evento di advertising .....	74
Figura 16: Evento di scanning .....	76
Figura 17: Evento di connessione.....	77
Figura 18: Pacchetto BLE.....	78
Figura 19: Pacchetto LE 1M e 2M .....	80
Figura 20: Pacchetto LE Coded.....	80
Figura 21: PDU di un pacchetto di advertising .....	81
Figura 22: Payload di un pacchetto di advertising .....	81
Figura 23: PDU per pacchetto dati .....	82
Figura 24: PDU per header a 16 bit.....	82
Figura 25: PDU per header a 24 bit.....	82
Figura 26: Struttura dei dati del GATT .....	89
Figura 27: Esempio di servizio GATT .....	93
Figura 28: Pacchetto iBeacon .....	101
Figura 29: Pacchetto Eddystone .....	102
Figura 30: Pacchetto Altbeacon.....	103
Figura 31: Architettura operativa .....	108
Figura 32: Tecnica della trilaterazione .....	109
Figura 33: Caso ideale di trilaterazione.....	118
Figura 34: Caso reale di trilaterazione.....	120
Figura 35: Rappresentazione del TW-ToF .....	122
Figura 36: Esempio di unità di produzione 1 .....	130
Figura 37: Esempio di unità di produzione 2 .....	130
Figura 38: Esempio di minuteria 1 .....	131
Figura 39: Esempio di minuteria 2 .....	132
Figura 40: Architettura conteggio pezzi .....	139
Figura 41: Output dell'applicazione.....	140
Figura 42: Architettura del sistema Cisco .....	141
Figura 43: Mappa del reparto .....	142

## 1 Introduzione

### 1.1 Abstract

Questa tesi è volta ad evidenziare l'importanza di alcune tematiche dell'Internet of Things (IoT) nei processi produttivi. Infatti, l'IoT è uno degli argomenti centrali dell'industria 4.0, l'introduzione di nuove tecnologie di tipo sensoristico hanno un risvolto benefico per l'intera azienda.

Nello specifico verrà toccato in modo approfondito l'argomento di localizzazione indoor, analizzato nello scenario di un plant produttivo.

A differenza della localizzazione outdoor, nella quale il servizio del GPS è diventato quasi uno standard per le applicazioni, per ciò che riguarda la localizzazione all'interno di locali ed edifici, esistono un gran numero di tecnologie, ognuna che presenta vantaggi e svantaggi.

Dunque, c'è ancora molta ricerca nell'ambito della localizzazione indoor, questo perché ogni locale è diverso ed è difficile individuare un sistema standard che funzioni bene in tutti gli scenari.

Dopo un approfondito studio dello stato dell'arte, grazie all'innovazione tecnologica è stato deciso di sfruttare le tecnologie di ultima generazione e implementare un sistema basato sulla tecnologia Bluetooth, in particolare il Bluetooth Low Energy. La scelta viene dai vantaggi che questa tecnologia offre, come il basso costo dei dispositivi, il livello di precisione di localizzazione discreto e i bassi consumi di potenza. La tecnologia Bluetooth viene impiegata per la realizzazione di un sistema di appello di oggetti. Verrà posizionato un gateway in prossimità della linea di produzione di test e gli oggetti equipaggiati con un beacon vengono avvicinati ad esso al momento del conteggio pezzi.

È stata quindi realizzata un'applicazione in linguaggio di programmazione Python che, qualora bisogni eseguire il conteggio pezzi, l'operatore digiterà il codice

dell'articolo che deve essere prodotto e il sistema darà un feedback riguardo quante unità sono presenti e mostrerà una lista di unità mancanti.

La seconda applicazione del progetto è la localizzazione. Essa è stata implementata attraverso un software cloud commerciale di Cisco chiamato "Detect and Locate". Un sistema di questo tipo viene realizzato con dei Gateway Bluetooth predisposti nell'area di interesse e utilizzando dei beacon Bluetooth che saranno associati fisicamente agli oggetti da tracciare. Gli oggetti sono dei macchinari di medie dimensioni, denominati come "unità di produzione". Essi sono composti da una struttura metallica che contiene rulli, parti saldanti, coltelli, a seconda di qual è la loro funzione. Per poter eseguire localizzazione e conteggio, viene associato fisicamente un beacon al telaio metallico.

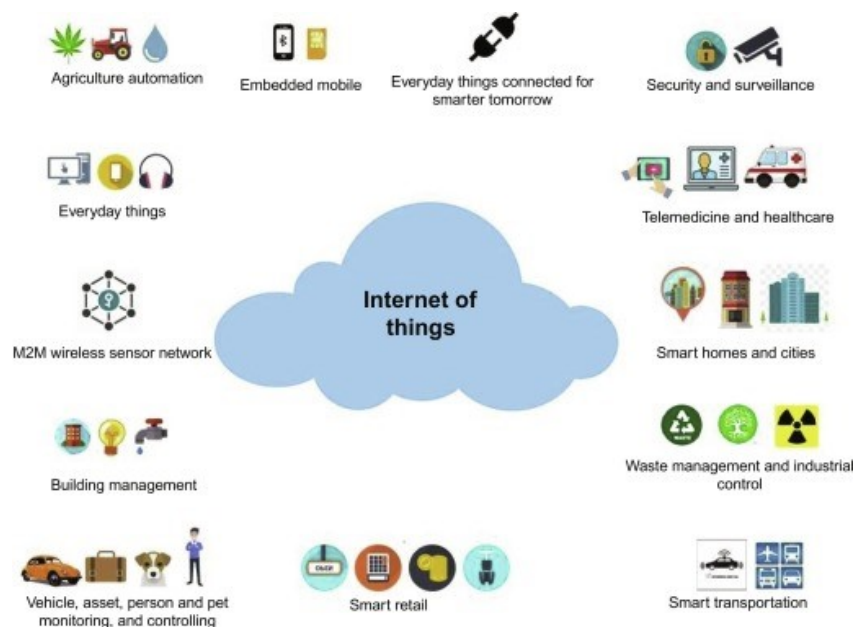
## 1.2 Internet of Things (IoT)

Il termine e il concetto di IoT sono stati coniati da uno dei membri di Radio Frequency Identification (RFID) nel 1999, ma solo dopo un decennio, questo concetto diventa realmente importante [7][8].

Nel mondo dell'IoT ci sono un gran numero di oggetti o dispositivi intelligenti, che comunicano tra loro attraverso reti pubbliche o private, connesse a Global Internet. Questi oggetti sono in grado di condividere informazioni, attraverso diversi tipi di protocolli di comunicazione (ZigBee, IPv6, IPv4, Bluetooth, WiFi, ...) e gestire i dati che ricevono. Essi sono in grado di cooperare con altri oggetti, comunemente detti "things", al fine di creare nuove applicazioni o servizi e raggiungere obiettivi comuni. Sono capaci di prendere decisioni sulla base dei dati che trasmettono e sulla base delle informazioni sui dispositivi stessi, come la durata della loro batteria e la temperatura interna del chip.

Gli oggetti che compongono una rete IoT sono molto diversi da loro, sia per il loro hardware e sia per le loro funzionalità. Ad esempio, una rete IoT molto semplice è composta da sensori di temperatura, di umidità, di pressione, telecamere IP e stampanti.

Uno dei principali obiettivi dell'IoT è di rendere disponibili gli oggetti per essere connessi in ogni luogo a qualsiasi ora e i loro servizi devono essere raggiungibili da qualunque dispositivo o persona autorizzato all'utilizzo di suddetta rete.



**FIGURA 1: PANORAMA DELL'IOT**

Possiamo definire una sorta di architettura IoT, che è utile per capire come le varie tecnologie impiegate in quest'ambito interagiscono tra loro.

### **Sensor Layer:**

è il primo livello ed è composto da oggetti smart che dispongono di sensori di vario genere. Come descritto in precedenza, i sensori sono di molteplici tipologie e misurano dati del mondo reale, convertendoli in dati leggibili anche da altri dispositivi. Sono dei dispositivi elettronici che hanno scarsa capacità computazionale e caratteristiche di funzionamento a bassa potenza.

Si parla quindi di reti di sensori, che possono essere wireless (WSN) o cablate (SN). Solitamente una rete di sensori è composta dai dispositivi che acquisiscono i dati e da un gateway che raggruppa le informazioni inviate dai sensori, giungendo ad un'architettura di rete che può essere una PAN o una LAN. Quando la rete di sensori non richiede un aggregatore, quindi un gateway, l'architettura di rete



realizzata potrebbe essere una WAN, come nel caso in cui i sensori sono collegati tra loro tramite rete GSM o LTE, e comunicano sfruttando le infrastrutture esistenti connesse a queste reti geografiche.

### **Gateways e Networks:**

il gran numero di informazioni generate dai sensori, richiede un'infrastruttura robusta e affidabile, che sia una rete cablata o wireless, come mezzo di trasporto. Queste reti possono essere di tipo privato, pubblico o ibrido e sono realizzate per garantire i requisiti di latenza, larghezza di banda e sicurezza.

I gateways, a differenza dei sensori, hanno capacità di calcolo molto maggiori, essi servono per raccogliere ed aggregare i dati trasmessi dai dispositivi del layer precedente ed hanno anche la funzione di abilitare la comunicazione tra reti eterogenee (es. rete Bluetooth, LoRa, WiFi, ...).

I gateway sono di rete, come quelli WiFi, LTE, Ethernet oppure gateway che svolgono funzioni di processing, come i microcontrollori, sistemi operativi, moduli SIM.

### **Management service:**

il management service rende possibile il processing di informazioni attraverso analisi, controlli di sicurezza, modellamento del processo e gestione dei dispositivi.

La rete di sensori si occupa di fornire i dati ottenuti dai dispositivi ad essa connessi. Questi dati hanno bisogno di essere processati o trasmessi a sistemi di post-processing, per effettuare valutazioni, svolgendo studi sulle informazioni grezze. In tale ambito, esistono molti software che permettono l'estrazione di informazioni importanti dai dati grezzi e li processano ad alta velocità.

Nel livello "Management Service", oltre la corretta gestione delle informazioni, è molto importante la loro sicurezza, quindi, è necessario introdurre delle misure di sicurezza dallo scambio di dati tra sensori fino al livello applicativo, come ad esempio autenticazione, hashing, autorizzazione.

### Application Layer:

è l'ultimo livello di questa classificazione in layer del mondo IoT, comprende quindi gli utilizzi finali dei dati provenienti dai livelli inferiori, che riguardano diversi ambiti, come le smart house, smart roads, smart factory, ecc.

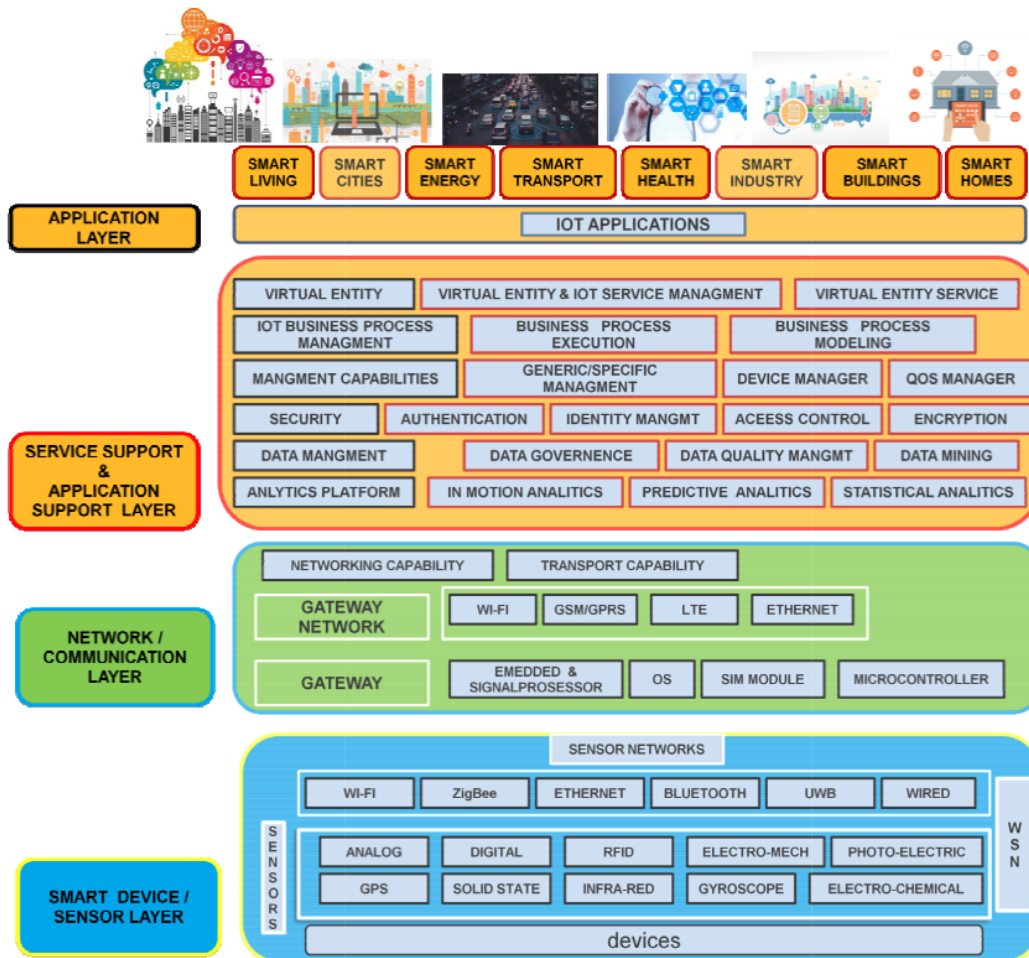


FIGURA 2: STACK DELL'IOT

Un altro modo di descrivere i layer dell'IoT che differisce leggermente dal precedente, ma più tecnico, è quello illustrato nella seguente figura, nella quale i primi due layer sono gli stessi e gli ultimi due sono diversi. Vengono introdotti i concetti di "Fog" e di "Cloud".

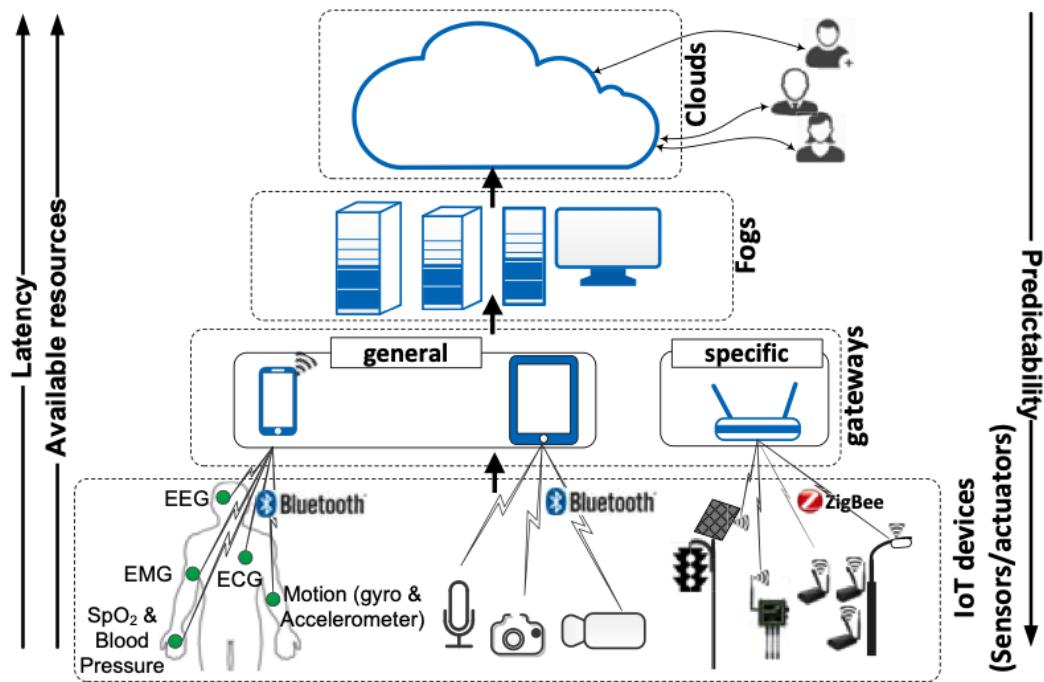


FIGURA 3: ARCHITETTURA IOT

**Fog layer:** il concetto di fog computing è un'estensione del cloud computing. I dispositivi appartenenti a questo layer forniscono una grande potenza computazionale, se confrontata a quella dei gateways ed hanno una latenza inferiore rispetto i server cloud (a seconda di dove sono collocati geograficamente e la loro distribuzione). Fog computing significa che i dati presi dal layer precedente vengono pre-elaborati in alcuni data center centralizzati prima che avvenga lo storage nel cloud.

**Cloud layer:** si occupa di fornire soluzioni per gestire i Big Data e processarli. È un layer caratterizzato da grandi capacità di calcolo e grandi capacità di memoria, che consentono di ottenere un alto QoS ed aiutare sistemi informatici e umani a prendere decisioni. I dati esaminati da questo layer saranno impiegati nelle applicazioni.

Molte applicazioni richiedono l'utilizzo di tecnologie di comunicazione wireless piuttosto che quelle cablate. Questo, soprattutto in ambito industriale, nello specifico in un plant di produzione, è molto utile, poiché solitamente sono ambienti

di grandi dimensioni e con una serie di macchinari disposti nell'area, che rendono difficile la stesura di cavi.

Quindi, si discuterà delle WSNs (Wireless Sensor Network), cioè reti nelle quali è garantita la comunicazione via onde radio tra i sensori e uno o più eventuali gateways. Rivolgersi ad applicazioni basate sulle WSNs non è sempre la scelta più semplice, soprattutto in locali industriali, nei quali la presenza di macchine, pareti e soffitti di materiale metallico, rende difficile la propagazione del segnale, inoltre alcuni macchinari che hanno componenti elettronici che funzionano a determinate frequenze, possono interferire con la rete di sensori.

Le tecnologie wireless maggiormente impiegate nel mondo dell'IoT sono [8]:

- **NFC:** è una tecnologia di comunicazione a corto raggio (fino a 20 cm). La configurazione classica è costituita da un tag che contiene una piccola quantità di dati di sola lettura o riscrivibile e da un device che legge/scrive i dati del tag, ad esempio uno smartphone dotato di modulo NFC.
- **Bluetooth:** è una delle maggiori tecnologie impiegate nell'ambito dell'IoT, le sue versioni sono Bluetooth Classic, BLE e BLE 5.x, che hanno caratteristiche molto diverse tra loro, di cui si discuterà nel capitolo x.
- **ZigBee:** una tecnologia low-power, low-cost, che supporta diversi tipi di configurazioni (mesh, stella, albero). Garantisce un largo raggio di comunicazione ed è molto utilizzata per applicazioni industriali.
- **WiFi 802.11 ah:** detto anche WiFi HaLow, è lo standard dedicato ad applicazioni che consumano una piccola quantità di potenza, trasmettendo ad un data-rate minore rispetto gli altri standard del WiFi. Questo standard soffre di meno delle interferenze causate da altri dispositivi operanti nella sua banda.
- **Rete Cellulare:** riguarda l'impiego della rete 3G ed LTE in IoT, l'unico svantaggio è il consumo di potenza dei dispositivi, che non è basso come le

altre tecnologie ed in più non sono consigliate per comunicazioni Local Network o M2M.

- **LPWAN:** il loro vantaggio principale è quello di consentire una connessione a lungo raggio, fino a 10 km di distanza tra i nodi e i gateway. I sensori trasmettono i dati con una rate minore di 1 Kbps e la banda nella quale lavorano è quella sub-GHz. SigFox e LoRaWAN sono tecnologie appartenenti a questo tipo di reti.

Seguono delle tabelle che raggruppano le principali informazioni tecniche per fare un confronto tra le tecnologie descritte, applicati a vari scenari [8]:

**TABELLA 1: DIFFERENZE TRA LE TECNOLOGIE ABILITANTI IOT**

		NFC	Bluetooth	BLE	BT v5	ZigBee	HaLow 802.11 b/g/n	LP WiFi 802.11ah	LPWAN	Cellular network	
										3G	LTE
Range	indoor	<0.2 m	1–100 m	~100 m	<300 m	<20 m	<70 m	<700 m	<10 Km	>5 Km	>5 Km
	outdoor					<1500 m	<230 m	<1000 m			
Bit rate [Mbps]		0.424	1–3	1	2	0.25	>1	0.15–40	<0.05	0.17	75–300
Throughput [Mbps]		0.22	1.5	0.30	1.5	0.15	2–50	>0.1	<0.05	NA	
freq. [GHz]		0.014	2.4–2.5	2.4–2.5	2.4	2.4	2.4/5	0.9	sub-GHz	0.8–1.9	2.1
Network topology		p2p	scatternet	star, scatternet	NA	star, tree, mesh	star	star	star	NA	

**TABELLA 2: DOMINI APPLICATIVI DELLE TECNOLOGIE IOT**

		Application domains					Local Network (M2M)
		Healthcare	Smart Cities	Smart Building	Automotive	Industry	
wireless tech.	NFC	medium	high	low	very low	very high	medium
	BLE	very high	low	low	very low	low	high
	ZigBee, BT v5	medium	high	very high	low	high	high
	WiFi b/g/n	low	high	medium	medium	low	high
	HaLow	high	very high	high	high	high	very high
	LPWAN	low	very high	high	high	very high	high
	Cellular networks (3G, LTE, etc.)	low	high	high	high	medium	very low

Dopo questa breve introduzione al mondo dell'IoT, in una visione più specifica, applicata al contesto aziendale si può dare una definizione all'acronimo IIoT (Industrial IoT) [9].

L'IIoT è l'applicazione di tecnologie IoT nell'ambito prettamente industriale, noto quindi con la nascita delle industrie 4.0, che riguardano la produzione in sé o l'energy management. Possiamo vedere l'IIoT come una ramificazione dell'IoT.

In una visione generale, l'IIoT, oltre che stabilire comunicazioni tra smart objects, dispone di funzionalità per interfacciare l'essere umano con il sistema ed uno dei suoi grandi vantaggi è di far svolgere i lavori automatici e semplici, ai dispositivi che fanno parte della rete di sensori.

L'IIoT applicata ai processi produttivi può apportare grandi migliorie nelle industrie. Gli approcci IIoT danno la priorità ai dati dei consumatori/clienti, che vengono raccolti da più fonti. Questo facilita un soddisfacimento del cliente nell'utilizzare i prodotti finiti di quella particolare azienda.

Una rete di questo tipo può ridurre i tempi di comunicazione delle informazioni, che senza l'aiuto dei sensori, sarebbero stati molto lunghi. Inoltre, aiuta a ridurre gli errori, grazie alle funzioni di monitoraggio e di manutenzione predittiva.

Dato che in un'industria 4.0 vengono impiegate nuove tecnologie, si devono considerare i fattori che possono ostacolare la loro introduzione nel mondo industriale.

**Connettività e visibilità:** il problema principale è quello di avere una buona connettività, soprattutto in un plant di produzione. Grazie all'utilizzo di sensori, le macchine comunicheranno tra loro, quindi deve essere garantita una connessione continua, senza interruzioni improvvise, ad alta velocità. Se dovesse verificarsi un blackout, un'interruzione di servizio o una perdita di connessione ad Internet, avere un sistema di fault tolerance o un sistema di backup che consente la continuità del servizio può essere una soluzione.

Se si verifica la situazione in cui un sensore si spegne o non è più connesso alla rete, in quel momento non sarà visibile nella rete IIoT, causando possibili danni.

**Sicurezza:** la questione sicurezza e privacy nelle reti IIoT sono un argomento molto caldo e delicato. Bisogna prima rendere sicuri i dispositivi IoT, quindi

difficilmente attaccabili e poi proteggere la comunicazione che avviene tra loro, attraverso appositi protocolli di sicurezza per la comunicazione. L'attenzione cade sull'argomento, se i dati che circolano nella rete, fossero dati personali o dati aziendali, che devono rimanere segreti o consultabili solo a chi ne ha l'autorizzazione. Degli attaccanti malevoli tenteranno di sfruttare le falle nel sistema e potrebbero nel peggiore dei casi causare enormi danni all'azienda.

Una rete IIoT è sicura se prevede l'applicazione di tools di sicurezza.

**Data storage:** molte aziende non tengono memoria di alcuni dati che invece potrebbero essere importanti per fare della analisi e delle verifiche e da questi report, riuscire a risolvere problemi futuri. La soluzione sarebbe quella di prevedere un sistema di memorizzazione sicura dei dati della rete IIoT.

### 1.3 Industria 4.0

Il termine "industria 4.0" viene coniato per la prima volta nel 2011 in una conferenza nella città tedesca di Hannover, indica che negli ultimi anni, il settore industriale sta subendo così tanti cambiamenti da nominare questo fenomeno, come quarta rivoluzione industriale [14][15].

Negli anni passati, si sono susseguite altre 3 precedenti rivoluzioni industriali storiche, che hanno avuto luogo in seguito alla scoperta di nuove tecnologie che hanno rivoluzionato totalmente il regime produttivo, aumentandone significativamente la produttività e cambiando completamente il concetto di industria.

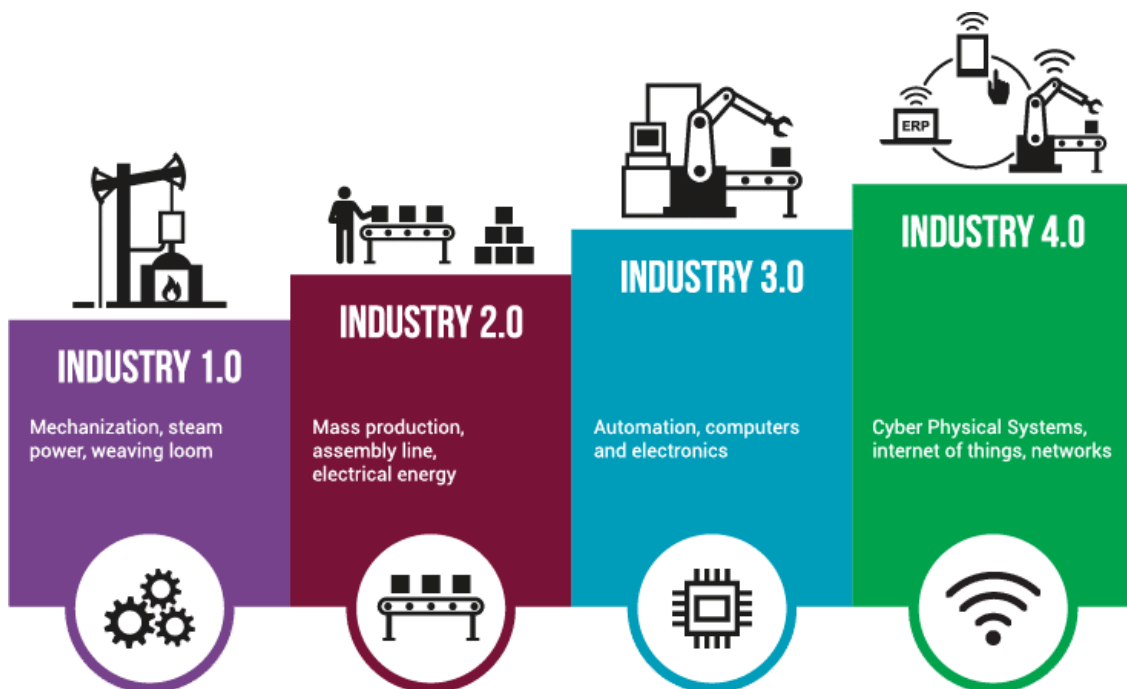


FIGURA 4: EVOLUZIONE INDUSTRIALE

- **Industria 1.0:** Nasce con la scoperta di nuove invenzioni in ambito meccanico a partire dal 1780 in Inghilterra e poi diffusosi in tutta l'Europa. L'invenzione che ha contribuito di più tra questa serie di innovazioni è sicuramente la macchina a vapore, che ha sostituito operazioni che prima di allora venivano effettuate dalla forza dell'uomo.
- **Industria 2.0:** Intorno al 1870 vennero introdotte in ambito industriale molte scoperte tecnologiche che hanno rivoluzionato il mondo, come la scoperta del petrolio e dell'elettricità. Grazie a queste innovazioni, nascono le catene di montaggio, che rendono il processo produttivo quasi automatico e lanciano il concetto e l'attuazione della produzione di massa.
- **Industria 3.0:** nasce dopo la seconda metà del Novecento, con l'avanzamento dell'era digitale e con l'implementazione dei circuiti integrati, computer e successivamente di Internet. Queste nuove features hanno permesso che nelle fabbriche ci siano macchinari controllati e gestiti con sistemi Information Technology che semplificano di molto alcune operazioni industriali.



L'industria 4.0 può considerarsi una vera e propria rivoluzione industriale in quanto con essa, si cambia pagina e si apre un nuovo capitolo che abbandona i sistemi aziendali tradizionali.

Il termine "industria 4.0" riguarda nuovi concetti e paradigmi industriali ed abbraccia un insieme di nuove tecnologie da adottare in ambito industriale, come i Cyber Physical Systems (CPSs), IoT, Cloud computing, Big Data, Cybersecurity, realtà aumentata e molti altri.

L'avvento dell'industria 4.0 è caratterizzato da una miriade di innovazioni nel campo delle tecnologie digitali ed apporta la scoperta di nuovi materiali, prodotti innovativi e nuovi processi produttivi.

L'introduzione di queste novità, oltre che migliorare la produttività dell'azienda e quindi consentire maggiori guadagni, tengono conto del fattore ambientale, come ad esempio la realizzazione di prodotti in nuovi materiali che una volta utilizzati siano biodegradabili, oppure la presentazione di nuovi macchinari che riducono gli scarti in fase di produzione, ecc.

Con l'ausilio delle innovazioni tecnologiche, i processi produttivi diventano smart ed i dispositivi, macchinari, moduli di produzione e prodotti saranno in grado di scambiare informazioni e svolgere azioni di controllo su loro stessi, realizzando così ambienti produttivi intelligenti.

Questo nuovo concetto unirà il mondo fisico al mondo digitale attraverso il CPS, con l'obiettivo di migliorare la produttività e l'efficienza dei prodotti, avendo cura delle esigenze dei clienti.

L'industria 4.0 è un concetto che abbraccia gli ambiti tecnologici di digital manufacturing, network communication, computer e automazione.

I CPSs rappresentano una delle più importanti innovazioni riguardo l'ambito computer science e information technology. Questi sistemi consistono nell'interazione tra il mondo fisico e quello virtuale, integrando, controllando e coordinando processi e simultaneamente, fornendo l'accesso all'utilizzo ed elaborazione dei dati all'interno del sistema. Il CPS viene definito come gruppo di

tecnologie innovative che consentono la gestione di sistemi interconnessi attraverso l'integrazione del loro ambiente fisico e computazionale. Nelle aree di produzione, i CPS giocano un ruolo importante, in questa specifica applicazione vengono nominati CPPS (Cyber Physical Production Systems). Essi consentono una interconnessione a tutti i livelli della catena produttiva, tra elementi autonomi e cooperativi e consentendo l'integrazione orizzontale e verticale dei sistemi IT. Quando un CPS viene abilitato alla connessione ad Internet, è meglio conosciuto come IoT, che analizzeremo nello specifico. [1]

Il vantaggio per le aziende che adottano il paradigma industria 4.0, è un aumento della produttività e della qualità dei prodotti, dovuto all'aggiunta di features tecnologiche che consentono di raggiungere questo scopo. Viene aggiunto un livello di efficienza maggiore in ogni punto della linea produttiva, in modo da ottenere un prodotto finito che rispecchia tutte le esigenze che un cliente richiede e con un tempo e un costo di produzione minore.

Pian piano un gran numero di aziende piccole medie e grandi di tutto il mondo, hanno iniziato ad approcciarsi e ad interessarsi all'introduzione di queste tecnologie nel loro ambito lavorativo, sia per i grandi vantaggi che se ne possono trarre e sia per mantenere alta la competizione con aziende dello stesso settore.

Le principali proprietà dell'industria 4.0 sono caratterizzate da 3 tipi di integrazione [1]:

- **Orizzontale:** si riferisce all'integrazione di molteplici sistemi, processi, risorse e flussi informativi relativi al campo Information Technology. Questa integrazione avviene dentro la singola organizzazione o tra diverse organizzazioni.
- **Verticale:** interessa l'integrazione tra i vari reparti e i livelli gerarchici in un'azienda, quindi riguarda la filiera produttiva, il prodotto finito, la logistica e le vendite.

- **End-to-end:** l'integrazione verticale ed orizzontale hanno l'obiettivo di fornire una soluzione end-to-end lungo l'intera "value chain", il cui scopo è quello di ridurre i costi operativi e facilitare la personalizzazione del prodotto, attraverso l'utilizzo di CPSs.

Da questa descrizione, si evince il fatto che i cambiamenti avvengono lungo tutta la linea di produzione, non solo, interesseranno anche aree diverse come il reparto R&D (ad esempio la progettazione fisica e chimica di un nuovo prodotto tramite tecnologie a realtà aumentata) e il magazzino merci (ad esempio con l'utilizzo di tecniche di localizzazione indoor dei prodotti finiti).

Nella letteratura scientifica, molti documenti danno definizioni diverse al concetto di industria 4.0, ma in alcuni di essi si possono individuare dei concetti comuni, come i paradigmi dell'industria 4.0.

I paradigmi principali dell'industria 4.0 sono 3 [2]:

- **Smart product:** sono gli oggetti e i macchinari dotati di sensori e microchips, controllati via software e connessi ad internet. Gli smart products possono memorizzare dati in modo indipendente e possono comunicare alcune informazioni all'ambiente circostante, come ad esempio quando produrre e quali parametri devono essere cambiati per l'inserimento di un nuovo articolo. In questo modo i prodotti intelligenti partecipano attivamente al processo produttivo.
- **Smart machine:** questo termine si riferisce ad un dispositivo dotato di tecnologie machine-to-machine (M2M) e/o cognitive, come il machine learning o l'IA. In questo modo le macchine possono "ragionare", prendere decisioni o risolvere problemi comuni che sorgono nell'ambito industriale. Questi dispositivi comunicheranno tra loro attraverso una rete e sarà presente un sistema di controllo locale intelligente che comunica con i

dispositivi, moduli di produzione e prodotti. In questo modo, le “smart machines” saranno in grado di migliorare i processi operativi attraverso l’auto-ottimizzazione e processi decisionali autonomi.

- **Augmented operator:** questo paradigma enfatizza l’importanza del supporto tecnologico del lavoratore, che avviene con una maggiore flessibilità e modularità. I lavoratori, in questi sistemi di produzione, hanno a che fare con una gran varietà di tasks, come monitoraggio e verifica della strategia di produzione. I lavoratori svolgono il ruolo di decisori strategici e risolutori di problemi ove le sole tecnologie impiegate nel sistema non riescono ad intervenire.

Partendo da questi 3 paradigmi, alcuni ricercatori hanno individuato 6 principi che bisogna considerare quando si ha a che fare con un’azienda che vuole approcciarsi al mondo dell’industria 4.0 [3]:

- **Interoperabilità:** è il principio più importante. Si traduce come l’abilità di due sistemi di comunicare tra loro, capirsi e utilizzare funzioni l’uno dell’altro, quindi, è la capacità di scambiare e condividere informazioni e conoscenze tra due sistemi. Questo principio determina la possibilità che avvenga la comunicazione tra prodotti, macchine e umani.
- **Virtualizzazione:** viene utilizzata per il monitoraggio di processo e la comunicazione M2M. Consente a un dispositivo di monitorare un processo fisico. I dati dei sensori sono collegati ad impianti virtuali e modelli di simulazione, che insieme formeranno la copia virtuale di un oggetto fisico (anche detto “digital twin”). Il modello virtuale è in grado di fare simulazioni di vari scenari sulla base dei dati che monitora. Ogni dispositivo può essere virtualizzato e in questo modo entrerà a far parte del sistema. Un vantaggio di questo principio è che una volta individuati dei potenziali

rischi o guasti nel modello virtuale, gli operatori potranno agire in maniera preventiva, prima che si verifichi il problema.

- **Decentramento:** significa che il personale operativo, le aziende e i dispositivi sono in grado di prendere decisioni autonomamente, invece che dipendere da un processo decisionale centralizzato. Può essere ottenuto con l'uso di un calcolatore integrato, anche detto embedded, che fornisce al personale operativo o ai dispositivi, capacità di controllo e autonomia. Un esempio di decentramento è la linea di produzione flessibile, cioè non vi è un controllo centralizzato di tutte le linee di produzione in uno stabilimento, ma la gestione avviene su ogni linea in modo indipendente. In questo modo si ottiene un processo decisionale efficiente.
- **Capacità real-time:** indica la grande velocità con la quale vengono trasmessi ed inviati i dati. Nelle aziende smart è necessario raggiungere questo obiettivo, per avere un monitoraggio delle macchine in tempo reale e poter correggere eventuali errori. Questo concetto è legato all'argomento dei Big Data, poiché ogni informazione presa dopo un certo numero di millisecondi verrà memorizzata in un sistema e questo gran numero di dati relativi a macchinari, prodotti e attrezzi verranno utilizzati per future analisi.
- **Orientazione ai servizi:** significa che i dispositivi devono essere in grado di soddisfare i bisogni degli utenti, attraverso l'internet of service. Essendo le entità del sistema produttivo tutte interconnesse, non si parlerà più del solo prodotto ma anche del servizio. Significa che in fase di progettazione del prodotto, si devono già valutare concetti come la facilità d'uso o la praticità per la manutenzione del prodotto stesso. Quindi non valutare solamente ciò che è il prodotto ma anche tutto il contorno.
- **Modularità:** fa riferimento se un dispositivo o i suoi componenti sono stati prodotti secondo uno standard. Se così fosse, potrebbero essere

modificati secondo le esigenze in modo modulare, quindi più veloce e a costi e sprechi minori.

Dopo aver parlato dei concetti chiave dell'industria 4.0, è utile elencare le principali tecnologie cardini, poiché senza di esse, non sarebbe stato possibile parlare di digitalizzazione delle industrie.

L'utilizzo di queste tecnologie è il fulcro dello sviluppo di processi di produzione smart, che inglobano dispositivi, macchine, moduli di produzione e prodotti capaci di scambiare informazioni, eseguire azioni e monitorarsi a vicenda, così da realizzare un ambiente di produzione intelligente.

Uno degli obiettivi di un'azienda che vuole accogliere i concetti di innovazione tecnologica, riuscendo a creare uno scenario in cui ogni settore è interconnesso e gode di miglioramenti dati dalla digitalizzazione di alcune funzioni, è il concetto di smart factory.

Una smart factory è uno stabilimento produttivo, nel quale avviene integrazione, digitalizzazione, uso di strutture flessibili.

Queste soluzioni consentono la realizzazione di soluzioni ed elementi intelligenti lungo la catena produttiva, che abilitano l'esecuzione di processi flessibili e adattivi. Nelle smart factories avviene quindi un'interconnessione real-time tra ogni risorsa produttiva, (sensori, macchine, robots, ...) e questo permette di migliorare la produttività [1].

Alcune di questi sviluppi innovativi dati dall'inclusione del mondo digitali sono: robotica avanzata, intelligenza artificiale, sensori hi-tech, cloud computing, IoT, data capture e data analytics, fabbricazioni digitali, Software-as-a-service e molte altre.

Nelle smart factories verranno implementati i Cyber-Physical-Systems (CPSs), cioè i sistemi che focalizzano le loro risorse all'introduzione di prodotti intelligenti e processi industriali che permetteranno all'azienda di essere pronta ai rapidi cambiamenti del mercato e di mantenere un'alta competitività con le altre aziende

del settore. Nell'articolo vengono analizzate le diverse tecnologie descritte in precedenza e viene fatto uno studio su come potrebbero venire impiegate nel caso dell'azienda in questione e se il loro impatto contribuisce al miglioramento dell'immagazzinamento di risorse, della logistica e di funzioni di approvvigionamento [4][6].

### 1.3.1 Tecnologie principali dell'industria 4.0

**IIoT:** con questo acronimo si intende la rete composta da tutti quei dispositivi che possono essere connessi ad internet, in special modo formata dai sensori, che prendono dati di diverso tipo dal mondo esterno. L'IIoT si applica in ambiti industriali, sensori per la manutenzione predittiva, bracci meccanici, carrelli a guida autonoma e così via.

Per l'IIoT è importante che i dispositivi possano comunicare correttamente tra loro senza delay o perdita di dati, soprattutto per quanto riguarda alcune applicazioni dove il requisito del real-time è molto stringente, come per le macchine a guida autonoma o robot industriali. È necessaria una comunicazione M2M, senza avere l'uomo come intermediario che gestisce le operazioni tra due dispositivi. Questo è un enorme vantaggio, in quanto incrementa sia la velocità che l'affidabilità dell'utilizzo di una rete M2M e per alcuni casi d'uso, consente anche di ridurre gli sprechi energetici.

**Big Data:** bisogna prima dare una definizione del termine "Big Data", che negli ultimi anni si è sentito spesso nominare in molti articoli scientifici e nell'ambito informatico. Esso descrive un insieme di dati informatici di grandi dimensioni che non possono essere analizzati e memorizzati con strumenti tradizionali. Serve quindi l'ausilio di strumenti che permettano di comprendere e studiare la grande mole di dati con la quale si lavora. Per compiere queste operazioni bisognerà eseguire i calcoli con elaboratori ad alta capacità computazionale. Quest'ambito è in forte crescita, poiché i dati che circolano in rete al giorno d'oggi, sono

molteplici, eterogenei ed in gran quantità (si pensi alla mole di dati che uno smartphone è capace di produrre). Sempre più tecnologie facilitano la cattura di dati, come immagini, dati di navigazione sui browser, dati provenienti dai social, dati ottenuti dai sensori e molti altri. Un sistema, che lavora con questa gran quantità di informazioni di diverso tipo, deve essere in grado di estrarli, analizzarli e metterli a confronto, in modo tale da rendere noti legami tra fenomeni che si possono verificare ed avere la capacità di prevederli in futuro.

È necessaria una potenza di calcolo parallelo eseguita da migliaia di server. I dati possono provenire sia da fonti omogenee, quindi ad esempio un sistema di calcolo che produce uno stesso tipo di dato messi dentro una struttura, come un database, oppure da fonti eterogenee. In questo caso i dati non sono strutturati e si cerca di correlarli in modo opportuno.

Le 5 “V” indicano degli obiettivi che un sistema finalizzato all’analisi e all’utilizzo dei Big Data deve raggiungere per fornire un servizio ottimale.

Le 5 “V” dei Big Data sono le seguenti:

1. **Volume**, la grande quantità di dati di un’attività;
2. **Velocità**, l’acquisizione dei dati alla velocità in cui arrivano;
3. **Varietà**, catturare dati eterogenei per ottenere informazioni dettagliate;
4. **Veridicità**, l’affidabilità dei dati della fonte;
5. **Valore**, l’importanza del valore dei dati per i processi aziendali.

**Cloud Computing:** con l’espressione “cloud” si intende un sistema di memorizzazione centralizzato, accessibile tramite connessione ad Internet. In passato i dati venivano memorizzati in server locali, quindi il fattore del luogo fisico era un vincolo per i client che dovevano accedere a certi file o programmi. Con la nascita del mondo cloud esiste la possibilità di avere a disposizione le informazioni in tempo reale e che siano disponibili, indipendentemente dal luogo fisico nel quale il client si trova.

I servizi cloud vengono offerti da un vendor, come ad esempio Google, che mette a disposizione i suoi server che verranno utilizzati dagli utenti per memorizzare i



loro dati e a seconda della quantità di dati che si vuole memorizzare, il costo di questo servizio varia, come accade con Google Drive. Altri servizi cloud, non riguardano la memorizzazione dei dati, bensì l'utilizzo di programmi che girano sui server del vendor e quindi utilizzano le loro risorse computazionali, come Google Colab.

Nell'utilizzare servizi Cloud, un argomento delicato è il trattamento dei dati, che siano personali o aziendali. Diventa critico migliorare sistemi per la sicurezza, poiché suddetti dati potrebbero essere letti o eliminati da chi fornisce questi servizi o da un hacker malintenzionato.

Nel corso degli anni, però, sono nati dei protocolli di sicurezza che garantiscono la privacy e l'integrità dei dati che rendono i servizi cloud molto affidabili e sicuri.

I servizi di cloud computing più comuni e ampiamente adottati sono [5]:

- **IaaS (Infrastructure-as-a-Service):** in questo tipo di sistemi, l'utente è responsabile del sistema operativo, delle applicazioni, del middleware e del runtime, il provider offre servizi di gestione di rete, server, virtualizzazione e storage.
- **PaaS (Platform-as-a-Service):** l'hardware e il software sono ospitati nell'infrastruttura del provider. L'utente avrà a disposizione una piattaforma sulla quale l'utente può sviluppare, eseguire e gestire applicazioni, senza dover gestire l'infrastruttura sia hardware che software.
- **SaaS (Software-as-a-Service):** è noto anche con il termine servizi applicativi cloud, un provider si occupa di fornire all'utente l'intera applicazione gestita da lui stesso, tramite un browser web. È il provider che fa operazioni di manutenzione sul software. L'utente si connetterà tramite un'API o una dashboard per utilizzare i servizi. Non bisogna installare software, si accede ai servizi tramite browser web.

**Cyber Security:** per via della grande crescita della virtualizzazione, del Cloud Computing e di tutte quelle attività che ora si possono svolgere da remoto, nasce la necessità di proteggersi da possibili attacchi da parte di utenti malevoli.

Per questo ed ulteriori motivi legati alla sicurezza, nasce la Cybersecurity. È una vasta materia di studio che ha l'obiettivo di rendere sicuri i sistemi cyber. Vengono analizzati e studiati i possibili pattern d'attacco che un utente o un gruppo di utenti malevoli potrebbero compiere e le misure di protezione dei sistemi che si potrebbero attuare per renderli sicuri e idealmente immuni da attacchi esterni.

Nel corso degli anni, per via della virtualizzazione dei servizi e dell'aumento della digitalizzazione delle aziende, diventa importante prevenire i cyber attacchi, che non solo possono causare un danno economico per l'azienda, ma anche una violazione della privacy, in quanto i dati (che siano personali o aziendali) potrebbero finire in mani sbagliate.

Le aziende stanno per l'appunto, investendo sempre più su sistemi di sicurezza cyber.

Ragionando su un ambiente di produzione, alcuni macchinari sono controllati a distanza grazie a determinati protocolli di comunicazione (si pensi ad un braccio meccanico o transpallet autonomi), inoltre con l'avvento dell'IIoT, un gran numero di dispositivi saranno connessi alla rete aziendale. È facile capire che tipo di portata di danno può causare un attacco cyber. Se un malintenzionato riuscisse ad accedere alla rete aziendale, potrebbe causare un fermo dell'attività o rubare dati aziendali segreti, mettendo economicamente in ginocchio quell'impresa. La scelta di adottare le Blockchain, come strumento di sicurezza, sta prendendo piede in molte aziende.

**Realtà virtuale e realtà aumentata:** la simulazione virtuale è utilizzata soprattutto nel settore manifatturiero, in quanto permette con delle simulazioni di valutare se è conveniente adottare una nuova tecnica produttiva, andando a considerare tutti i possibili riscontri a livello produttivo e organizzativo e potendo fare delle modifiche al modello durante la simulazione.

Questo permette un abbattimento dei costi e dei tempi di studio di queste nuove tecniche.

La realtà aumentata consente di fornire ulteriori informazioni oltre a quelle visive, su un particolare oggetto.

La realtà aumentata arricchisce l'ambiente che ci circonda con informazioni ulteriori, oltre a quelle visive che già abbiamo a disposizione. È possibile interagire con gli oggetti introdotti dall'AR tramite computer, smartphone, occhiali AR, poiché con il loro utilizzo, è possibile visualizzare elementi non visibili nella nostra realtà. Esempi di AR riguardano soprattutto il mondo dell'intrattenimento, come quello dei videogame a realtà aumentata. In ambito industriale viene utilizzata per svolgere controlli in modo accurato e sicuro.

La realtà virtuale, invece, crea un mondo nuovo, uno spazio virtuale, realizzato tramite componenti hardware e software, quindi a tutti gli effetti una simulazione. Gli strumenti CAD sono un esempio di RV, poiché con loro è possibile realizzare un modello virtuale digitale e da esso poter continuare i passi successivi della progettazione.

#### 1.4 Industria 5.0

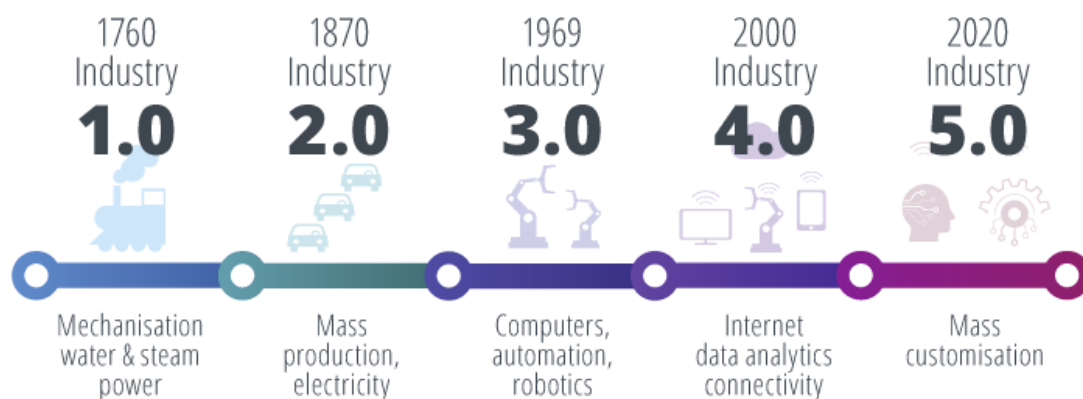


FIGURA 5: INTRODUZIONE DELL'INDUSTRIA 5.0

A partire dal secondo decennio degli anni 2000, alcuni ricercatori hanno lanciato le basi di studio per l'avvento di una nuova rivoluzione industriale di cui alcune applicazioni pratiche vengono già attuate in alcune industrie manifatturiere [10].

Con la crescita dell'industria 4.0, le macchine assumono un ruolo centrale e subiscono una nuova concezione del loro termine, diventando macchine intelligenti, in grado di prendere decisioni riguardanti il processo produttivo. Il ruolo dell'essere umano nell'industria rimane comunque rilevante ma passa in secondo piano.

Con l'industria 5.0, invece, l'uomo diventa fondamentale. Ci si aspetta che l'alta velocità e la precisione di calcolo delle macchine si uniscano alle capacità cognitive e creative degli umani.

La "mass personalization" è uno degli obiettivi principali dell'industria 5.0, questo termine indica che le aziende realizzeranno per i consumatori prodotti personalizzati e su misura, in base al loro gusto e le loro esigenze.

L'industria 5.0 incrementerà significativamente l'efficienza produttiva e creerà versatilità tra uomini e macchine e la loro collaborazione porterà ad un'espansione della produzione ad un ritmo rapido. Il modus operandi delle industrie innovative prevede che i task monotoni e ripetitivi vengano eseguiti dalle macchine, invece, i task che richiedono pensiero critico e ragionamenti difficili, verranno affidati ad un personale qualificato.

**TABELLA 3: PRINCIPALI DIFFERENZE TRA INDUSTRIA 4.0 E 5.0**

<b>Industria 4.0</b>	<b>Industria 5.0</b>
Produzione su larga scala	Produzione secondo l'esigenza dei consumatori
Maggior importanza ai CPSs	Maggior importanza al fattore umano, che si relazionerà con i cobots
Fattore ambientale non come obiettivo principale	Dà priorità a tecnologie green

L'industria 4.0 ha messo al centro dei bisogni l'incremento della produttività e l'abbattimento dei costi di produzione, inserendo nei processi industriali tutte quelle tecnologie descritte in precedenza. Uno dei lati negativi di questa scelta è il fatto di non dare la giusta importanza al fattore umano, poiché alcuni lavori più automatici, sono stati rimpiazzati dalle macchine, trovando lo scontento dei sindacati. Nell'industria 5.0 si cerca di risolvere questo lato negativo, aumentando la partecipazione dell'uomo nei processi produttivi.

Un altro argomento fondamentale è l'inquinamento prodotto dai processi industriali, il quale subisce un sostanziale incremento a partire dalle scoperte tecnologiche che hanno dato origini alle rivoluzioni industriali, come ad esempio le macchine a vapore che dovevano essere alimentate dalla combustione del carbone che è altamente inquinante. Le industrie manifatturiere, soprattutto negli ultimi decenni, hanno cercato di contenere gli sprechi e ridurre l'impatto ambientale, ma l'argomento non è mai stato posto in cima ai fabbisogni principali. L'industria 5.0 assicura sostenibilità ambientale, riducendo i materiali di scarto, attraverso la bioeconomia, cioè l'economia volta all'uso di risorse naturali rinnovabili e sulla loro trasformazione in beni e servizi finali o intermedi.

#### **1.4.1 Nuovi argomenti di studio nell'industria 5.0**

##### **Smart additive manufacturing:**

è un argomento riguardante la produzione sostenibile, cioè l'approccio economicamente più popolare per le attuali industrie manifatturiere, che supportano i produttori nell'esecuzione di piani di sviluppo, nella riduzione dell'inquinamento e nell'utilizzo delle risorse durante tutto il ciclo di vita dello sviluppo.

L'applicazione della produzione sostenibile diventa possibile, adoperando l'insieme di tecnologie che contraddistinguono l'industria 4.0, con l'aggiunta di alcune features.

Si parla di Smart Additive Manufacturing (SAM), un termine che definisce i vari processi di produzione che saranno divisi in livelli. SAM ha la capacità di ridurre i costi energetici, aiutare il consumo di materiali e risorse e guida la produzione sostenibile per l'ambiente.

SAM consente di ottimizzare i processi coinvolti nella gestione della supply chain e ridurre i tempi di consegna dei prodotti. La supply chain è una rete che comprende persone, risorse, tecnologie e attività che riguardano la realizzazione di prodotti a partire dalle materie prime.

### **Manutenzione predittiva:**

altro argomento importante, riguarda la manutenzione predittiva. Diventa un tema principale quando si parla di manufacturing 4.0, poiché consente di aumentare la qualità e la produttività, riducendo gli errori che possono verificarsi durante il processo produttivo.

In passato, la manutenzione dei macchinari veniva eseguita in modo manuale, quindi, era il lavoratore che verificava se il macchinario funzionava a dovere oppure doveva essere riparato, ora nelle smart factories, chi si occupa del monitoraggio sono proprio i sensori, che trasmetteranno dati ad un sistema che li analizzerà in modo opportuno e da questa analisi si dedurrà preventivamente se il funzionamento di quel macchinario è corretto.

Il fatto di poter sostituire un componente o l'intero macchinario prima che avvenga la sua interruzione di servizio è una cosa molto importante, perché le macchine che partecipano al processo produttivo devono essere sempre disponibili e devono avere un alto tasso di affidabilità.

Esistono in letteratura dei prediction tools che processano i dati e fanno delle stime in modo tale che il personale addetto sia in grado di prendere decisioni sulla base delle informazioni apprese. L'implementazione di reti IoT fornisce un framework base per implementare la manutenzione predittiva.

### **Hyper customization:**

nell'industria 4.0 non si è tenuto conto del fattore di customizzazione che diventa sempre più importante. Quindi, con la crescita della tendenza, molte aziende decideranno di investire sulla personalizzazione dei prodotti.

L'utilizzo di tecnologie come AI, ML, sistemi cognitivi e computer vision, con la collaborazione del fattore umano, riescono a calcolare e individuare quali sono i prodotti, servizi e contenuti che piacciono e potrebbero piacere ai consumatori. L'obiettivo per implementare la personalizzazione di massa è di ottenere la massima accuratezza con il minimo costo, quindi, prima capire i gusti dei clienti e poi avviare un processo di personalizzazione dei prodotti, quindi fornire varianti di quel prodotto.

### **Cyber physical cognitive systems CPCS:**

nell'industria 4.0 i CPS diventano essenziali per implementare il progresso tecnologico di un'azienda, i processi produttivi da sistemi completamente manuali hanno trovato una transizione digitale, verso i CPS.

Nell'industria 5.0 i CPS vengono impiegati in processi cognitivi, come ad esempio la sorveglianza, l'automazione industriale e il monitoraggio ambientale, vengono anche detti CPCS. Le capacità cognitive come lo studio e l'osservazione dell'ambiente e il fatto di eseguire azioni, di conseguenza sono contenute nei nodi di un CPCS.

#### **1.4.2 Applicazioni dell'industria 5.0**

**Intelligent healthcare:** i medici, negli ospedali più tecnologici, utilizzano sistemi di Machine Learning come strumento d'aiuto per diagnosticare patologie ai pazienti. Una funzionalità che garantisce esigenze personalizzate per ogni paziente, come il monitoraggio di pressione sanguigna, livello di zuccheri e fornire un trattamento personalizzato ai pazienti con l'assistenza dei medici, è una feature molto richiesta ai giorni nostri. Questo sarà reso possibile, grazie alle tecnologie che seguono il concetto di industria 5.0, ad esempio tramite una molteplicità di

sensori che prendono dati biometrici e comunicano i risultati al sistema che sarà in grado di dare in output una diagnosi.

**Cloud manufacturing:** riprende alcuni concetti analizzati nell'industria 4.0, come l'IoT e il Cloud computing, quindi, gode di tutti i vantaggi che essi apportano in ambito industriale.

Il Cloud manufacturing raggruppa un insieme di tecnologie che permettono di avere un operato efficiente e una diminuzione dei costi di produzione, considerando anche l'impatto ambientale.

In questo modo, avendo la possibilità di far funzionare i sistemi di produzione in cloud, alcune industrie decideranno di effettuare un dislocamento del reparto della produzione, nei pressi dei luoghi di raccolta delle materie prime, in modo da ridurre i costi di trasporto o in luoghi dove il costo di produzione è minore.

Le informazioni riguardo il processo produttivo vengono collezionate tramite i sensori della rete IoT e analizzate in Cloud.

Ci si aspetta che nell'immediato futuro, l'integrazione del Cloud Manufacturing con tecnologie evolute come AI, ML, reti 5G, espanderà le capacità dei sistemi basati sul Cloud Manufacturing.

**Supply chain management (SCM):** il paradigma della personalizzazione di massa dell'industria 5.0 richiede che ci sia un cambiamento dell'organizzazione dei vari livelli di una linea di produzione.

Per realizzare una corretta gestione della supply chain, si potrebbe utilizzare un gemello digitale di essa. Il gemello digitale supporta l'intero ciclo di vita di SCM, dalla costruzione alle operazioni e attraverso la simulazione di sistemi SMC real-time, il gemello digitale riesce a prelevare dati dal mondo reale grazie ai sensori IoT.

Il gemello digitale aiuta le industrie nel ridurre i costi operazionali ed aumentare i margini di produzione durante le fasi produttive.



### 1.4.3 Nuove tecnologie abilitanti nell'industria 5.0

**Edge Computing (EC):** è relativo al processamento dei dati che avviene dopo il livello “gateways” dell'IoT. EC consente di far incontrare costi di latenza, limiti circa la vita della batteria, requisiti di tempi di risposta, protezioni dati e privacy. EC fornisce comunicazioni real-time per applicazioni industriali future, come i veicoli autonomi o il monitoraggio di pazienti da remoto.

**Digital twins (DT):** viene chiamata così la replica digitale di un sistema fisico o di un oggetto. Grazie all'IoT è stato possibile implementare l'idea di DT ed è oggi accessibile a varie industrie. I dati forniti dai dispositivi IoT vengono utilizzati per eseguire la rappresentazione digitale per una simulazione. L'importanza di crescita dei DT è data anche dall'avanzamento dell'AI, ML e Big Data Analytics.

DT in industria 5.0 offre un valore significativo per la personalizzazione dei prodotti sul mercato, migliorando la user experience. Inoltre, migliora alcune funzioni aziendali, riduce i difetti e aumenta la velocità di crescita di modelli aziendali innovativi.

**Cobots:** con i grandi cambiamenti nel campo dell'AI, tutti i dispositivi che hanno capacità computazionali diventano più “smart” ed è stata introdotta una nuova tecnologia chiamata cobot. Un cobot è un robot collaborativo, progettato per collaborare attivamente con l'essere umano.

Di solito vari sensori sono integrati ai cobots, che li rendono molto più intelligenti e sicuri. L'aiuto dei cobots garantisce una produzione ad alto volume per ciò che riguarda i processi produttivi e aiutano ad avviare la personalizzazione di massa, ma non hanno pensiero critico come gli umani.

**Internet of everything (IoE):** IoE è l'interconnessione tra persone, processi, informazioni e cose. Il ruolo dell'IoE nell'Industria 5.0, migliora la soddisfazione dei clienti, costruendo un'esperienza di personalizzazione basata sui dati generati

dall'IoE. Un altro vantaggio che apporta è di minimizzare gli sprechi nella supply chain e ottimizza i processi produttivi. L'implementazione dell'IoE avviene principalmente con reti di sensori wireless, per tutti i vantaggi che apporta la comunicazione senza fili.

**Blockchain:** un problema dell'industria 5.0 è il controllo centralizzato di un gran numero di dispositivi, la Blockchain può essere un'ottima soluzione. Questa tecnologia implementa una comunicazione sicura peer-to-peer e gestisce un registro immutabile nel quale vengono memorizzati dei records. Sul registro si possono compiere operazioni con una completa trasparenza e in modo tale che le informazioni di chi scrive sul registro rimangano private.

La blockchain può essere utilizzata per creare identità digitali a diverse entità in un'Industria 5.0, e garantisce lo scambio sicuro di dati. Inoltre, la produzione cloud basata su blockchain facilita la connessione a livello di macchina e la condivisione dei dati basata sulla tecnologia blockchain.

## 2 Indoor Positioning Systems

Uno degli argomenti più importanti del mondo IoT, riguarda la ricerca di oggetti o cose all'interno o all'esterno di edifici, complessi, residenze ecc. Nasce quindi, la necessità di localizzare oggetti per fini diversi, come ad esempio conoscere la loro posizione all'interno di una stanza oppure tracciare il percorso che compie un robot.

Le tecnologie di questo tipo sono rese possibili grazie all'utilizzo di dispositivi che calcolano la posizione degli oggetti, con un certo margine d'errore. Per ciò che riguarda la localizzazione outdoor, il più delle volte, si sfruttano le tecnologie satellitari.

La più importante a livello globale è il GPS, un sistema gestito dal governo degli USA, fin dal 1973 e accessibile da chiunque disponga di un dispositivo con modulo GPS (come gli smartphones).

Inizialmente era nato per scopi militari, ma poi, vista la sua utilità, venne applicato in vari contesti. I satelliti, in orbita a 26560 km dal centro della terra, interagiscono con i dispositivi GPS a terra e grazie a particolari modulazioni e processamenti del segnale, i satelliti riescono a captare il segnale dei dispositivi, per poi calcolare la loro posizione geografica, identificata da latitudine e longitudine, tramite la triangolazione.

I satelliti sono disposti in orbita in modo tale da coprire tutta la superficie terrestre. Esistono anche altre alternative al sistema GPS, come NavIC (sistema di navigazione satellitare indiano), GLONASS (sistema di navigazione satellitare russo), Galileo (sistema di navigazione satellitare Europeo) alcuni di essi hanno un'area di copertura regionale e non globale.

I sistemi satellitari che offrono una copertura a livello globale sono detti GNSS (Global Navigation Satellite System) Seppur offrono una precisione di localizzazione maggiore rispetto al GPS (che è di circa 10 m), esso rimane il sistema più utilizzato e conosciuto a livello globale.

Di conseguenza, quando si parla di localizzazione outdoor il più delle volte ci si rivolge al GPS, che essendo un servizio gratuito e standardizzato riesce a risolvere problemi che richiedono un'accuratezza non troppo stringente.

Ovviamente per avere una precisione più accurata, bisogna che tra il dispositivo ricevitore e i satelliti che effettuano la triangolazione, vi sia la condizione di LoS, altrimenti l'onda elettromagnetica fa fatica a giungere al ricevitore, soprattutto se si trova all'interno di un edificio.

Per questo principale motivo è impensabile utilizzare un sistema di GNSS per la localizzazione all'interno di costruzioni, ammesso che il dispositivo riesca a comunicare con i satelliti, l'errore di posizione sarebbe troppo elevato, in quanto la propagazione delle onde elettromagnetiche risulta ostacolata durante il loro percorso.

Al momento, non esiste un sistema standard che offre alte prestazioni, poiché ogni ambiente è diverso, quindi, cambiano le caratteristiche di propagazione del segnale. Effettuare la localizzazione in un magazzino merci, ad esempio, è molto

più semplice rispetto un ufficio, in cui la presenza di ostacoli come muri, scrivanie e persone in movimento rende difficile la trasmissione delle onde elettromagnetiche.

Inoltre, bisogna considerare anche il tipo di materiali che compongono le parti di un certo luogo, perché le onde elettromagnetiche al variare della frequenza interagiscono diversamente con essi.

Per questi motivi, è necessario effettuare uno studio del locale e poi capire quale sistema di localizzazione è più adatto allo scopo.

Il termine che raggruppa tutte quelle tecnologie utilizzate per effettuare la localizzazione di dispositivi è IPS.

Come detto in precedenza, la localizzazione all'interno di spazi chiusi si è espressa come una sfida per molti ricercatori. A differenza della localizzazione all'esterno, che può essere implementata dai sistemi GNSS, quindi, grazie a informazioni inviate dai satelliti si riesce ad ottenere la posizione di un ricevitore a terra, con un relativo errore di posizionamento, per applicazioni comuni, come ad esempio la ricerca della posizione di uno smartphone con GPS ha un errore medio è di circa 10 m.

È stata investita molta ricerca negli Indoor Positioning Systems. Le problematiche legate a questo discorso sono non poche, poiché ogni locale ha una sua disposizione dei muri, degli armadi, scrivanie, colonne e tutti gli oggetti di grandi dimensioni che possono disturbare la propagazione di onde elettromagnetiche, quindi, ogni per ogni locale si dovrebbe progettare un sistema di IPS ad hoc per lo specifico caso.

Bisogna combattere con i fenomeni di riflessione, scattering, rifrazione che causano deviazioni delle onde. I principali motivi sono gli effetti di multipath e shadowing.

Altro problema da valutare è l'effetto di interferenza che può generare un sistema IPS o viceversa interferenze generate da altri dispositivi che generano disturbo all'IPS. Ad esempio, in ambito ospedaliero, può accadere che l'uso di un certo tipo

di tecnologie (come RFID), interferisca con dispositivi medici, che lavorano nella stessa banda di frequenze, ciò non deve mai accadere per ovvi motivi.

## 2.1 Parametri e tecniche per il calcolo della posizione

Prima di illustrare i principali parametri utilizzati per calcolare la posizione tramite un IPS, bisogna definire i 3 principali tipi di localizzazione [13]:

- **Device based localization (DBL):** un dispositivo user utilizza dei nodi di riferimento per ottenere la sua locazione.
- **Monitor based localization (MBL):** un set di nodi di riferimento ottengono passivamente la posizione di un dispositivo user.
- **Proximity detection:** si vuole trovare la stima della distanza tra un user e un Point of Interest (PoI), cioè un punto fisso.

### 2.1.1 Received Signal Strength Indicator (RSSI)

È uno degli approcci più semplici e più largamente utilizzati per la localizzazione indoor. La forza del segnale ricevuto è misurata al lato ricevitore e tipicamente è espressa in decibel-milliwatt (dBm) o in milliwatt (mW), viene usata per stimare la distanza tra ricevitore e trasmettitore, maggiore è il valore dell’RSS e minore sarà la distanza tra i due dispositivi. La distanza assoluta può essere stimata usando diversi modelli di propagazione del segnale, a seconda del tipo di scenario considerato, avendo come dato noto la potenza del segnale trasmesso da un dispositivo di riferimento.

L’RSSI è un indicatore dell’RSS, cioè una misurazione relativa dell’RSS che ha unità arbitrarie (esempio da 0 a 100) ed è definita tipicamente dal produttore del chip.

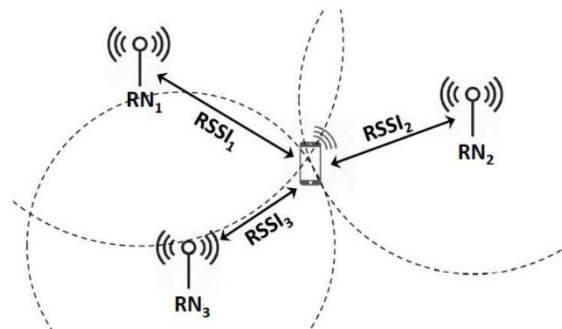
Utilizzando l’RSSI insieme a un modello di pathloss semplice, si può estrarre il dato della distanza “d”:

$$RSSI = -10n \log_{10}(d) + A \quad (1)$$

$$d = 10^{(A - RSSI)/10n} \quad (2)$$

Il termine “ $n$ ” è l’esponente di pathloss (che vale 2 in free space e tra 4 e 6 in edifici con oggetti di grandi dimensioni) ed “ $A$ ” è il valore dell’RSSI ad una distanza di riferimento dal ricevitore.

Nel caso DBL è richiesta la trilaterazione o la multi-laterazione per identificare la posizione di un dispositivo. Quindi, il dispositivo ottiene i dati di RSS per stimare la distanza assoluta tra lui stesso e i punti di riferimento e in seguito per il calcolo della sua posizione vengono applicate semplici regole geometriche.



**FIGURA 6: TRILATERAZIONE E TRIANGOLAZIONE ATTRAVERSO SEGNALI RSSI**

Nel caso di MBL, invece, viene calcolato il valore di RSS ai nodi di riferimento e questi ultimi inviandosi le informazioni, riescono a calcolare una stima della posizione esatta del dispositivo target. Un altro modo è quello di inviare i valori di RSS collezionati dai nodi ancora a un controllore centrale che riceve, analizza ed elabora i dati e infine fornisce la posizione di un determinato target. Nel caso di servizi basati sulla prossimità, c’è bisogno di un solo nodo di riferimento, viene stimata la prossimità del target usando il modello di pathloss più conforme alla situazione stimando la distanza dal punto di riferimento.

Il grande svantaggio dei metodi basati su RSS è la bassa accuracy dei risultati. Influisce pesantemente la presenza di muri e ostacoli di grandi dimensioni, che causano attenuazione del segnale e bisogna valutare le fluttuazioni dei valori di RSS dovute dal multipath.

Per mitigare questi effetti negativi, applicando opportuni filtri del segnale (uno dei più famosi è il filtro di Kalman), può migliorare l'accuratezza dell'algoritmo di localizzazione.

### 2.1.2 Channel State Information (CSI)

In molti sistemi wireless come quelli basati sullo standard IEEE 802.11 o UWB, la banda di coerenza del canale wireless è minore della banda del segnale.

Se essa è minore della banda del segnale, accade che l'effetto del canale non è piatto ma diventa selettivo, quindi può generare interferenza intersimbolica e la conseguente degradazione del segnale. Inoltre, in un transceiver multi-antenna le risposte in frequenza del canale per ogni coppia di antenna sono varie, ciò dipende dalla distanza tra le antenne e la lunghezza d'onda del segnale.

Parametri come il CIR (Channel Impulse Response) o il suo duale nel dominio delle frequenze o la Channel Frequency Response (CFR), risultano essere più granulari rispetto l'RSS, infatti, possono ottenere sia l'ampiezza che la fase delle risposte del canale alle diverse frequenze, tra ricevitore e trasmettitore.

La risposta del canale in frequenza può essere scritta nella sua forma polare:

$$H(f) = |H(f)|e^{j\angle H(f)} \quad (3)$$

Dove  $|\cdot|$  indica l'ampiezza e  $\angle$  indica la fase della risposta del canale a una certa frequenza " $f$ ".

Ad oggi, esistono dei chip IEEE 802.11 che forniscono misurazioni del canale a livello delle sotto-portanti per sistemi che usano la modulazione OFDM, che

possono essere tradotte in informazioni dettagliate del multipath, misurazioni più stabili e una accuratezza di localizzazione maggiore.

### 2.1.3 Fingerprinting/ Scene Analysis

Questa tecnica consiste nel memorizzare diverse misurazioni dell’RSSI in punti diversi del locale, durante la fase off-line. Durante la fase on-line vengono confrontati i valori di RSSI raccolti in real-time e confrontati con quelli memorizzati in precedenza, per stimare la posizione del target. Solitamente i valori di fingerprint sono espressi in RSSI o tramite CSI.

Per poter trovare un match tra i valori nella fase off-line e quelli nella fase on-line, sono stati sviluppati diversi tipi di algoritmi che vengono distinti in base ai loro principi ai quali si basano:

1. **Metodi probabilistici:** fanno affidamento sulla stima di verosimiglianza tra i valori ottenuti in real-time e quelli memorizzati in precedenza. Supponendo che un set di posizioni candidate sia  $L = \{L_1, L_2, \dots, L_m\}$ , per ogni valore del vettore di RSSI trovato in fase on-line “ $O$ ”, la posizione del target è uno di quegli elementi “ $L_j$ ” dell’array “ $L$ ” se:

$$P(L_j|O) > P(L_k|O) \quad \text{per } j, k = 1, 2, 3, \dots, m \quad k \neq j \quad (4)$$

Ciò mostra che un target si troverà nella posizione stimata  $L_j$ , se la sua stima, è maggiore di quella di ogni altra posizione.

Se  $P(L_i) = P(L_k)$  per ogni valore di “ $i$ ” e “ $j$ ” usando il teorema di Bayer si ottiene la probabilità del vettore di segnale osservato “ $O$ ”, data la posizione del target “ $L_j$ ”, in termini probabilistici  $P(O | L_j)$ . Il target verrà identificato nella posizione “ $L_j$ ” se:



$$P(O|L_j) > P(O|L_k) \quad \text{per } j, k = 1, 2, 3, \dots, m \quad k \neq j \quad (5)$$

La funzione di probabilità verrà calcolata come prodotto di tutte le probabilità calcolate da tutti i nodi di riferimento.

Si può ottenere una stima della posizione più accurata, riducendo le distanze tra i punti di misurazione che si registrano nella fase offline, ottenendo una griglia più densa. Però, in questo modo, la differenza tra gli RSS di due punti vicini, sarà inferiore al valore di forza del segnale dovuta alle irregolarità del canale, rendendo difficile la stima corretta della posizione. Bisogna trovare quindi un trade-off tra la granularità del metodo fingerprinting e la probabilità di trovare la posizione giusta. Bisogna anche tener conto se questa tecnica è applicabile, poiché alcuni luoghi sono soggetti a cambiamenti fisici continui.

2. **Artificial Neural Networks (ANN):** la rete neurale ha bisogno di essere allenata, quindi, si utilizzano come dati di training i valori di RSSI in diverse coordinate note del locale, nella fase offline. Una volta allenata, la ANN restituirà come risultato la locazione del target dalle misurazioni dell’RSSI ottenute dalla fase online.
3. **K-Nearest Neighbor (KNN):** è una tecnica di machine learning utilizzata soprattutto in ambito di classificazione. Consiste nell’ottenere dei k-nearest matches (cioè delle corrispondenze tra valori vicini secondo un fattore “k”) tra i valori dell’RSSI calcolati al momento e quelli memorizzati, in posizioni note, nella fase offline, usando il root mean square error (RMSE). Le prestazioni sono influenzate dal valore “k” che dev’essere accuratamente scelto a seconda dei dati con i quali si sta lavorando. Le corrispondenze che hanno un RMSE più piccolo, vengono mediate per ottenere una stima della locazione del target.
4. **Support Vector Machine (SVM):** un’altra famosa tecnica di machine learning usata per la classificazione di dati.

È una tecnica più affidabile rispetto quella che utilizza la triangolazione con RSSI, perché non dipende fortemente dal modello di pathloss, anche gli effetti pseudocasuali che possono causare errore nelle misure non agiscono. L'unico svantaggio è quello di dover eseguire una fase di registrazione dei valori di RSSI in molti punti per costruire una mappa di valori RSSI, ciò è difficile da applicare in scenari molto grandi e dinamici, in aggiunta bisogna fare una fase di training offline.

#### **2.1.4 Angle of Arrival (AoA)**

Per applicare questa tecnica è necessario avere a disposizione degli array di antenne al lato ricevitore, che stimano l'angolo col quale incide l'onda elettromagnetica in arrivo, rispetto l'asse in cui si trova l'array di antenne.

Il vantaggio di questa modalità è che la posizione 2D di un target può essere stimata utilizzando 2 ricevitori (nel caso 3D i ricevitori richiesti ne sono 3) che non hanno bisogno di sincronizzazione dei clock tra tag ed antenne. In più, il calcolo dell'AoA fornisce un'accurata stima quando la distanza trasmettitore-ricevitore è breve, ma rispetto le tecniche RSS-based, richiede un hardware più costoso e operazioni di calibrazioni iniziali delicate. Un piccolo errore sull'angolo, se il trasmettitore e il ricevitore sono distanti, si traduce in un enorme errore di posizione.

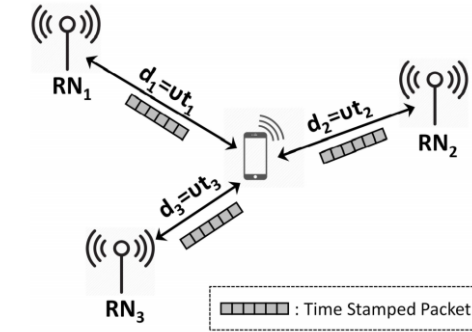
è comunque un metodo molto utilizzato se si vuole ottenere dei livelli alti di accuracy di localizzazione.

#### **2.1.5 Time of Flight (ToF)**

Chiamato anche con un altro nome, Time of Arrival (ToA), è una tecnica che sfrutta il tempo di propagazione del segnale in un certo ambiente, per calcolare la distanza tra un trasmettitore e un ricevitore tramite la formula:

$$d = c \cdot t_d \quad (6)$$

in cui “ $c$ ” è la velocità della luce, “ $t_d$ ” è il ToF, cioè una differenza di tempi.



**FIGURA 7: RAPPRESENTAZIONE GRAFICA DEL TOF**

In figura viene mostrato il ToF per 3 diversi nodi di riferimento che serve ad estrarre le 3 informazioni della distanza tra nodo di riferimento e target e in seguito vengono applicate le regole geometriche che consentono di calcolare la posizione del target. Questo è un approccio molto simile a quello basato su RSS e viene valutato allo stesso modo per entrambi gli scenari DBL e MBL.

ToF richiede una sincronizzazione temporale stringente tra i trasmettitori e i ricevitori, in molti casi per implementare la sincronizzazione, ogni dispositivo trasmette oltre al segnale informativo anche un timestamp.

I fattori più rilevanti che degradano l'accuracy del ToF sono la banda del segnale e la rate di campionamento. Un basso sampling rate riduce la risoluzione del ToF, bisogna comunque rispettare la legge di Nyquist per il campionamento.

In ambienti indoor affetti da multipath, più è larga la banda del segnale e più precisa è la stima del ToF. Le tecniche di super-risoluzione nel dominio della frequenza sono utili per ottenere valori di ToF più precisi, ottenendo un'alta risoluzione della risposta in frequenza del canale. Il problema sorge quando non è garantito il cammino diretto tra trasmettitore e ricevitore, poiché i valori di ToF saranno molto distanti da quelli reali. Gli ostacoli deflettono il segnale, che arriva al ricevitore in un tempo maggiore, dando l'informazione errata sul ToF.

Generalmente la misurazione diretta di ToF incorre in due problemi, uno è che tutti i ricevitori e i trasmettitori devono essere tutti sincronizzati in modo preciso, il secondo è la necessità di etichettare un timestamp all'interno del segnale trasmesso. Il ToF può essere misurato attraverso tecniche come direct sequence spread-spectrum (DSSS) o misurazioni UWB.

Un approccio semplice utilizza una tecnica geometrica per calcolare i punti di intersezioni delle misure ToF. La posizione del target può essere calcolata minimizzando la somma dei quadrati di una funzione costo non lineare, come ad esempio l'algoritmo least-square.

Considerando che il target si trovi in una posizione  $(x_0, y_0)$  e trasmetta segnale al tempo " $t_0$ ". Sono presenti  $N$  stazioni riceventi di coordinate  $(x_i, y_i)$  che ricevono il segnale a un tempo " $t_i$ ".

La funzione costo sarà:

$$F(\mathbf{x}) = \sum_{i=1}^N \alpha_i^2 f_i^2(\mathbf{x}) \quad (7)$$

Con:

$$f_i(\mathbf{x}) = c(t_i - t) - \sqrt{(x_i - x)^2 + (y_i - y)^2} \quad (8)$$

Dove  $\alpha_i$  viene scelta a seconda di quale è l'affidabilità del segnale ricevuto al ricevitore " $i$ ". la velocità della luce è " $c$ " ed  $\mathbf{x} = (x, y, t)^T$ . Questa funzione viene formata per ogni ricevitore ed  $f_i(\mathbf{x})$  diventa 0 scegliendo i giusti parametri  $x, y$  e  $t$ . Minimizzando la funzione  $F(\mathbf{x})$  si ottiene una stima della posizione. Altri algoritmi basati sul ToF sono il Closest Neighbor (CN) e il RWGH. Il primo stima la posizione dell'utente come la posizione dell'access point più vicino a lui e il secondo è una specie di algoritmo Least Squares pesato che funziona anche per scenari NLOS.

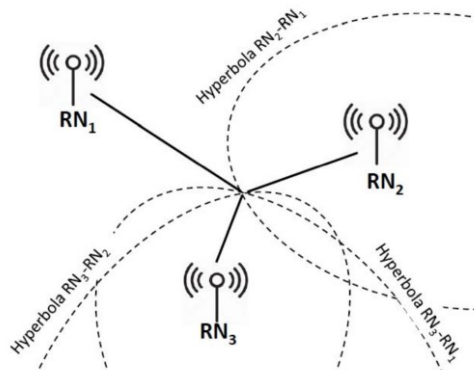
### 2.1.6 Time Difference of Arrival (TDoA)

Si basa sulla differenza in tempi di propagazione dei segnali da diversi trasmettitori, misurati al lato ricevitore. Si distingue dalla tecnica del ToF, in quanto in quel caso viene utilizzato il tempo assoluto di propagazione del segnale. Nel TDoA, le quantificazioni del tempo sono espresse in questo modo,  $T_{D(i,j)}$  dove  $i,j$  sono i trasmettitori. Da quel dato si può ricavare il valore della distanza fisica,  $L_{D(i,j)} = c T_{D(i,j)}$ .

Il ricevitore è individuato nel punto in cui si intersecano gli iperboloidi, dati dall'equazione:

$$L_{D(i,j)} = \sqrt{(X_i - x)^2 + (Y_i - y)^2 + (Z_i - z)^2} - \sqrt{(X_j - x)^2 + (Y_j - y)^2 + (Z_j - z)^2} \quad (9)$$

In cui  $(X_i, Y_i, Z_i)$  sono le coordinate del nodo di riferimento “ $i$ ”, cioè il trasmettitore e  $(x,y,z)$  sono le coordinate del target ricevitore.



**FIGURA 8: RAPPRESENTAZIONE GRAFICA DEL TDOA**

Il TDoA utilizza almeno 3 trasmettitori per calcolare l'esatta posizione di un ricevitore, data dall'intersezione di 3 o più iperboloidi. Il sistema di equazioni di iperbole può essere risolto attraverso la regressione lineare o linearizzando le equazioni con l'espansione in serie di Taylor.

Nella figura è mostrato come avviene una localizzazione 2D di un certo nodo ricevente. L'accuracy della stima del TDoA dipende anch'essa dalla banda del

segnale, dalla rate di campionamento del ricevitore e dall'esistenza della condizione di LoS tra ricevitore e trasmettitore.

Anche in questo caso è richiesta una sincronizzazione stringente, ma diversamente dal ToF, è richiesta la sola sincronizzazione tra trasmettitori.

La locazione del target 2D può essere ottenuta facendo stime del punto di intersezione di 2 o più misurazioni TDoA. Vengono formate 2 iperboli, ottenute grazie alla misurazione dei 3 punti fissi  $RN_1, RN_2, RN_3$  per poi ottenere il punto di intersezione P.

I metodi classici di calcolo del TDoA usano tecniche di correlazione, poiché la TDoA può essere stimata a partire dalla cross-correlazione di segnali ricevuti.

Supponendo che il segnale trasmesso sia  $s(t)$  e il segnale ricevuto da un'ancora "i" è  $x_i(t)$ . Si assume che il segnale ricevuto sia corrotto da rumore  $n_i(t)$  e ritardato di un tempo " $d_i$ ", quindi, si avrà che:

$$x_i(t) = s(t - d_i) + n_i(t) \quad (10)$$

Lo stesso ragionamento viene fatto per un secondo segnale  $x_j(t)$  che assume la stessa equazione. La funzione di cross-correlazione tra questi segnali, ad un certo periodo " $T$ " sarà:

$$\hat{R}_{x_i, x_j}(\tau) = \frac{1}{T} \int_0^T x_i(t)x_j(t - \tau)dt \quad (11)$$

Il TDoA stima il valore " $\tau$ " che massimizza la funz di cross-correlazione. Questa operazione richiede che i ricevitori condividano tra loro, precisi riferimenti temporali e segnali di riferimento. Per calcolare il tau vengono utilizzate tecniche di processing nel dominio della frequenza.

### **2.1.7 Return Time of Flight (RToF)**

Misura l'intero viaggio che compie il segnale, cioè il tempo impiegato per arrivare dal trasmettitore al ricevitore ed il tempo di volo dal ricevitore al trasmettitore, quindi viene valutato anche il segnale di risposta. In base a questo "round-trip" del segnale si stima la distanza tra nodo di riferimento e target, similmente al modo di lavorare di un radar.

Il suo funzionamento di base è molto simile al ToF, ma ciò che c'è di diverso è che non è richiesta una sincronizzazione stringente tra trasmettitore e ricevitore. Tuttavia, la stima dell'accuracy di RToF è affetta dagli stessi fattori del ToF ed agiscono 2 volte in ogni misurazione, dato che si deve analizzare il tempo di arrivo al ricevitore e il tempo di ritorno al trasmettitore.

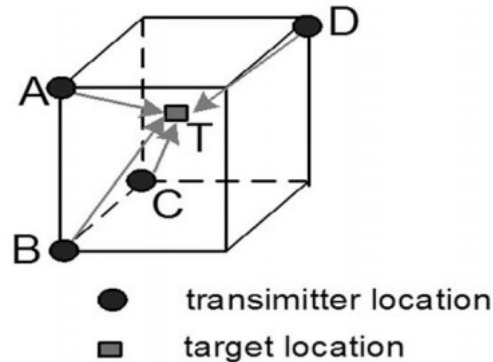
Un altro problema che sorge è il ritardo di risposta da parte del ricevitore.

I sistemi a medio o lungo raggio, il ritardo di risposta del dispositivo può essere trascurato, se confrontato col tempo di trasmissione, ma nelle comunicazioni a corto raggio no. Per questo motivo esistono degli approcci adatti ai sistemi a corto raggio che usano ad esempio, il concetto di riflessione modulata.

### **2.1.8 Phase of Arrival (PoA)**

Approcci di questo tipo utilizzano la fase o la differenza di fase del segnale per la stima della distanza. Per determinare la fase di un segnale si fa l'assunzione che i segnali trasmessi dai nodi di riferimento sono forme sinusoidali pure, avendo la stessa frequenza e un offset di fase pari a 0.

Esistono varie tecniche di localizzazione con PoA, una di queste è di assumere che ci sia un ritardo di transito finito tra ricevitore e trasmettitore che può essere espresso come frazione della lunghezza d'onda del segnale. Il segnale che arriva all'array di antenne in ricezione incide con una differenza di fase alle diverse antenne dell'array, che può essere sfruttata per ottenere la posizione del trasmettitore.



**FIGURA 9: RAPPRESENTAZIONE DI POA**

Per capire meglio, nell'immagine vengono mostrati 4 nodi ancora ricevitori A, B, C, D le cui posizioni formano dei vertici di un cubo. Il ritardo viene espresso come:

$$\varphi_i = (2\pi f D_i)/c \quad (12)$$

Il segnale è:

$$S_i(t) = \sin(2\pi f t + \varphi_i) \quad \text{per } i = A, B, C, D \quad \text{e } 0 < \varphi_i < 2\pi \quad (13)$$

Quando la lunghezza d'onda del segnale trasmesso è maggiore della diagonale del cubo, si può ottenere la stima della distanza:

$$D_i = (c\varphi_i)/(2\pi f) \quad (14)$$

La sola informazione della differenza di fase consente di ottenere la distanza dal target ma non la sua posizione, quindi, si è pensato di integrare questa tecnologia con alcune delle altre descritte in precedenza (RSSI, ToF, TDoA, ...) per migliorare l'accuracy del sistema.

Anche con l'approccio PoA è richiesto LoS tra i dispositivi e questo in molti ambienti non è sempre garantito.



## 2.2 Tecnologie per l'IPS

Rispetto alla localizzazione all'aperto, l'IPS rappresenta una sfida molto più grande, poiché bisogna fronteggiare le situazioni di NLoS, la presenza di persone o oggetti in movimento che possono modificare le condizioni di propagazione del canale, una grande densità di ostacoli che può causare fenomeni di degradazione del segnale come scattering e diffrazione. In molte di queste situazioni solitamente è richiesta un'alta precisione (errore minore di 2 m).

In generale, non esiste una tecnica di indoor positioning migliore delle altre, bisogna guardare che livello delle metriche di valutazione descritte in precedenza bisogna raggiungere per la propria applicazione. Segue un elenco di alcune applicazioni di sistemi basati sull'IPS [11][12].

### 2.2.1 Sistemi di visione

Consistono nel processare e analizzare le immagini catturate da una videocamera al fine di individuare un oggetto o un soggetto all'interno di quell'immagine. Questi sistemi hanno avuto un gran miglioramento con il passare degli anni, grazie all'utilizzo di tecnologie con throughput molto alto e latenza minima. Inoltre, in passato questa tecnologia era considerata costosa da implementare, ma nei giorni nostri esistono soluzioni low-cost, soprattutto pensando di realizzare questo sistema con telecamere di comuni smartphones.

Si possono fare due tipi di distinzione per un sistema di visione:

- **Sistemi a camera fissa:** vengono installate telecamere in posizioni fisse, l'obiettivo di questi sistemi è individuare un target in movimento, confrontando le immagini catturate dalle telecamere. Bisogna capire quali features caratterizzano il target, cercando di individuarlo all'interno dei frames di un video che presentano quelle features. La sua posizione viene

calcolata rispetto alla posizione fissa della telecamera e considerando la distribuzione spaziale di features del target in una certa immagine.

- **Sistemi a camera mobile:** il target mobile viene equipaggiato con una videocamera e viene realizzata la localizzazione scegliendo dei landmark fissi in posizioni e orientazioni note all'interno della stanza. Un altro modo alternativo all'utilizzo di landmark è quello di estrarre features dell'ambiente circostante dalle immagini catturate dalla camera mobile. Nel primo caso, la videocamera rileva due o più landmarks ed individua la sua posizione e orientazione. Nel secondo caso, viene prima fatta un'analisi pre-localizzazione, detta off-line stage, nella quale vengono catturate immagini in specifiche locazioni e da esse vengono estratte le features più rilevanti che vengono salvate in un database. Nell'on-line stage la videocamera ottiene una certa immagine, estrae le sue features e le confronta con gli elementi nel database. In tutti e due i casi l'obiettivo è di individuare la posizione finale della camera mobile.

### 2.2.2 Infrarossi

Un sistema di localizzazione a infrarossi che permette di individuare la posizione di oggetti o persone, ha bisogno di ricevitori e trasmettitori a infrarossi.

Un raggio infrarossi, non può penetrare i muri, quindi per via di questa particolarità, è possibile ottenere un confinamento del segnale dentro una stanza. Inoltre, la tecnologia IR è quasi totalmente immune alle interferenze elettromagnetiche e la potenza di un trasmettitore IR può essere facilmente regolata a seconda del raggio d'azione di preferenza. A fronte di questi vantaggi, bisogna evidenziare che l'errore generato dal multipath, riduce drasticamente l'accuracy di localizzazione, l'hardware di un sistema a infrarossi risulta essere molto costoso ed ha alti costi di manutenzione e per avere buone prestazioni bisogna che tra il trasmettitore e ricevitore ci sia LoS.

### 2.2.3 Visible Light Communication (VLC)

È una tecnologia emergente che fornisce una trasmissione di dati ad alta velocità che usa la luce visibile tra i 400 e i 800 THz, modulata ed emessa da LEDs (Light Emitting Diodes). Si è pensato di realizzare un sistema di localizzazione con VLC, vengono usati sensori di luce che misurano la posizione e la direzione di emettitori LEDs. I LEDs quindi, trasmettono il segnale, che viene catturato dai sensori di luce che fungono da ricevitori. Per effettuare la ricerca della posizione, è stata proposta la tecnica dell'AoA che presenta risultati accurati. Questa applicazione però, ha buone prestazioni se è garantito il LoS tra i LEDs e i sensori ricevitori.

### 2.2.4 Ultrasuoni

Un sistema di localizzazione a ultrasuoni tipico, si basa sulle misurazioni del ToF di segnali a ultrasuoni, cioè con frequenza maggiore di 20 KHz e sui valori della velocità del suono, per calcolare la distanza tra il trasmettitore e il ricevitore. In alcuni scenari è stato dimostrato che un sistema di questo tipo riesce a raggiungere accuratezza al livello del centimetro.

Vengono utilizzate le onde ultrasoniche per misurare la distanza tra una stazione fissa ed un target mobile al fine di localizzarlo all'interno di una zona.

Per implementare questo sistema e calcolare il ToF, c'è bisogno di un gran numero di ricevitori ad ultrasuoni sincronizzati tra loro. Questa sincronizzazione solitamente viene fatta tramite IR o onde radio, poiché le onde radio sono più veloci delle onde ultrasoniche.

Il trasmettitore invia segnali radio e ultrasonici allo stesso momento, il segnale radio raggiunge i ricevitori istantaneamente, garantendo la sincronizzazione. I ricevitori iniziano a misurare il tempo tra il segnale di sincronizzazione e le onde ultrasoniche ricevute, in modo tale da riuscire a calcolare la distanza tra ricevitore e trasmettitore.

Lavorando con gli ultrasuoni e quindi onde di tipo meccanico e non elettromagnetiche, giocano un ruolo importante nella loro propagazione l'umidità e i cambi di temperatura. Per questo conviene integrare anche sensori di temperatura che aiutano a correggere i dati dei segnali ultrasonici.

Alcuni vantaggi di questa tecnologia sono il costo di questi dispositivi e la capacità delle onde di penetrare attraverso numerosi ostacoli. Gli svantaggi riguardano gli effetti di multipath che possono disturbare la misurazione della distanza tra ricevitore e trasmettitore e la complessità di implementazione a larga scala di questo sistema.

Inoltre, alcuni fattori ambientali possono far variare il segnale delle onde ultrasoniche, come la pressione dell'aria, la concentrazione di CO<sub>2</sub> nell'aria e l'inquinamento acustico circostante, ma il problema principale riguarda la temperatura. La temperatura dell'ambiente può influire sulla velocità del suono, per questo molti dei sensori a ultrasuoni prevedono al loro interno un chip che serva a compensare l'errore dato dalla variazione di temperatura, ma rimane comunque il problema della stima della temperatura durante il percorso trasmettitore-ricevitore.

### **2.2.5 Wi-Fi**

Lo standard IEEE 802.11 per le tecnologie WLAN, riguarda il Wi-Fi, che opera nella banda ISM, nasce per poter garantire la connessione a Internet a diversi dispositivi di uso privato, pubblico o commerciale. Tipicamente il Wi-Fi ha un raggio di azione di 100 m, ma per le esigenze del mondo IoT, nasce lo standard IEEE 802.11ah che ha un raggio di copertura di circa 1 km. Il principale vantaggio di questa tecnologia è di essere integrata in ogni tipo di dispositivo, ciò la rende una tecnologia alla portata di tutti, basta pensare che nei paesi più sviluppati quasi in ogni casa c'è un modem/router che garantisce la connessione Internet attraverso il proprio ISP.

Per questo motivo si è pensato di effettuare la localizzazione indoor tramite il Wi-Fi, in molti casi senza dover cambiare l'infrastruttura di rete del locale.

Essendo uno standard nato per garantire connessione di rete e non per la localizzazione, c'è bisogno di rivolgersi ad algoritmi di localizzazione efficaci, per migliorare i risultati. Le tecniche che forniscono un servizio basato sulla localizzazione Wi-Fi sono RSS, CSI, ToF e AoA. Un'altra difficoltà di questi sistemi è far fronte alle interferenze che agiscono sui segnali che portano le informazioni di localizzazione, soprattutto nella banda libera dei 2,4 GHz che risulta essere molto affollata.

Una WLAN può essere sfruttata per individuare la posizione di dispositivi mobili all'interno della sua area di copertura. Sarà presente un access point che invia e riceve segnali RF ai dispositivi della sua rete, essi rispondono a questi segnali e i dati ottenuti dal router o access point vengono utilizzati per stimare la posizione del dispositivo. Dato che la tecnologia Wi-Fi è ormai a disposizione di ogni tipo di azienda e/o casa privata, uno dei principali vantaggi delle tecniche di localizzazione basate sui segnali Wi-Fi è il rapporto costo-efficacia dato dalla possibilità di poter localizzare quasi tutti i dispositivi Wi-Fi all'interno di una rete senza dover installare software aggiuntivo. Inoltre, non è richiesto LoS tra l'access point e il dispositivo da localizzare. Il metodo più noto e più semplice della localizzazione WLAN è quello di sfruttare il dato di RSSI relativo ai dispositivi Wi-Fi.

L'approccio RSS nelle WLAN ha tre modalità base per localizzare un target:

- **Cell of Origin (CoO):** con questo metodo, per effettuare la localizzazione è necessario rendere nota la posizione fissa dell'access point ai dispositivi connessi ad esso. La posizione viene calcolata a seconda della vicinanza del dispositivo all'access point.

- **Metodi basati sulla triangolazione/trilaterazione:** la posizione del target viene calcolata tramite triangolazione o trilaterazione, utilizzando le informazioni di RSSI da almeno 3 ricevitori.
- **Metodi basati sul fingerprinting:** è la soluzione più efficace dei sistemi basati su RSSI per la localizzazione indoor. Questa tecnica consta in 2 fasi, la fase offline e la fase online. Durante la fase offline, vengono collezionati dagli access points i valori di RSS del target, in diverse posizioni, per costruire una mappa del segnale dell'ambiente specifico. Nella fase online, viene stimata la posizione fisica del target, confrontando l'RSS misurato con i valori di RSS memorizzati.

L'accuracy della tecnologia Wi-Fi per la localizzazione è molto bassa in genere, ma se viene integrata con altre tecnologie che correggono i valori di RSSI o aggiungono informazioni per un calcolo più preciso, l'accuracy può arrivare fino a 3-5 m.

Uno dei problemi più noti di questa applicazione è il consumo di energia, poiché i dispositivi mobili che vengono localizzati consumano molta potenza per inviare e ricevere segnali Wi-Fi.

### 2.2.6 RFID

Questo sistema è molto simile al concetto dei codici a barre, nei quali grazie a un lettore ottico si scansiona l'area in cui è presente il codice a barre e vengono decodificate le sue informazioni.

RFID nasce negli anni '70, può essere meglio definita come un sistema di identificazione di prossimità e di transazione di dati.

Uno dei primi papers pioniere dell'RFID, fu scritto da Harry Stockman, "Communication by Means of Reflected Power", nel 1948, che discuteva dei radar e delle ricerche della tecnologia radio di quei tempi. Altre tecnologie si avvicinavano a quello che si può definire ora un sistema RFID, come ad esempio

il sistema di transponder a lungo raggio di IFF (Identification Friend or Foe) per identificare gli aerei. La ricerca in quest'ambito continua fino agli anni '60, nei quali vari ricercatori e inventori sviluppano i primi prototipi. Alcuni di essi sono stati commercializzati, come "Sensormatic" ed usavano tags di 1 bit di memoria, servivano per verificare la presenza o l'assenza di oggetti in una certa area, furono molto utilizzati nei magazzini o nei negozi come dispositivi antifurto di vestiti od oggetti di valore.

Il primo grande sviluppo della tecnologia RFID si ebbe dagli anni '70, iniziato da grandi aziende di apparati elettronici e vengono esplorati altre nuove applicazioni, come il tag di animali. Dagli anni '80 inizia la distribuzione commerciale di dispositivi RFID anche in paesi dell'Europa. Dal 1990 in poi viene utilizzato in molti ambiti lavorativi, uno dei più importati è nelle autostrade, con il Telepass. Dopo l'Europa questa tecnologia viene condivisa anche con gli altri paesi del mondo.

I tag, grazie alla continua ricerca nella microelettronica, diventano di dimensioni sempre più ridotte, per adattarsi anche ad altre applicazioni.

Un sistema RFID è comprensivo dei seguenti componenti:

- Un tag RFID;
- Un reader RFID che dispone di antenna o un sistema formato da antenna RFID e reader RFID separati;
- Un sistema host o una connessione al sistema di rete aziendale.

**Tag:** i tag si distinguono in 2 categorie, quelli attivi e quelli passivi. I tag attivi sono a tutti gli effetti dei transponder, hanno bisogno di una batteria per ricevere e trasmettere il segnale. Tipicamente sono dispositivi che implementano opzioni di lettura e scrittura.

L'altra tipologia di tag sono quelli passivi, essi non hanno bisogno di batterie perché sono alimentati dalle onde a radio frequenza trasmesse dai lettori o antenne RFID e per induzione, trasmettono a loro volta un segnale di risposta. Il loro costo

è molto minore rispetto i tag attivi, a discapito della capacità di memoria che risulta inferiore, del range di trasmissione e della potenza maggiore impiegata dal reader, ma hanno tutti i vantaggi che apporta il fatto di non essere alimentati da una batteria (ovvero durata di vita media più lunga, nessun consumo di potenza e il non dover sostituire la batteria periodicamente). Sono di dimensioni minori e possono avere una memoria di sola lettura.

Esistono anche dei tipi di tag detti “semi-passivi” che hanno una batteria che alimenta il circuito del chip ma per comunicare si comportano esattamente come dei tag passivi, quindi, sfruttano le onde trasmesse da un reader.

I tag possono essere di varie forme, dimensioni e tipologie, variano da un minimo di 0.4 mm x 0.4 mm (di spessore trascurabile) a un massimo di 120 x 100 x 50 mm e a seconda dell’ambiente di utilizzo sono stati realizzati tipi di tag appositi, come ad esempio tag per materiali metallici, tag resistenti a temperature estreme e tag resistenti ad umidità.

La memoria dei tag può essere:

- **ROM:** di sola lettura;
- **RAM:** volatile, di lettura/scrittura;
- **WORM:** di scrittura singola ma lettura multipla.

La memoria ROM è usata per memorizzare dati di sicurezza, un identificatore univoco e istruzioni al sistema operativo, la RAM è usata per memorizzare durante le interrogazioni del transponder e per la risposta.

**Range di frequenze:** le bande di frequenza tipiche dei segnali RFID sono mostrate in tabella, con il relativo range di lettura (per tag passivi):



**TABELLA 4: FREQUENZE OPERATIVE RFID**

Frequency Range	Frequencies	Passive Read Distance
Low Frequency (LF)	120-140 KHz	10-20 cm
High Frequency (HF)	13.56 MHz	10-20 cm
Ultra-High Frequency (UHF)	868-928 MHz	3 meters
Microwave	2.45 & 5.8 GHz	3 meters
Ultra-Wide Band (UWB)	3.1-10.6 GHz	10 meters

Le frequenze occupate dai dispositivi RFID sono diverse a seconda del paese, ad esempio in Europa sono classificati come UHF i segnali con frequenze di 868-870 MHz, mentre in USA e Canada quelli con frequenze 902-928 MHz.

- **Low frequency (LF):** i tag LF sono tipicamente passivi ed hanno un cortissimo range trasmissivo. Possono essere utilizzati in ambienti ostili, possono operare in prossimità di metallo e liquidi. Il loro svantaggio è di avere una bit rate di lettura inferiore rispetto tag che operano a frequenze più alte ed il loro costo è maggiore. Scenari applicativi: tracciabilità di animali con tag sottocutanei, sistemi di controllo degli accessi;
- **High Frequency (HF):** specificata nello standard ISO 18000-3. I tag hanno una rate trasmissiva maggiore dei tag LF, ma non interagiscono al meglio con metalli o liquidi. La frequenza HF si trova in una parte dello spettro radio fortemente regolata, quindi, la banda occupabile risulta essere molto stretta, questo può essere un problema per dispositivi elettronici (come gli apparecchi medici) che lavorano a frequenze vicine a quella dei 13,56 MHz. Spesso questi tag sono contenuti in carte plastificate. Applicazioni: lettura carte di credito contact-less, ID badges, tracciamento di libri in biblioteca;
- **Ultra-High Frequency (UHF):** I tag RFID UHF sono comunemente utilizzati per il tracciamento e applicazioni che riguardano le linee produttive. Il loro range di comunicazione è moderatamente lungo e sono più economici rispetto i tag LF e HF. Lo svantaggio maggiore di questi tags è di soffrire di interferenze con liquidi e metalli. Per questo, sono stati realizzati dei tag

speciali UHF, schermati da materiali, che riescono a resistere alle distorsioni del segnale indotte da metalli. Applicazioni: logistica ed inventario, manutenzione di impianti, tracciabilità alimentare;

- **Microwave:** anche dette Super-High Frequencies (SHF), la tecnologia Microwave RFID ha trovato piede recentemente ed è in rapido sviluppo. I tag sono principalmente semi-passivi o attivi, hanno rate di lettura molto alti e in alcune applicazioni, anche i range di lettura sono elevati. Ci sono diversi svantaggi nel loro utilizzo, come il fatto di essere molto costosi rispetto i tag UHF, ma il problema principale è di operare nella banda dei sistemi Wi-Fi 802.11b/g che possono generare interferenze, così come lo standard wireless ZigBee 802.15;
- **Ultra-Wideband:** la tecnologia UWB è stata introdotta recentemente in ambito di RFID. La particolarità di questi tag è di trasmettere un segnale a bassa potenza ma a una banda di frequenza molto estesa. I vantaggi sono di avere un range di lettura in LoS che in alcuni casi arriva fino a 200 m e i tag UWB sono compatibili con metalli e liquidi. Se un segnale a una certa frequenza è molto debole, esso non interferisce con questi tag RFID a UWB. Uno svantaggio è che le implementazioni di questa tecnologia sono possibili solo con tag attivi o semi-passivi ed essi hanno un consumo di potenza non trascurabile. Applicazioni: asset tracking in ambito ospedaliero.

**Casi d'uso di RFID:** ci sono 4 categorie in cui si possono classificare gli utilizzi di dispositivi RFID:

- **EAS (Electronic Article Surveillance):** per rivelare la presenza o l'assenza di un oggetto, tipicamente sono sistemi a 1 bit. Tipicamente sono utilizzati nei negozi come antitaccheggio;

- **Portable data capture:** nei casi in cui i dati che l'oggetto memorizza tratta, sono molto vari, ad esempio dati di sensing come temperatura, movimento, umidità. quindi, queste informazioni vengono memorizzate all'interno di un dispositivo portatile, che possono essere richiesti in un secondo momento;
- **Networked systems:** sono caratterizzati da lettori in posizione fissa ed utilizzati per tracciare i movimenti di oggetti taggati che generalmente vengono connessi direttamente alla rete aziendale;
- **Positioning systems:** per fornire una localizzazione automatica di oggetti di vario genere.

**Funzionalità di RFID:** una delle principali è l'identificazione, un lettore invia richieste di lettura nella sua area di copertura e i tag che le ricevono rispondono non solo con il loro identificativo ma anche con altri dati che essi memorizzano. Ci sono in totale 5 classi di funzionalità dei tag RFID:

**TABELLA 5: CLASSI DI RFID**

Class	Name	Memory	Power Source	Features
A	EAS	None	Passive	Article Surveillance
B	Read-only EPC	Read-Only	Passive	Identification Only
C	EPC	Read/Write	Passive	Data Logging
D	Sensor Tags	Read/Write	Semi-Passive	Environmental Sensors
E	Motes	Read/Write	Active	Ad Hoc Networking

Descrizione delle classi:

- A. I tag Electronic Article Surveillance (EAS), sono i primi tag della storia, infatti, sono in commercio da più di 40 anni. Essi non contengono un identificatore univoco, annunciano semplicemente la loro presenza a un reader;
- B. I tag di questa classe contengono anche un'informazione per identificarsi, che può essere un product code o un'ID univoco che viene impresso nella

memoria in fase di produzione. Possono essere anche di tipo semi-passivo o attivo, ma il loro prezzo e dimensioni saranno maggiori.

- C. I tag Electronic Product Code (EPC) offrono operazioni di WORM o memoria riscrivibile. Hanno comunque un'ID impresso in memoria al momento della loro realizzazione fisica, ma questo ID può essere settato anche da un utente finale e può essere cambiato varie volte. Più costosi delle categorie A e B;
- D. Essi contengono dei sensori ambientali nel chip e possono memorizzare dati senza l'aiuto di un reader. Possono essere utilizzati per formare una rete di sensori.
- E. I tags di questa classe sono detti anche "smart dust" motes, possono essere in grado di iniziare comunicazioni con altri tag motes e possono formare reti ad hoc, per questo sono tag attivi. La loro struttura elettronica e il funzionamento sono molto più complessi rispetto altri tag EPC.

**Svantaggi della tecnologia RFID:** un problema che non risolve questa tecnologia è sicuramente la sicurezza informatica [36]. Nello specifico possono verificarsi rischi di sicurezza, in quanto utenti malevoli potrebbero causare danni o blocchi a un sistema RFID per trarne un vantaggio e rischi di privacy che avvengono quando i dati da salvare nella memoria dei tag sono informazioni personali (come dati anagrafici o dati di pagamento).

Dei tipici attacchi ai sistemi RFID possono essere classificati come segue:

- **Tag isolation:** è l'attacco più semplice e comune, consiste nel bloccare le comunicazioni tra il tag e il reader;
- **Tag cloning:** l'identificatore univoco contenuto nei tag RFID viene copiato e inserito in un altro tag;

- **Denial of Service:** al reader vengono trasmessi flussi di informazioni che possono mandare il sistema in out of service, non essendo in grado di leggere le informazioni dei tag leciti;
- **Command injection:** comandi trasmessi in remoto a un reader, da un utente non autorizzato;
- **Signal replaying:** consiste nel registrare segnali RFID in un certo tempo per poi utilizzarli in futuro;
- **Man-in-the-Middle:** un dispositivo attivo si interpone tra la comunicazione di tag e lettore, catturando i dati mantenendo la sua presenza nascosta;
- **Malware injection:** viene inserito in un tag un codice malevolo in grado di essere trasmesso ad altri tag;
- **Accesso non autorizzato a dati personali;**
- **Tracking della persona:** le informazioni personali contenute in tag RFID potrebbero essere usate da alcuni attaccanti per ricostruire le abitudini di una certa persona.

**Localizzazione con RFID:** in un sistema RFID, si utilizzano dei tag attivi o passivi e uno o più RFID readers, equipaggiati con una o più antenne RFID. Tipicamente, il reader comunica con i tags attraverso le antenne, che trasmettono e ricevono il segnale RFID, poi i dati vengono trasmessi dal reader ad un sistema di processing, ad esempio ad un computer.

Un tag contiene tipicamente, come informazione principale, il suo numero identificativo, ma può contenere anche informazioni sulla sua posizione. La localizzazione RFID si può distinguere in due modi: localizzazione del reader o localizzazione del tag.

Nella localizzazione del reader le prestazioni dipendono fortemente dalla densità dei tags e dal massimo range di lettura. Avendo quindi, dei tag in posizioni fisse, un reader all'interno di un locale può essere identificato leggendo il tag più vicino e ottenendo l'informazione sulla sua posizione. Lo svantaggio di questo metodo è

l'utilizzo di un gran numero di tags che hanno bisogno di preregistrare nella loro memoria l'informazione sulla propria posizione.

Nella seconda metodologia, vengono utilizzate tecniche di multi-laterazione basate sull'RSSI, così facendo si ottiene una localizzazione non precisa. Contrariamente al primo metodo, c'è bisogno di almeno 3 RFID readers messi in posizioni note, quindi i costi incrementano di molto.

### **2.2.7 Bluetooth (IEEE 802.15.1)**

È uno standard per le Wireless Personal Area Networks (WPANs) ed opera nella banda ISM dei 2,4 GHz, il range tipico di è di 10-15 m è una tecnologia facilmente integrabile all'interno di diversi dispositivi, inserendo un chip nella sua scheda. Il Bluetooth è una tecnologia low-cost, a basso consumo energetico ed ha un buon rapporto costo-efficienza per quanto riguarda sistemi di localizzazione indoor. I tags Bluetooth sono transceiver di piccole dimensioni, ognuno di essi ha un ID unico e tipicamente la batteria ha un periodo di vita di alcuni mesi o anche di anni, dipende dal tipo di utilizzo e dalla rate del segnale.

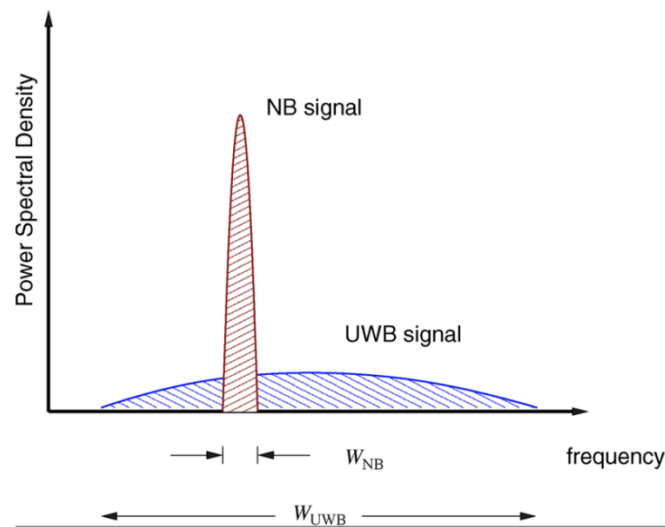
Uno degli inconvenienti è la latenza dei segnali Bluetooth, tipicamente 20 s, che per applicazioni real-time è impraticabile. Un altro svantaggio è l'accuracy di localizzazione non troppo precisa (2-3 m) che offre un sistema basato su Bluetooth, inoltre se lo scenario indoor risulta complesso (per la presenza di materiali metallici o ostacoli grandi) ed è dinamico, l'accuracy decresce ancora di più.

### **2.2.8 Ultra-Wide Band (UWB, IEEE 802.15.4a)**

La tecnologia radio UWB venne implementata intorno al 1960 ed utilizzata per i radar e per scopi militari [20] [21]. Per capire come è fatto un segnale UWB, è necessario di citare la banda frazionaria " $B_f$ ", definita come:

$$B_f = 2 \frac{f_H - f_L}{f_H + f_L} \quad (15)$$

Dove “ $f_H$ ” e “ $f_L$ ” rappresentano la larghezza di banda maggiore e minore a misurate a -3 dB, rispettivamente. Un segnale è UWB se la sua banda frazionaria è maggiore di 25%.



**FIGURA 10: DIFFERENZE TRA SEGNALE NB E UWB**

Dal 1990 questa tecnologia diventò importante in applicazioni commerciali come, per i suoi vantaggi, come:

- **Trasmissione ad elevata data rate:** poiché, seguendo la formula di Shannon per la capacità del canale, l’uso di una banda molto estesa garantisce una capacità del canale elevata;
- **Robustezza agli effetti di fading:** i sistemi UWB sono resistenti agli effetti del fading multipath e capaci di risolvere le componenti del multipath, anche in ambienti dove il fenomeno del multipath è molto forte;
- **Sicurezza:** dato che i segnali UWB operano al di sotto del livello del rumore, da parte di un eavesdropper è difficile captare il segnale;
- **Alta precisione nel ranging:** i sistemi UWB hanno una buona risoluzione temporale, ciò consente di ottenere misurazioni della distanza molto

precise, utile per applicazioni di localizzazione e tracking (al livello del centimetro);

- **Capacità di oltrepassare gli ostacoli:** UWB è in grado di operare in condizioni di LoS e di NLoS, specialmente i muri di cemento, ma non nel caso di materiali metallici e liquidi;
- **Bassa densità spettrale:** dato che hanno una potenza molto bassa, essi possono coesistere con altre tecnologie che lavorano alle stesse frequenze, come il WiFi, GPS, UMTS/LTE;
- **Tecnologia a basso consumo:** Il duty cycle è molto basso, ciò si traduce in un ridotto consumo di energia, in più le potenze in gioco con UWB sono molto basse.

Il segnale UWB può essere bloccato da grandi oggetti metallici. La Federal Communications Commission (FCC) degli USA, ha istituito delle bande UWB non licenziate, nel range di frequenze 3.1 GHz -10.6 GHz.

Dal 2002 l'FCC approva l'UWB per uso commerciale, il suo utilizzo diventa più pratico ed economico con lo sviluppo di chipset digitali ad alta velocità.

Alcune caratteristiche di UWB sono un'alta data rate, maggiore di 100 Mbps, un range del segnale molto piccolo circa 10 metri. Alternativamente un'altra modalità di UWB è di fornire una data-rate molto bassa, minore di 1 Mbps, ad un range molto maggiore aumentando lo spreading factor.

Alcune applicazioni dell'UWB riguardano la penetrazione del suolo con radar, through-wall imaging, sorveglianza, radar veicolari, comunicazioni ultraveloci ed applicazioni indoor a corto range.

È una tecnologia che viene applicata spesso nell'ambito IoT, come il tracking, localizzazione ad alta precisione.



Lo spettro di frequenze di UWB si sovrappone ad altri servizi operanti le stesse frequenze, però dato che l'emissione di potenza del UWB è molto inferiore rispetto al rumore di fondo, UWB non interferisce con questi servizi.

Per via della trasmissione a bassa potenza, la distanza trasmissiva del segnale UWB è limitata a pochi metri. La densità spettrale massima dettata dall'FCC è di -41.25 dBm/MHz.

Un impulso UWB occupa lo spettro di frequenze per pochi nanosecondi, quindi, l'energia del segnale viene distribuita su uno spettro molto grande, consentendo la generazione di un segnale a bassa potenza. Il ricevitore e il trasmettitore devono essere sincronizzati con una differenza dell'ordine del picosecondo.

In UWB lo spettro del segnale trasmesso e ricevuto dipende dalla larghezza e la forma dell'impulso generato, la cui forma è stata progettata per diffondere l'energia dell'impulso su frequenze tali che minimizzano la densità spettrale di potenza e l'interferenza con altri segnali. Inoltre, la forma dell'impulso è selezionata in modo da evitare la componente DC, al fine di ottenere l'efficienza di radiazione d'antenna. Alcune forme di impulso utilizzate in UWB sono: Gaussian Monopulse, Gaussian second derivative, RZ Manchester.

In termini numerici gli impulsi trasmessi hanno durata temporale  $< 1$  ns con e con banda  $> 500$  MHz, con range di frequenze da 3.1 a 10.6 GHz. È una tecnologia che si appresta ad essere utilizzata per l'indoor localization, essendo immune alle interferenze causate da altri segnali, dovuto dal fatto di avere un tipo di segnale e uno spettro molto differenti da quelli comunemente usati per gli altri segnali trasmessi da altre tecnologie RF.

Altro vantaggio di un segnale UWB (soprattutto alle frequenze più basse) è di riuscire a penetrare molti materiali, specialmente i muri di cemento. È importante sapere che la particolare forma di un segnale UWB fa sì che gli effetti di multipath siano molto ridotti, poiché è semplice individuare il cammino principale di un segnale, quindi, si può avere una buona stima del ToF e in alcune circostanze UWB raggiunge livelli di precisione di localizzazione di 10 cm.

### 2.2.9 ZigBee

È uno standard implementato seguendo lo standard IEEE 802.15.4, che riguarda i livelli fisico e MAC per le PAN che siano low cost, a bassa data-rate e energy-save. In ZigBee il livello network è responsabile del routing multi-hop e il livello applicazione è responsabile della comunicazione distribuita e lo sviluppo di applicazioni.

ZigBee è molto utile per effettuare la localizzazione in una rete wireless di sensori, ma al contrario del Wi-Fi o del Bluetooth nella maggior parte dei dispositivi non è presente un chip che implementa questa tecnologia.

questa tecnologia si basa sul realizzare una rete di dispositivi ZigBee, vengono posizionati diversi nodi sensori detti “reference”, in posizioni note ed è presente un nodo target, detto “sink node” la cui posizione è ignota. I nodi di riferimento comunicano tra loro e si scambiano informazioni sulla forza del segnale radio ricevuto, che poi verranno utilizzate per il calcolo della posizione del sink. Esistono, inoltre, diversi algoritmi di localizzazione di ZigBee, che hanno performances diverse anche a seconda del tipo di luogo che si intende analizzare.

### 2.3 Metriche di valutazione per un sistema IPS

**Disponibilità:** si intende che una certa tecnologia è disponibile nel dispositivo venduto all’utente finale e non richiede hardware proprietario all’utente finale. Questo è molto importante per l’adozione a larga scala di una tecnologia IoT. È importante riuscire ad implementare un sistema di localizzazione che può comunicare senza problemi con dispositivi largamente utilizzati, come gli smartphones. Un esempio di tecnologia largamente utilizzata è il Wi-Fi, che è disponibile in quasi tutti gli smartphones.

**Costo:** l’obiettivo è di minimizzare il costo di un sistema di localizzazione. Un sistema ideale non deve prevedere nessun costo di infrastruttura addizionale e non

dovrebbe richiedere l'utilizzo di dispositivi di una fascia di prezzo alta, se essi in pratica non vengono largamente sfruttati. Un sistema che ha nodi di rete proprietari potrebbe migliorare l'accuratezza di localizzazione, ma incrementerebbe di molto i costi, rispetto le soluzioni che si trovano in commercio. Soprattutto per realizzare un sistema di localizzazione a larga scala, bisogna sicuramente dare molta importanza all'analisi dei costi.

**Consumo energetico:** è uno dei paradigmi principali del mondo IoT, si punta a realizzare un'applicazione che consente di funzionare bene senza generare un consumo elevato di energia, quindi, i dispositivi scelti dovranno consumare una potenza minima, per garantire una lunga durata di vita della batteria. Se si pensa a una rete di sensori con centinaia di nodi, è impossibile pensare di cambiare la batteria di ogni nodo ogni mese o anche meno, l'ideale sarebbe se le batterie abbiano una vita superiore a un anno.

Per ciò che riguarda il servizio di localizzazione, i nodi che forniscono le informazioni sulla posizione di altri nodi target devono avere un consumo di potenza molto limitato, al contrario, sarà previsto un nodo aggregatore o anche un gateway che raggruppa le informazioni ottenute e svolge i calcoli, esso deve avere accesso alla rete elettrica, in modo diretto o indiretto, poiché consumerà molta più energia rispetto i nodi sensore.

È importante per un sistema di localizzazione trovare un trade off tra il consumo energetico e la latenza, alcuni fattori che possono influire sono:

- **Periodicità:** è l'intervallo di tempo con il quale un nodo trasmette (es. la periodicità è 0,5 secondi, quindi un nodo trasmette dati ogni 0,5 secondi). Questo parametro influisce molto sul consumo di energia, più alta è la periodicità con la quale si trasmettono i dati e minore è il consumo.
- **Potenza trasmissiva:** è la potenza con la quale vengono trasmessi i segnali di un nodo, maggiore è il suo valore, maggiore sarà il consumo energetico, ma sarà maggiore anche il range del segnale (però una potenza troppo

elevata è sconveniente, poiché un segnale trasmesso da un nodo potrebbe interferire con quelli trasmessi dagli altri nodi). In un sistema MBL questo non è un problema, in quanto i nodi ancora o di riferimento avranno accesso alla rete elettrica, cosa non vera in uno scenario IoT dove i dispositivi sono tipicamente alimentati da una batteria, quindi, l'obiettivo è di fornire un servizio di localizzazione efficiente ma con basso consumo di energia.

- **Complessità computazionale:** i nodi sensore devono svolgere funzioni elementari, non devono svolgere calcoli complessi, perché far svolgere pesanti algoritmi ad un nodo aumenterà il suo consumo di energia. Conviene far svolgere le funzioni più difficile a un dispositivo terminale che aggrega i dati ricevuti dai nodi.

**Range:** è il raggio di copertura di un certo dispositivo wireless. Per fornire un buon servizio di localizzazione, si deve studiare l'area da coprire, capire quale è il range trasmissivo nominale dei nodi e valutare il numero di nodi ancora da installare per avere una copertura ideale.

È essenziale considerare che le performances del sistema diminuiscono se la distanza tra i ricevitori e i trasmettitori aumenta.

**Accuratezza di localizzazione o tracking:** è la precisione con la quale si ottengono i dati sulla posizione stimata di un device target. Come descritto in precedenza, lo studio di propagazione dell'onda elettromagnetica all'interno di locali ha diversi fattori da considerare, che possono degradare il segnale. È quindi importante per un sistema di localizzazione limitare l'impatto degli effetti di multipath e le interferenze provenienti da altri sistemi, per avere una stima della posizione molto accurata.

**Latenza o Ritardo:** se si vuole realizzare un'applicazione real-time, questo requisito diventa uno dei più importanti e delicati. La latenza indica il tempo

impiegato da un nodo per compiere operazioni sui segnali ricevuti. Un servizio di localizzazione real-time ideale dovrebbe identificare un nodo target con un numero minimo di segnali trasmessi dai nodi di riferimento e far svolgere operazioni complesse ai nodi in pochi millisecondi. Questa richiesta nella maggior parte delle applicazioni non è possibile, considerando anche che il sistema deve adattarsi bene anche a larga scala. Perciò c'è molta ricerca in ambito signal processing, per algoritmi che sono molto veloci (ordine del millisecondo) ed energy saving.

**Scalabilità:** un sistema di localizzazione, per essere scalabile, deve mantenere le sue prestazioni pressoché invariate se lo si utilizza per individuare la posizione di un gran numero di dispositivi. La scalabilità è un problema maggiore da affrontare per i sistemi MBL, rispetto i DBL, poiché in questi ultimi la posizione viene calcolata dal dispositivo target stesso, che non è influenzato dalla numerosità di altri dispositivi target. L'obiettivo sarebbe di riuscire a localizzare tutti i nodi target con un livello di precisione simile, allo stesso tempo.

## 2.4 Sfide per un sistema di localizzazione

**Effetti di multipath e rumore:** il multipath nasce proprio dalla natura dei segnali, che possono essere riflessi o rifratti incidendo su superfici di ogni tipo. È un tipo di effetto che fa degradare le prestazioni dei sistemi di localizzazione e tracking, basati su RSSI, ToF, TDoA, AoA. Quando capitano situazioni in cui l'effetto di multipath è non trascurabile, il ricevitore catturerà, oltre il segnale vero e proprio, tante sue repliche che saranno attenuate e ritardate nel tempo. Il più delle volte non si riesce a distinguere quale di questi segnali giunti al ricevitore sia quello del primo percorso. È quindi necessario ottenere un segnale LoS per avere una buona stima della posizione.

Si possono comunque applicare algoritmi per lo più complessi, che identificano il segnale LoS ed eliminano o minimizzano le componenti del multipath.

**Effetti del canale radio:** i servizi di IPS sono fortemente dipendenti dalle caratteristiche dell'ambiente indoor. Le performances del sistema variano se ci sono cambiamenti delle dinamiche dell'ambiente, ad esempio se in alcuni giorni c'è alta densità di persone oppure se vengono cambiate le disposizioni di mobili o di oggetti di grandi dimensioni.

Quando si installa un sistema di localizzazione bisogna tener conto anche di queste problematiche, perché può mostrare prestazioni molto diverse anche in ambienti simili.

Nella maggior parte di questi sistemi, si richiede che ci sia almeno un percorso LoS tra un target e i nodi di riferimento, ma può capitare che per la presenza di ostacoli questa condizione non venga più garantita, quindi, le prestazioni crollano. In uno scenario industriale, diventa difficile capire dove fissare i nodi di riferimento, per la presenza di grandi oggetti metallici che riflettono il segnale e la grande dinamicità dell'ambiente, si pensi solo al movimento delle macchine lungo la linea produttiva e ai carrelli che circolano da una zona all'altra.

### 3 Bluetooth Low Energy

Garantisce comunque l'interoperabilità con la vecchia versione del Bluetooth, il Bluetooth Classic [16][17][18][19].

Rispetto l'architettura del Bluetooth Classic, quella del BLE ha mantenuto molte caratteristiche, in modo da poter garantire nei dispositivi il dual mode (si chiamano dispositivi Smart Ready). Tuttavia, alcune differenze con il precedente stack ci sono, in figura sono mostrate le diversità tra i 3 principali stack sui quali si basa il funzionamento del chip Bluetooth dei dispositivi:

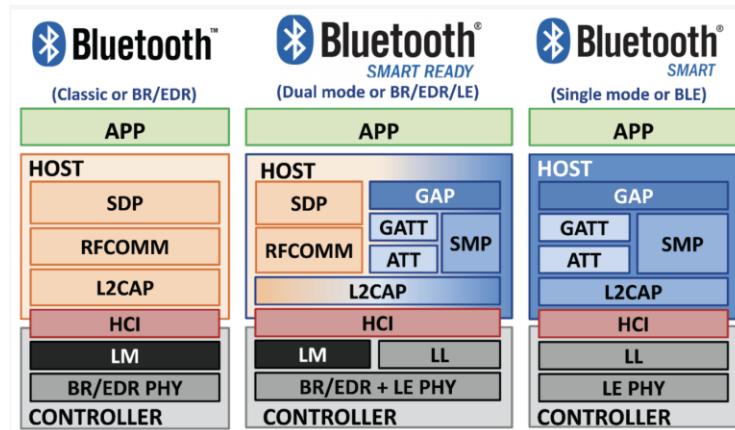


FIGURA 11: MODALITÀ DEL BLUETOOTH

Nasce con la versione 4.0, leggere modifiche vengono fatte nella versione 4.1 e 4.2. la versione 5.0 apporta grandi migliorie, come l'incremento della data rate, la versione 5.1 introduce tecniche di direction finding.

Nato per garantire un consumo minimo di energia, con il nascere dell'importanza del mondo IoT.

Migliorie della versione 5.0:

- Raddoppio della data rate, fino a 2 Mb/s, grazie ad una nuova modulazione;
- Range aumentato di 4 volte (LE long range);
- Aumento di 8 volte della capacità di broadcast, grazie all'estensione delle procedure di advertising (LE advertising extension);
- Una potenza di trasmissione maggiore (fino a +20 dBm);
- Abilitazione della funzione di direction finding attraverso le tecniche di AoA e AoD.

In BLE sono disponibili 3 tipi di comunicazione:

- Modalità di sola trasmissione di informazioni in broadcast;
- Modalità di sola ricezione di dati;
- Modalità mista, di trasmissione e ricezione.

La comunicazione in BLE avviene attraverso segnali di advertising, trasmessi su canali dedicati, lo scambio di dati è diretto. Ci saranno dispositivi che trasmettono

su questi canali ed altri dispositivi che sono in fase di scanning, quindi di ascolto di pacchetti su quei canali.

I dispositivi più caratterizzanti della tecnologia BLE si chiamano Beacons, che hanno la funzione principale di trasmettere segnale e sono incentrati sull'energy-saving, quindi, negli intervalli di tempo nei quali non devono trasmettere, entrano in modalità stand-by.

Nella versione 5 i canali dati sono utilizzati come canali ausiliari. In modalità advertising non viene avviata una connessione, ma i dati vengono trasmessi sfruttando i canali dati e prendono nome di pacchetti ausiliari (AUX). Questo processo si chiama offloading ed è utile per ridurre il traffico di pacchetti nei 3 canali di advertising.

Un altro modo di far comunicare tra loro due dispositivi è creare una connessione tra loro, ciò avviene come nel Bluetooth Classic, attraverso le Piconet.

nella versione 5 sono state introdotte novità per il livello fisico, vengono presentati 3 tipi di livello fisico, i quali hanno diversi tipi di modulazione, codifica e data rates.

PHY	Blue-tooth LE	Modulation scheme (GFSK) gross data rate	Coding		Net data rate	Direction Finding via CTE
			Access header	Payload		
LE 1M	Mandatory	Nominal Frequency Deviation 250 kHz 1 Msymbols/s	Uncoded		1 Mbit/s	yes
LE 2M	Optional	Nominal Frequency Deviation 500 kHz 2 Msymbols/s	Uncoded		2 Mbit/s	yes
LE coded	Optional	Nominal Frequency Deviation 250 kHz 1 Msymbols/s	S = 8	S = 2 S = 8	500 kbit/s 125 kbit/s	no

**FIGURA 12: TIPI DI PACCHETTO NEL BLUETOOTH 5.0**

$S=n$  significa “ $n$ ” simboli per bit, LE 1M è un livello fisico obbligatorio ed è compatibile anche con la versione 4.0, inoltre con LE 1M e LE 2M è possibile utilizzare tecniche di direction finding.

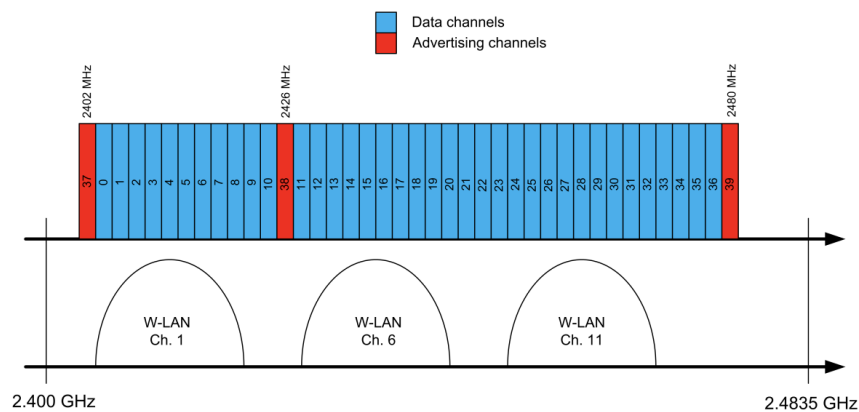


Essendo i livelli fisici di tipo LE 1M e LE 2M non codificati, ogni bit trasmesso equivale a un simbolo, invece, con LE coded si usa uno schema di 2 simboli per bit (per la rate a 500 kbps) oppure di 8 simboli per bit (per la rate 125 kbps), ciò significa un vantaggio per la robustezza delle trasmissioni, ma una rate trasmissiva minore.

### 3.1 Controller

#### 3.1.1 Physical Layer

Il livello fisico descrive il modo in cui vengono trasmessi i dati nella banda dei 2,4 GHz (precisamente da 2,402 GHz a 2,480 GHz con spaziatura tra canali di 2 MHz), divisa in 40 canali di cui il 37 (2402 MHz), 38 (2426 MHz) e 39 (2480 MHz) sono dedicati alla trasmissione di pacchetti di advertising e gli altri per il trasferimento dei dati. I tipi di modulazione sono l'AFH e la GFSK (Gaussian Frequency-Shift Keying). Sono stati scelti proprio quei canali poiché subiscono minor interferenza dallo spettro del Wi-Fi.



**FIGURA 13: SPETTRO DI FREQUENZE DEL BLE E DEL WIFI**

**Modulazione:** in BLE si utilizza un solo tipo di modulazione, la GFSK, la stessa utilizzata in Bluetooth Classic, con deviazione di frequenza di 250 kHz, che

garantisce una rate di trasferimento di 1 Mbps (con LE 1M e livello fisico codificato).

Nella versione 5 in LE 2M, la deviazione di frequenza nominale della GFSK è di 500 kHz, che fa risultare una rate di 2 Mbps. Viene utilizzato un filtro gaussiano con BT (bandwidth time product) pari a 0,5 e indice di modulazione compreso tra 0,45 e 0,55.

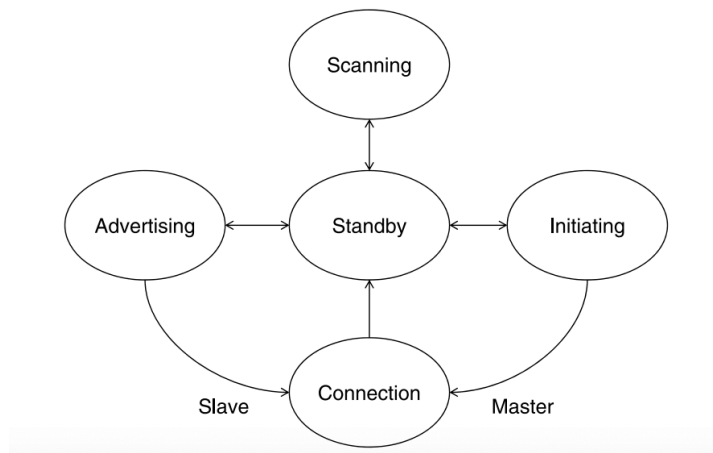
### 3.1.2 Link Layer (LL)

Si interfaccia direttamente con il livello fisico, è composto da una combinazione di parti hardware e parti software. Il LL definisce il tipo di comunicazioni che possono avvenire tra dispositivi BLE, attraverso la gestione dello stato dei collegamenti che avvengono nel canale radio. In questo layer vengono definiti i ruoli che può assumere un dispositivo BLE: scanner, advertiser, master e slave.

Il ruolo di un dispositivo è relativo al tipo di stato in cui si trova, inoltre, bisogna distinguere quali tipi di comunicazioni avvengono in BLE:

- **Connection-less:** significa che i dispositivi BLE si scambieranno dati senza iniziare una procedura di connessione tra loro (come con il protocollo di trasporto UDP). In questo caso un device assume il ruolo di advertiser, trasmette segnale e uno scanner che è in ascolto di pacchetti BLE.
- **Connection-oriented:** i dispositivi BLE effettuano una comunicazione creando una connessione (come con il protocollo di rete TCP), quindi, si scambieranno dei pacchetti di sincronizzazione e una volta iniziata la connessione, potranno scambiarsi i dati.

Il LL del BLE è caratterizzato da 5 stati:

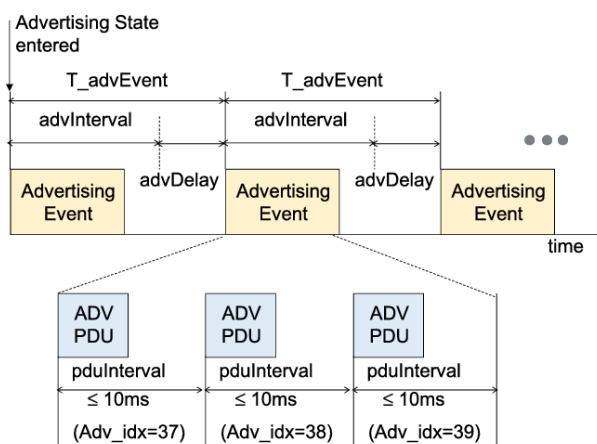


**FIGURA 14: STATI DEL LINK LAYER**

**Advertising:** la funzione principale di questo stato è di permettere a un dispositivo, detto scanner, di rilevare nelle vicinanze altri dispositivi, detti advertiser. Quindi, il compito dello scanner sarà quello di mettersi in ascolto nei canali di advertising e ricevere pacchetti trasmessi da parte degli advertisers.

Il dispositivo advertiser trasmette un pacchetto ogni periodo di advertising ( $T_{adv}$ ). Ogni volta che vengono inviati pacchetti di questo tipo, l'advertiser lo fa attraverso uno dei 3 canali di advertising.

Al fine di evitare interferenze con altri dispositivi, dopo ogni evento di advertising viene aggiunto un tempo randomico che non eccede i 10 ms, in cui il dispositivo trasmittente è in idle.



**FIGURA 15: EVENTO DI ADVERTISING**

I tipo di pacchetti di advertising sono 4:

- **ADV\_IND (Connectable undirected advertising event):** una volta che l'advertiser ha inviato il pacchetto, esso riceverà dallo scanner un pacchetto di tipo SCAN\_REQ, che richiede informazioni aggiuntive. A questo l'advertiser risponde con un altro pacchetto SCAN\_RSP usando lo stesso canale di advertising. Infine, lo scanner può richiedere una nuova connessione con il pacchetto di tipo CONNECT\_REQ.
- **ADV\_DIRECT\_IND (Connectable directed advertising event):** quando l'advertiser manda questo pacchetto esso riceve un pacchetto CONNECT\_REQ dallo scanner.
- **ADV\_NONCONN\_IND (Non-connectable undirected advertising event):** quando l'advertiser manda questo pacchetto, non accetta più connessioni.
- **ADV\_SCAN\_IND (Scannable undirected advertising event):** ha la stessa funzione del pacchetto ADV\_IND, ma in questo caso non accetta nessuna connessione.

**Scanning:** è lo stato complementare a quello di advertising, durante il processo di discover, il dispositivo che assume questo stato diventa uno scanner e si mette in ascolto su ogni canale di advertising, per i pacchetti di advertising, durante una finestra temporale lunga  $T_{scanWindow}$ .

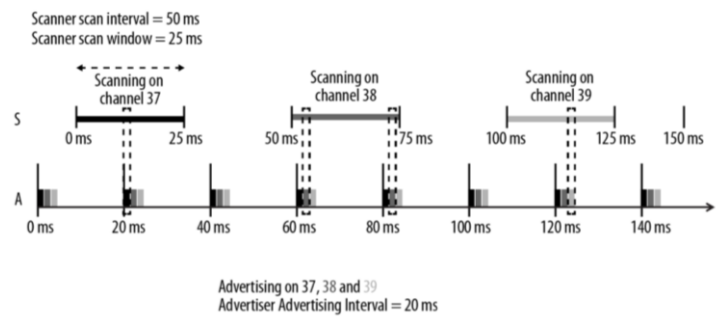
Questo processo verrà ripetuto ogni  $T_{scanInterval}$ , che sarebbe il periodo di scansione, non deve eccedere i 10,24 s.

Ci sono due modalità di scanning:

- **Scansione passiva:** lo scanner riceve i pacchetti dagli advertisers ma non gli risponde.
- **Scansione attiva:** rispetto al tipo di pacchetto di advertising che lo scanner ha ricevuto, risponderà al dispositivo advertiser, cioè il mittente del messaggio.

Il vantaggio del BLE è che all'interno dei pacchetti di advertising di tipo ADV\_IND, ADV\_NONCONN, ADV\_SCAN\_IND, è possibile incorporare fino a 31 bytes di dati, ed è importante perché non è richiesta una connessione preliminare tra i due dispositivi comunicanti.

La figura successiva mostra la sincronizzazione tra l'intervallo di trasmissione dell'advertiser  $T_{adv}$  e tra i periodi nel quale uno scanner è in ascolto su un certo canale,  $T_{scanWindow}$  e  $T_{scanInterval}$ .



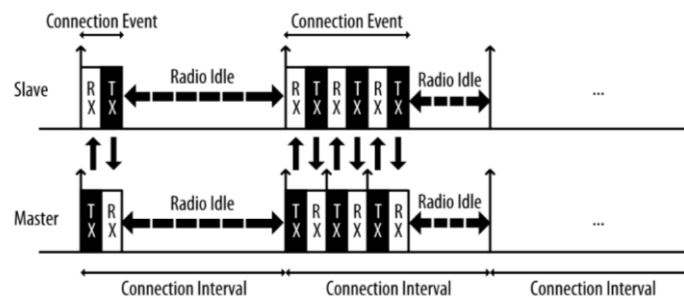
**FIGURA 16: EVENTO DI SCANNING**

**Initiating:** in questo stadio, il ricevitore viene utilizzato per mettersi in ascolto di dispositivi che vogliono iniziare una connessione. Se un pacchetto di advertising viene ricevuto da un dispositivo, il LL invierà una richiesta di connessione all'advertiser. Il ricevente entrerà nel connection stage, assumendo che l'advertiser farà lo stesso. Il pacchetto di advertising che inizia una richiesta di connessione sarà di tipo ADV\_DIRECT\_IND e ADV\_IND.

**Connection:** per stabilire una connessione, il dispositivo che la inizia (initiator) prende il nome di “master” nel LL e si mette in attesa di dispositivi advertiser che accettano la richiesta di connessione. I pacchetti di advertising saranno filtrati secondo l'indirizzo Bluetooth o secondo i dati che il pacchetto trasporta. Quando viene individuato un dispositivo che accetta la richiesta di connessione, esso

diventa uno “slave” e la connessione viene compiuta. Il pacchetto di richiesta di connessione contiene anche un numero, detto il “frequency hopping increment” che determina la sequenza di salto utilizzata da entrambe le parti in tutta la durata della connessione.

Si intende come connessione, una sequenza di scambio di dati tra uno slave ed un master in tempi predefiniti, inoltre ogni scambio di dati è detto “evento di connessione”.



**FIGURA 17: EVENTO DI CONNESSIONE**

Durante l’instaurazione di una connessione, il master comunica allo slave alcuni importanti parametri:

- **Connection Interval:** il tempo trascorso dall’inizio di due eventi di connessione consecutivi, è un valore che varia da un minimo di 7.5 ms a un massimo di 4s;
- **Slave latency:** il numero di eventi di connessione che uno slave sceglie di non effettuare, senza rischiare una disconnessione;
- **Connection supervision timeout:** il tempo massimo che passa tra due pacchetti dati validi ricevuti, prima che una connessione viene considerata persa.

Dato che in una certa area possono esistere un numero di dispositivi BLE, molti dei quali sconosciuti, per motivi di sicurezza il Link Layer prevede una white list che contiene gli indirizzi Bluetooth di dispositivi (sia scanner che advertiser)

interessati. I pacchetti ricevuti che hanno come indirizzo Bluetooth sorgente un indirizzo non presente nella white list, verranno droppati.

Esiste quindi, una policy chiamata “filter policy” che indica se è previsto l’utilizzo di una white list.

Durante una connessione, i dispositivi scambiano pacchetti dati, l’integrità di tutti i pacchetti ricevuti viene verificata grazie al CRC (Codice di Ridondanza Ciclica) di 24 bit e nel caso la verifica non vada a buon fine, i pacchetti verranno ritrasmessi.

Il Link Layer è responsabile anche di:

- **Cambiamento dei parametri di connessione:** i parametri di connessione sono impostati dal master, ma le condizioni e i requisiti possono cambiare durante l’intera connessione. Per questo, il Link Layer permette di richiedere un cambio di parametri della connessione sia da parte del master che dallo slave. In questo modo ogni connessione garantirà il miglior rapporto tra throughput e consumo energetico.
- **Cifratura:** le chiavi che implementano la cifratura sono gestite e generate dall’host, ma il Link Layer esegue la cifratura e decifratura in modo trasparente ai livelli superiori.

### 3.1.3 Link Layer (Struttura dei pacchetti)

#### Struttura dei pacchetti (LE1 ed LE2 non codificati) per la versione 4.2

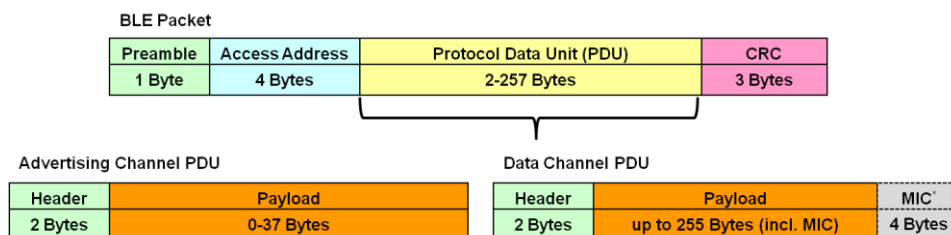


FIGURA 18: PACCHETTO BLE

- **Preambolo:** sequenza fissa di 0 e 1 utilizzata per la sincronizzazione temporale tra trasmettitore e ricevitore;
- **Access address:** un valore randomico che identifica l'accesso a un canale fisico;
- **PDU:** i dati che il pacchetto trasporta e include anche gli indirizzi del trasmettitore (source address) e ricevitore (destination address) sono lunghi 6 bytes e sono all'interno del PDU;
- **CRC:** codice di ridondanza ciclica, è una tecnica di codifica che serve per ricostruire i dati del pacchetto e ne garantisce l'integrità.

Gli indirizzi del trasmettitore (source address) e ricevitore (destination address) sono lunghi 6 bytes e sono all'interno del PDU.

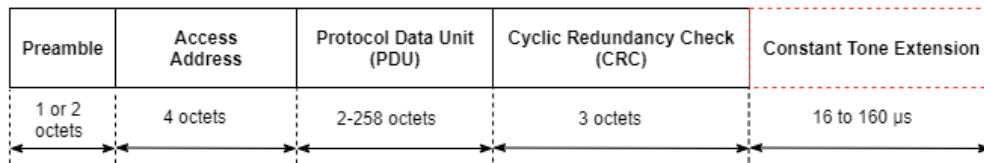
Le categorie di PDU nei pacchetti in BLE sono due:

- **Advertising Channel PDU:** il PDU utilizzato nei pacchetti di advertising, è lungo massimo 37 bytes e viene scambiato attraverso i canali di advertising.
- **Data Channel PDU:** il PDU utilizzato per lo scambio di dati, ha dimensioni massime molto maggiori dell'Advertising Channel PDU, al suo interno è possibile avere un Message Integrity Check, per incrementare la sicurezza.

## **Struttura dei pacchetti in BLE v5**

Come visto in precedenza, si hanno 3 tipi di livello fisico nella versione 5 del BLE, tra di essi si può fare un'ulteriore distinzione: i tipi LE 1M e LE 2M sono non codificati, mentre il tipo LE coded è codificato. Per via di questa differenza si hanno due strutture di pacchetti diversi.



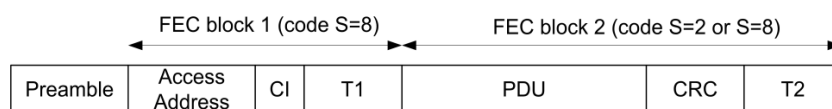


**FIGURA 19: PACCHETTO LE 1M E 2M**

Dopo il CRC, si aggiunge una parte opzionale detta Constant Tone Extension (CTE) che può essere utilizzata per il direction finding ed è disponibile per i pacchetti di advertising e di dati, la sua durata è compresa tra i 16 e i 160 microsecondi. Il preambolo è di 1 Byte per LE 1M e 2 Bytes per LE 2M.

Pacchetto per livello fisico codificato (LE Coded):

il preambolo è l'unica parte non codificata. L'access address, il CI (Coded Indicator) e il T1 (Termination field) fanno parte del blocco di codifica FEC 1, il PDU, il CRC e il T2 faranno parte del blocco di codifica FEC 2. Il primo blocco è quasi sempre trasmesso con S=8 invece il secondo blocco sia con S=8 che con S=2, CI specifica la codifica del secondo blocco. T1 e T2 sono generati usando un codificatore a correzione d'errore in avanti.



**FIGURA 20: PACCHETTO LE CODED**

Il PDU ha lunghezza variabile, un pacchetto codificato può essere lungo da 160 a 2200 bits, quindi, un pacchetto codificato con S=8 è lungo in termini di tempo da 720 a 17040 microsecondi e con S=2 da 462 a 4542 microsecondi.

PDU di un pacchetto di advertising:

Header (Advertising), 16 bits						Payload
PDU type	RFU	ChSel	TxAdd	RxAdd	Length	
4 bit	1 bit	1 bit	1 bit	1 bit	8 bit	8... 2040 bit

**FIGURA 21: PDU DI UN PACCHETTO DI ADVERTISING**

Il suo header in totale è lungo 16 bit e il payload può essere lungo da 8 a 2040 bits. Il campo PDU type definisce quale è il tipo di pacchetto di advertising (es. ADV\_IND per un avviso generale, CONN\_REQ per l’inizio di una connessione) e la lunghezza indica quanto è lungo il payload.

Il formato del payload del pacchetto di advertising introduce novità rispetto Bluetooth v4:

Payload (Advertising), 1...255 octets (8...2040 bit)			
Extended Header Length	Adv Mode	Extended Header	AdvData
6 bit	2 bit	0...504 bit	0...2032 bit

**FIGURA 22: PAYLOAD DI UN PACCHETTO DI ADVERTISING**

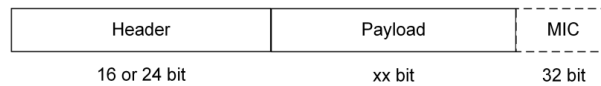
I campi nuovi sono descritti in seguito (i più significativi):

- **Extended Header Length:** indica la lunghezza dell’extended header in bytes;
- **AdvMode:** indica la modalità, “connectable” e/o “scannable” oppure “non connectable” e/o “non scannable”;
- **AdvData:** il payload del pacchetto di advertising;
- **Extended Header:** l’header estendibile che ha una lunghezza variabile:
  - **Ext Header Flags:** sono dei campi flags che indicano se nell’extended header sono presenti campi successivi oppure no;
  - **AdvA:** indirizzo dell’advertiser;
  - **Target A:** indirizzo del destinatario;
  - **CTEInfo:** Constant Tone Info è un campo per il Direction Finding;

In più, vengono introdotti nuovi tipi di pacchetti di advertising:

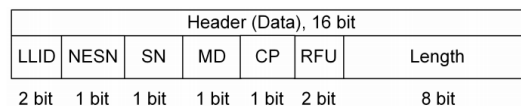
- **ADV\_EXT\_IND**: General advertising extended;
- **AUX\_ADV\_IND**: AUX packet;
- **AUX\_SYNC\_IND**: Periodic advertising
- **AUX\_CHAIN\_IND**: Chain of data

PDU per pacchetto dati:

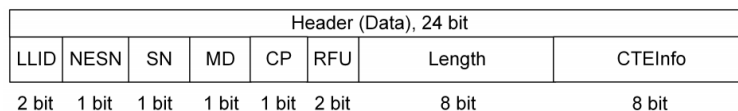


**FIGURA 23: PDU PER PACCHETTO DATI**

Ha un header di lunghezza variabile, di 16 o di 24 bits che dipende dall'utilizzo del Direction Finding e il payload lungo un numero indefinito di bits, dipende dai dati che il pacchetto trasporta.



**FIGURA 24: PDU PER HEADER A 16 BIT**



**FIGURA 25: PDU PER HEADER A 24 BIT**

Campi:

- **LLID**: indica se viene trasmesso un PDU data o un PDU control;

- **SN e NESN:** Sequence Number e Next Expected Sequence Number, sono utili per il controllo del flusso e agiscono come meccanismi di acknowledgement;
- **CP:** CTEInfo Present, indica se nel pacchetto ci sarà il campo CTEInfo oppure no, quindi, da questo campo si deduce se la dimensione dell'header è di 16 o 24 bits;
- **Lenght:** lunghezza del payload;
- **CTEInfo:** Constant Tone Info è un campo per il Direction Finding, che ha dei sottocampi:
  - **CTETime:** controlla la durata del CTE in unità di 8 microsec, assume un valore compreso tra 2 e 20, che indicano 16 e 160 microsec, rispettivamente;
  - **CTEType:** definisce il tipo di CTE.

### 3.1.4 Host Controller Interface

È un protocollo che si occupa di gestire la comunicazione tra il Controller e l'Host, quindi, ad esempio, è il livello che gestisce la comunicazione tra l'hardware e l'applicazione utilizzata dall'utente. L'HCI ha una serie di comandi ed eventi che consentono la connessione del Controller con l'Host, definisce anche come deve essere strutturato un pacchetto e le regole di controllo di flusso dei dati.

Il suo ruolo è quello di definire un set di comandi che hanno lo scopo di tradurre i dati grezzi provenienti dalla parte hardware in pacchetti che trasportano informazione. Poi questi pacchetti li dovrà inviare al livello Host e viceversa, tradurre i pacchetti in dati grezzi da fornire al livello inferiore. È il livello che permette l'interoperabilità tra hosts e controllers di diverse case produttrici.

Il controller è il modulo che ha requisiti di funzionamento real-time ed è a stretto contatto con il livello fisico, perciò, è semplice separarlo dal modulo Host che ha requisiti di tempo meno stringenti, ma effettua operazioni molto più complesse.

Ad esempio, negli smartphone l'Host, quindi anche l'applicazione, girano sulla CPU, mentre il Controller si trova in un chip a parte, connesso tramite UART o USB.

## 3.2 Host

### 3.2.1 L2CAP

Questo modulo implementa due funzionalità principali, prende protocolli multipli dai livelli più alti e li incapsula nel formato standard di un pacchetto BLE e viceversa.

È il livello che si occupa anche di frammentazione e ricombinazione, quindi, prende un pacchetto di dimensioni grandi e lo frammenta in pacchetti BLE aventi un payload massimo di 27 bytes. Al lato ricezione, i pacchetti multipli ricevuti vengono ricombinati opportunamente.

Il layer L2CAP è responsabile di due protocolli principali, Attribute Protocol (ATT) e Security Manager Protocol (SMP).

### 3.2.2 ATT

È un protocollo client/server di tipo state-less, basato sugli "attributi". In BLE un dispositivo è un client, un server o entrambi, indipendentemente dal fatto di essere un master o uno slave. Il protocollo prevede che se una richiesta viene inviata, ma non arriva ancora una risposta, una nuova richiesta non può essere fatta finché non si riceve quella risposta (vale sia se il dispositivo si comporta da client che da server).

Un server contiene dati organizzati in forma di attributi, ad ognuno dei quali è assegnato un identificatore universale (UUID), un gestore di attributi a 16 bit, un set di autorizzazioni ed un valore.

Un UUID è un Universally Unique Identifier, lungo 128 bit ed è un numero globalmente unico. Anche altri protocolli e tecnologie utilizzano l'UUID, ma nel Bluetooth, siccome i pacchetti trasmessi hanno dimensioni molto piccole, l'utilizzo di questo codice lungo 128 bit potrebbe essere un problema.

Per contrastare questo fatto, in BLE esistono due formati aggiuntivi dell'UUID, uno a 32 bit e uno a 16 bit e questi formati più piccoli possono essere utilizzati soltanto nei dispositivi Bluetooth e vengono definiti nella specificazione Bluetooth SIG.

Il SIG mette a disposizione un gran numero di UUIDs per tutti i tipi, i servizi e profili. Se si sviluppa una propria applicazione e si vuole implementare un nuovo caso d'uso che non è presente tra quelli descritti, si può generare un nuovo UUID dalla pagina di generazione dell'ITU.

Il gestore di attributi è un identificatore utilizzato per avere accesso ad un valore di un attributo, invece l'UUID specifica il tipo e la natura del valore dell'attributo.

Il protocollo ATT prevede delle operazioni:

- **Error Handling:** il server risponde alle richieste, con un messaggio di errore;
- **Server Configuration:** per la configurazione del protocollo ATT;
- **Find Information:** utilizzato dal client per ottenere informazioni circa il layout degli attributi del server;
- **Read Operations:** il client può ottenere informazioni di un valore di uno o più attributi;
- **Write operations:** il client può scrivere valori su uno o più attributi;
- **Queued Writes:** usato dal client per scrivere valori di attributi che sono troppo lunghi per entrare in un singolo pacchetto;
- **Server Initiated:** utilizzato dal server per trasmettere i valori degli attributi al client.

### 3.2.3 GATT

Esso è costruito sull'ATT, aggiunge un modello gerarchico e di astrazione di dati. Può essere considerato come il backbone del trasferimento dati BLE, perché definisce come i dati sono organizzati e scambiati tra le applicazioni. Nello specifico descrive come sono scambiati i profili e i dati utente su una connessione BLE.

L'architettura client/server vigente in ATT viene mantenuta, ma i dati in GATT sono incapsulati in "servizi" i quali contengono una o più "caratteristiche".

I dati scambiati vengono organizzati gerarchicamente in sezioni chiamate servizi che raggruppano pezzi di dati utente concettualmente correlati chiamati caratteristiche.

Ruoli dei dispositivi definiti dal GATT:

- **Client:** è uguale al ruolo di client nell'ATT. Il client GATT non conosce a priori gli attributi del server, quindi, per prima cosa deve inviare una ricerca circa la presenza e la natura di questi attributi per migliorare l'individuazione del servizio. Dopo questa fase, il client può iniziare a leggere e scrivere gli attributi trovati all'interno del server;
- **Server:** corrisponde al server descritto nell'ATT. Invia anche aggiornamenti avviati dal server stesso quando configurato per farlo, ed è il ruolo responsabile della memorizzazione e della messa a disposizione del client dei dati dell'utente, organizzati in attributi. Ogni dispositivo BLE deve avere almeno un GATT server che risponderà alle richieste del client.

Bisogna dire che i ruoli definiti del GATT sono indipendenti rispetto i ruoli definiti nel GAP, ma sono compatibili gli uni con gli altri, significa che un GAP central e un GAP peripheral, possono agire come GATT client o GATT server o entrambi allo stesso tempo.

## Attributo

Gli attributi sono la più piccola entità definita dal GATT e dall'ATT. Sono dei pezzi di informazione indirizzabili che contengono dati o metadati dell'utente circa la struttura e il raggruppamento di diversi attributi in un server. I moduli GATT e ATT lavorano con gli attributi, quindi le informazioni devono essere strutturate con la forma di un attributo per permettere l'interazione tra il client e il server. Concettualmente, gli attributi sono sempre memorizzati nel server e sono accessibili (talvolta anche modificabili) dal client.

Gli attributi possono essere memorizzati sia in una memoria non volatile e sia in una RAM.

Un attributo contiene nello specifico:

- Informazioni sull'attributo stesso e il dato attuale;
- **Attribute handle:** è un identificativo univoco a 16 bit di ogni attributo in un server GATT, È indirizzabile e non cambia nel tempo. Solo teoricamente il numero massimo di handles disponibili è di 65535 (in esadecimale 0xFFFFE);
- **Attribute Type:** è un UUID che può essere lungo 16, 32 o 128 bit, determina il genere di dati contenuti in un valore di un attributo e anche i meccanismi disponibili che permettono la ricerca di attributi a seconda del loro tipo;
- **Permissions:** sono metadati che dettano quali operazioni ATT possono essere eseguite su un particolare attributo e specificano i parametri di sicurezza. I tipi di permission sono:
  - **Access permission:** determinano come un client può interagire con un valore di un attributo. Un client può: scrivere un dato, leggerlo, leggerlo e scriverlo oppure non può fare nessuna di queste operazioni;



- **Encryption:** determina se è richiesto un certo livello di cifratura per un attributo. I livelli di cifratura sono, in ordine di sicurezza: Autenticazione e cifratura, solo cifratura e nessuna cifratura;
- **Authorization:** determina se un client deve possedere certi permessi per accedere a un attributo. Per un attributo si possono avere due opzioni: autorizzazione richiesta e nessuna autorizzazione richiesta.
- **Value:** contiene il dato attuale di un attributo, non ci sono limitazioni ai tipi di dato che il “value” può contenere, ma la massima lunghezza è 512 bytes. Il value può contenere anche informazioni aggiuntive ed è quella parte di un attributo, che a seconda del tipo di access permission, può essere sia letta che scritta.

**TABELLA 6: RAPPRESENTAZIONE TIPICA DI ATTRIBUTI**

Handle	Type	Permissions	Value	Value length
0x0201	UUID <sub>1</sub> (16-bit)	Read only, no security	0x180A	2
0x0202	UUID <sub>2</sub> (16-bit)	Read only, no security	0x2A29	2
0x0215	UUID <sub>3</sub> (16-bit)	Read/write, authorization required	“a readable UTF-8 string”	23
0x030C	UUID <sub>4</sub> (128-bit)	Write only, no security	{0xFF, 0xFF, 0x00, 0x00}	4
0x030D	UUID <sub>5</sub> (128-bit)	Read/write, authenticated encryption required	36.43	8
0x031A	UUID <sub>1</sub> (16-bit)	Read only, no security	0x1801	2

### Gerarchia tra gli attributi

GATT prevede una gerarchia che organizza gli attributi in maniera ordinata, questa struttura permette l’accesso e il ripristino di informazioni tra il client e il server, seguendo un set di regole che costituiscono il framework usato da tutti i profili GATT.

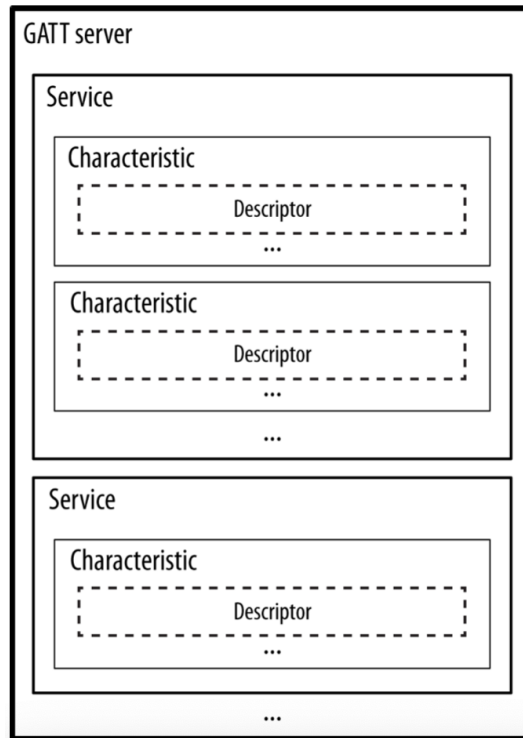


FIGURA 26: STRUTTURA DEI DATI DEL GATT

In un server GATT gli attributi sono raggruppati in servizi, ognuno dei quali contiene 0 o più caratteristiche. Ognuna di queste caratteristiche conterrà 0 o più descrittori.

Per la maggior parte degli attributi, bisogna fare la distinzione tra la loro:

- **Definizione:** l'intero set di attributi che lo compongono;
- **Dichiarazione:** un attributo singolo, messo in prima posizione, all'interno di esso possono essere presenti delle informazioni riguardo i metadati dei dati che seguono questo tipo di attributo. Tutte le dichiarazioni hanno il permesso di sola lettura e sono gli unici attributi che permettono al client di individuare il layout e la natura degli altri attributi nel server GATT.

## Servizi

Un servizio è formato da un set di attributi che mostrano informazioni e concetti comuni.

La specifica si riferisce a tutti gli attributi all'interno di un singolo servizio come "service definition". Gli attributi di un GATT server sono di fatto una successione di service definition, ognuno inizia con un singolo attributo che indica l'inizio di un servizio, esso ha il nome di "service declaration" ed ha la seguente forma:

**TABELLA 7: ATTRIBUTO SERVICE DECLARATION**

Handle	Type	Permissions	Value	Value length
0xNNNN	UUID <sub>primary service</sub> or UUID <sub>secondary service</sub>	Read Only	Service UUID	2, 4, or 16 bytes

Possono esistere servizi di tipo primario (con UUID 0x2800) o secondario (con UUID 0x2801), un servizio primario è la tipologia standard di un servizio GATT che contiene funzionalità standard e rilevanti esposte al GATT server. Un servizio secondario è incluso in altri servizi primari, ma è utilizzato raramente.

Il valore di un attributo di un service declaration contiene un UUID che corrisponde all'UUID del servizio che introduce la service declaration. La service declaration deve essere il primo attributo in un servizio.

In un servizio è possibile aggiungere uno o più riferimenti ad altri servizi, usando le "include definitions", che sarebbero un attributo singolo, detto "include declaration" che contiene tutte le informazioni necessarie per il client per far riferimento al servizio incluso. Si fa questo per evitare la duplicazione di dati nel GATT server, che può risultare ridondante.

Questa è la struttura di un attributo "include declaration":

**TABELLA 8: ATTRIBUTO INCLUDE DECLARATION**

Handle	Type	Permissions	Value	Value length
0xNNNN	UUID <sub>include</sub>	Read only	Included service handle, end group handle, Included Service UUID	6, 8, or 20 bytes

È presente un "UUID include" che è uno speciale UUID assegnato dal SIG dedicato solo alle include declaration e vale 0x2802.

## Caratteristiche

Una caratteristica è una sorta di contenitore dei dati utente. Esse contengono almeno 2 attributi, la “characteristic declaration”, che riguarda i metadati relativi ai dati utente e il “characteristic value”, un attributo che contiene i dati utente.

Un characteristic value può essere seguito da dei descrittori, che incrementano i metadati contenuti nella characteristic declaration.

Questa dichiarazione, valore e i descrittori, formano la “characteristic definition”, cioè la serie di attributi che compongono una singola caratteristica.

Nella tabella è riportata la struttura di attributi di tipo “characteristic declaration” e “characteristic value”:

**TABELLA 9: ATTRIBUTO CHARACTERISTIC DECLARATION**

Handle	Type	Permissions	Value	Value length
0xNNNN	UUID <sub>characteristic</sub>	Read only	Properties, value handle (0xMMMM), characteristic UUID	5, 7, or 19 bytes
0xMMMM	Characteristic UUID	Any	Actual value	Variable

Characteristic declaration: l’UUID di questo attributo è 0x2803, che denota l’inizio di una caratteristica. Il valore dell’attributo characteristic declaration è composto da 3 campi:

**TABELLA 10: CAMPI DELL'ATTRIBUTO CHARACTERISTIC DECLARATION**

Name	Length in bytes	Description
Characteristic Properties	1	A bitfield listing the permitted operations on this characteristic
Characteristic Value Handle	2	The handle of the attribute containing the characteristic value
Characteristic UUID	2, 4, or 16	The UUID for this particular characteristic

- **Characteristic properties:** rappresenta le operazioni e procedure che possono essere utilizzate con questa caratteristica. Queste proprietà sono del tipo Broadcast, Read, Write, quindi il client legge queste proprietà e vede quale tipo di operazione può eseguire sulla caratteristica in questione;

- **Characteristic Value Handle:** contiene l'attribute handle dell'attributo che contiene il valore della caratteristica;
- **Characteristic UUID:** è l'UUID di una caratteristica, può essere un valore approvato dal SIG, se si intende l'uso di una caratteristica inclusa nei profili standard, oppure un UUID a 128 bit, specificato dal produttore.

Si può fare un parallelismo con la programmazione ad oggetti se si pensa che un servizio GATT sia una classe che può essere istanziata diverse volte nel server GATT. Invece le "include definitions" sono dei puntatori a un'istanza dell'oggetto esistente.

Le caratteristiche, invece, sono come le proprietà di una classe e il profilo è come un'applicazione che fa uso di una o più classi.

Characteristic value attribute: esso contiene i dati utente che un client può leggere e/o scrivere. Il tipo di questo attributo è sempre lo stesso UUID nel campo value della characteristic declaration. Questi UUID riguardano i dati concreti, come ad esempio la lettura di un valore effettuata da un sensore.

Questo valore può contenere qualunque tipo di dato che può essere scambiato tra due dispositivi BLE.

### **Descrittori di caratteristiche o Descrittori**

Utilizzati per rendere disponibili a un client i metadati, cioè informazioni aggiuntive riguardo la caratteristica e il suo valore.

I descrittori hanno un singolo attributo detto "characteristic descriptor declaration" e il suo UUID è lo stesso del tipo di descrittore e il suo valore contiene tutto ciò che è definito da quel particolare descrittore.

Ci sono due tipi di descrittori:

- **GATT-defined descriptors:** sono i descrittori più utilizzati e aggiungono metainformazioni sulla caratteristica;

- Profile or vendor-defined descriptors: essi contengono tutti i tipi di dati anche informazioni aggiuntive riguardo i characteristic values, senza guardare se un profilo è specifico, quindi, pubblicato dal SIG oppure è proprietario di un certo produttore.

Heart Rate Service				
	Handle	UUID	Permissions	Value
Service	0x0021	SERVICE	READ	HRS
Characteristic	0x0024	CHAR	READ	NOT[0x0027]HRM
	0x0027	HRM	NONE	bpm
Descriptor	0x0028	CCCD	READ/WRITE	0x0001
Characteristic	0x002A	CHAR	READ	RD[0x002C]BSL
	0x002C	BSL	READ	<i>finger</i>

FIGURA 27: ESEMPIO DI SERVIZIO GATT

Viene mostrato il profilo di Heart Rate Service (HRS) che è un profilo standard che si trova anche in prodotti BLE commerciali. Intanto si può notare come la forma di un attributo prevede sempre la sequenza di handle, UUID, Permissions, Value:

- **Handle 0x0021 (Servizio):** contiene la service declaration per l'HRS che è formata da un UUID primary service che vale 0x2800 e da un valore che riguarda l'UUID assegnato dal SIG per l'HRS.
- **Handle 0x0024 (Caratteristica):** contiene la characteristic declaration per la caratteristica dell'HRM. I suoi campi sono l'UUID characteristic standard che vale 0x2803 e il valore che riguarda la proprietà della caratteristica di inviare solo una notifica. Il characteristic value handle è 0x0027 e il characteristic value UUID è quello per l'HRM che vale 0x2A37.

- **Handle 0x0027 (Caratteristica):** contiene il characteristic value, in questo caso dell'HRM, i suoi campi sono:
  - L'UUID che è lo stesso UUID presente negli ultimi 2 bytes del valore della characteristic definition;
  - I permessi, in questo caso il valore non può essere né letto né scritto, quindi il valore può essere ottenuto attraverso una notifica dal server;
  - Valore, cioè il valore attuale del battito cardiaco in bpm.
- **Handle 0x0028 (Descrittore):** questo attributo contiene un descrittore di tipo CCCD (Client Characteristic Configuration Descriptor), i suoi campi sono:
  - L'UUID, è quello relativo a un CCCD ed è standard 0x2902;
  - I permessi, il CCCD può essere sempre scrivibile o leggibile, il livello di sicurezza richiesto per definire le operazioni è definito dal profilo o dall'applicazione;
  - Il valore, in questo caso denota che questa notifica è abilitata per questa particolare caratteristica di HRM.

#### 3.2.4 SMP

È sia un protocollo che una serie di algoritmi di sicurezza, che servono a gestire e scambiare chiavi di sicurezza che permettono una comunicazione Bluetooth sicura tra i dispositivi attraverso canali cifrati. Sono utili anche per appurare l'identità di un dispositivo remoto e anche per nascondere l'indirizzo Bluetooth quando serve.

Vengono definiti 2 ruoli:

- **Initiator:** corrisponde al Link Layer master e al GAP central;
- **Responder:** corrisponde al Link Layer slave e al GAP peripheral.

È sempre l'initiator che si occupa di avviare la procedura, il responder farà una richiesta asincrona dell'inizio di una delle procedure prevista dal SM.

Procedure di Sicurezza:

- **Pairing:** con questa procedura, viene generata una chiave di cifratura temporanea che serve a garantire un collegamento sicuro e cifrato. La chiave non è memorizzata e non è utilizzabile per connessioni consecutive. Il pairing crea un collegamento sicuro solo per il tempo di una connessione;
- **Bonding:** una sequenza di "pairing" seguita dalla generazione e lo scambio di chiavi di sicurezza permanenti, che dovranno essere salvate all'interno di una memoria non volatile e seguita dalla creazione di un legame tra due dispositivi che permette un set up di collegamenti sicuri multipli consecutivi, molto veloce, senza dover iniziare un'ulteriore procedura di bonding per questi nuovi collegamenti. Il bonding crea una associazione permanente, utilizzata anche per le connessioni successive.
- **Encryption Re-establishment:** quando viene completata la procedura di bonding, le chiavi permanenti vengono salvate all'interno dei due dispositivi comunicanti. Questa procedura indica come devono essere utilizzate queste chiavi in connessioni consecutive e come ristabilire una connessione sicura senza dover effettuare un'altra procedura di bonding o di pairing.

### 3.2.5 GAP

Questo livello definisce come comunicano i dispositivi BLE al livello basso dello stack. Il GAP è molto importante perché definisce come i dispositivi debbano compiere operazioni di controllo, come il discovery di altri dispositivi, la connessione, stabilire requisiti di sicurezza ed assicura l'interoperabilità tra prodotti di altri vendor.

Nel GAP vengono descritti i seguenti aspetti:



- **Ruoli:** ogni dispositivo può assumere uno o più ruoli contemporaneamente, ogni ruolo ha le sue caratteristiche che un dispositivo deve rispettare. I dispositivi che assumono determinati ruoli possono comunicare tra di loro.
- **Modalità:** sono rifiniture del concetto di ruolo, una modalità è lo stato in cui un dispositivo si trova, in un certo periodo di tempo, per raggiungere un determinato obiettivo o nello specifico, di consentire a un peer di eseguire una procedura. I cambiamenti di modalità possono essere frequenti nei dispositivi BLE.
- **Procedure:** è una sequenza di azioni, solitamente sequenze di controllo del Link Layer o scambio di pacchetti, che consente a un dispositivo di raggiungere un obiettivo. Una procedura è tipicamente associata a una modalità sull'altro peer, quindi, sono due concetti che si accomunano.
- **Sicurezza:** il GAP definisce modalità e procedure di sicurezza che indicano come i peers debbano settare il livello di sicurezza richiesto per uno scambio di dati. Il GAP aggiunge proprietà di sicurezza addizionali, che non sono associati a modalità o procedure, che possono essere utilizzati da applicazioni per rinforzare il livello di sicurezza.
- **Altri formati definiti dal GAP:** il GAP viene utilizzato anche come "segnaposto" per alcune definizioni di formato dati aggiuntive, correlate alle modalità e procedure definite dalla specificazione GAP.

## **Ruoli**

Ne sono in totale 4: Broadcaster, Observer, Central, Peripheral. Ogni dispositivo può anche assumere più ruoli contemporaneamente, inoltre, i ruoli del GATT sono diversi e non riconducibili ai ruoli del GAP.

- **Broadcaster:** un ruolo utilizzato da applicazioni che prevedono una trasmissione regolare di dati, perché il broadcaster, trasmette a tutti i dispositivi che sono in ascolto nella sua area di copertura, pacchetti di

advertising. L'equivalente del ruolo broadcaster nel GAP è il ruolo advertiser nel Link Layer.

- **Observer:** riguarda applicazioni nelle quali è sufficiente ricevere dati e non trasmetterli. Un dispositivo che assume il ruolo di observer è in ascolto di pacchetti di advertising, trasmessi per l'appunto da un broadcaster. L'equivalente del ruolo observer nel GAP è il ruolo scanner nel Link Layer.
- **Central:** è un ruolo che prevede l'instaurazione di connessioni tra uno o più dispositivi alla volta. Il dispositivo con ruolo "central" è quello che inizia la connessione e abilita l'accesso agli altri dispositivi alla rete. L'equivalente del ruolo central nel GAP è il ruolo master del Link Layer. Il protocollo BLE è asimmetrico, cioè prevede che i requisiti tecnici e computazionali del master siano molto maggiori rispetto quelli degli slave, in modo tale da consentire connessioni multiple. Il dispositivo central inizia il suo lavoro mettendosi in ascolto di pacchetti di advertising e una volta ricevuti avvia una connessione con questi ultimi.
- **Peripheral:** un dispositivo peripheral invia pacchetti di advertising che permetteranno a dispositivi central, di individuarli e in seguito di stabilire una connessione con essi. Il protocollo BLE è ottimizzato nel richiedere solo le risorse necessarie, in termini di consumo di potenza e di occupazione di memoria.

Le configurazioni più comuni, che riguardano i ruoli del GAP, sono essenzialmente due:

- **Broadcast di dati:** in questa modalità viene implementata uno scambio di dati one-to-many, di tipo connection-less e unidirezionale. Ci sarà un dispositivo che assume il ruolo di "Observer", che è in ascolto sui canali per i pacchetti di advertising e uno o più dispositivi che assumono il ruolo di "Broadcaster". Essi trasmettono ogni intervallo pacchetti di advertising

in broadcast e non si occupano della ricezione di dati quando sono in questa modalità.

Non ci sono restrizioni nella documentazione ufficiale del BLE per quanto riguarda il numero massimo di Broadcaster che un Observer è in grado di ascoltare, le prestazioni di questa configurazione dipende dal grado di affollamento della banda dei 2,4 GHz anche di altri dispositivi che per trasmettere dati utilizzano questa banda che potrebbero causare interferenze. Questa è la configurazione utilizzata per la realizzazione di un sistema di localizzazione con i beacon Bluetooth.

- **Connessioni:** a differenza della configurazione precedente, l'instaurazione di una connessione consente una comunicazione one-to-one, connection-oriented e bidirezionale. Un dispositivo che ha una certa capacità di calcolo assumerà il ruolo di "Central", uno o più dispositivi che non dispongono di un'alta capacità di calcolo, di conseguenza consumano minor potenza per funzionare, assumono il ruolo di "Peripheral". Una tipica configurazione di questo genere prevede un device "Central" (ad esempio un Laptop o uno Smartphone) connesso a uno o più devices "Peripheral" (ad esempio cuffie, cardiofrequenzimetro, casse musicali ecc.). Lo scambio di dati avviene solo quando viene completata la connessione tra i due dispositivi ed in più, il "Central", ha bisogno di avere una certa capacità di calcolo che permetta la gestione di più connessioni con i "Peripherals" contemporaneamente.

## **Modi e Procedure**

Nelle seguenti tabelle vengono mostrati i modi con le procedure applicabili e le procedure con i modi richiesti.

**TABELLA 11: MODI**

Mode	Applicable Role(s)	Applicable Peer Procedure(s)
Broadcast	Broadcaster	Observation
Non-discoverable	Peripheral	N/A
Limited discoverable	Peripheral	Limited and General discovery
General discoverable	Peripheral	General discovery
Non-connectable	Peripheral, broadcaster, observer	N/A
Any connectable	Peripheral	Any connection establishment

**TABELLA 12: PROCEDURE**

Procedure	Applicable Role(s)	Applicable Peer Mode(s)
Observation	Observer	Broadcast
Limited discovery	Central	Limited discoverable
General discovery	Central	Limited and General discoverable
Name discovery	Peripheral, central	N/A
Any connection establishment	Central	Any connectable
Connection parameter update	Peripheral, central	N/A
Terminate connection	Peripheral, central	N/A

### 3.3 Beacons

Sono dei dispositivi Bluetooth dotati di un circuito elettronico molto semplice. La loro unica funzione è di trasmettere pacchetti Bluetooth di advertising in modalità broadcast unidirezionale ad intervalli di tempo prefissati (intervallo di advertising) ed i dispositivi ricevitori nelle vicinanze rileveranno quel segnale.

I beacons trasmettono un segnale che conterrà il suo id unico (cioè il bluetooth address) ed altri dati, che dipendono dal tipo di protocollo come ad esempio quelli di telemetria.

Un dispositivo BLE, che lavora in modalità scanner, effettua scansioni temporali per questi pacchetti con un certo periodo di scansione e una certa finestra di scansione, in seguito li decodifica per ricavarne il contenuto ed eseguire particolari azioni. Il periodo e la finestra di scansione del ricevitore sono settati individuando

un compromesso tra consumo energetico e quantità di dati da ricevere. Al lato del trasmettitore, allo stesso modo bisogna settare l'intervallo di advertising e la potenza trasmissiva considerando il rapporto risoluzione – consumo energetico.

Sono alimentati a batteria ed hanno la particolarità di consumare una quantità minima di energia, poiché sono basati sullo standard BLE. Il tipo di batteria dalla quale ricevono energia, è una caratteristica fondamentale, in quanto alcune batterie (ad esempio quelle a bottone) che hanno una durata di vita media molto inferiore rispetto altre.

I beacons sono adoperati in moltissime applicazioni, come il wayfinding, il retail offering, la localizzazione e la trasmissione in broadcast di notifiche.

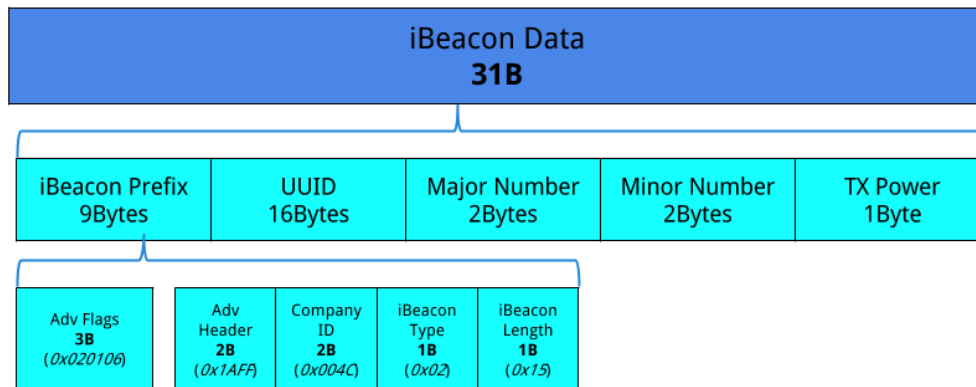
I protocolli beacon più noti sono iBeacon, Eddystone, AltBeacon.

### 3.3.1 Protocollo iBeacon

È il primo standard beacon, nasce nel 2013 da Apple, per i dispositivi IOS versione 7 ed è una tecnologia proprietaria. I dispositivi che implementano iBeacon inviano un solo tipo di segnale, l'iBeacon Advertising Packet, che contiene un identificatore unico del beacon codificato da tre numeri [23]:

- **UUID:** un numero esadecimale lungo 16 bit che identifica univocamente una particolare applicazione o caso d'uso;
- **Major Number:** descrive un sottogruppo di beacon;
- **Minor Number:** identifica il singolo beacon.

Major Number e Minor Number (il cui valore è compreso tra 0 e 65535) sono degli identificatori che riguardano il beacon, ad esempio in una sala di un cinema possono essere installati dei beacons che hanno stesso major number (che identifica tutti i beacons in quella stanza) e ognuno di essi avrà un minor number diverso, perché esso serve per identificare univocamente il dispositivo.



**FIGURA 28: PACCHETTO IBEACON**

Nel PDU del pacchetto advertising sono contenuti 2 ottetti di header, 6 byte del MAC address di chi ha trasmesso il pacchetto e da 0 a 31 bytes di dati. Dentro il campo data è presente la struttura di un pacchetto iBeacon, che prevede:

- 9 bytes di iBeacon prefix: sono 9 bytes fissi di preambolo, necessari per indicare che il dispositivo che ha trasmesso il dato è un dispositivo iBeacon;
- 16 bytes di Proximity UUID;
- 2 bytes di Major Number;
- 2 bytes di Minor Number;
- 1 byte di Tx power: viene data anche l'informazione sulla potenza trasmessa, per ottenere in ricezione, informazioni sulla distanza tra beacon e ricevitore. Solitamente inteso come valore di RSSI misurato ad 1 metro.

I dispositivi con sistema operativo IOS (da IOS 7 in poi) possono anch'essi generare messaggi iBeacon se viene impostata la modalità advertiser, ma hanno prestazioni inferiori rispetto i beacon stessi.

Il protocollo iBeacon presenta degli svantaggi, il primo è dovuto soprattutto perché esso ha una tecnologia e uno standard proprietari e questo fatto ha rallentato i progressi riguardo le applicazioni che possono essere sviluppate con iBeacon.

### 3.3.2 Protocollo Eddystone

Struttura dei pacchetti Eddystone:

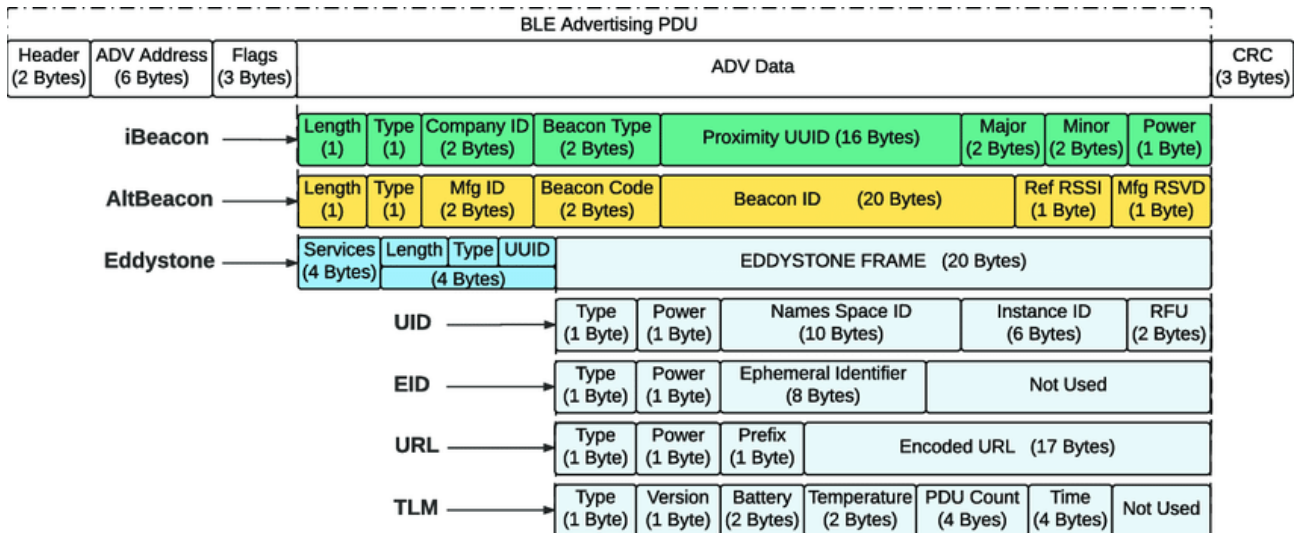


FIGURA 29: PACCHETTO EDDYSTONE

Eddystone, al contrario di iBeacon, è un open-standard, rilasciato da Google nel luglio del 2015, si distingue da iBeacon e AltBeacon in quanto definisce quattro diversi tipi di frame:

- **Eddystone-UID:** funziona proprio come iBeacon, quindi vengono trasmessi messaggi beacon con ID univoco e in ricezione serve un'applicazione in grado di leggere e interpretare il messaggio. L'ID è suddiviso in un namespace identifier di 10 byte (utilizzato per identificare un determinato gruppo di beacon), un instance identifier di 6 byte (identifica il singolo beacon all'interno del gruppo) ed 1 byte di power calibration (solitamente è il valore di RSSI misurato a 0m);
- **Eddystone-URL:** il messaggio trasmesso è una stringa URL compressa, quindi, il dispositivo che lo riceve può decodificare e utilizzare questa stringa per aprire un contenuto in un browser;

- **Eddystone-TLM:** serve per trasmettere dati di telemetria e salute del beacon stesso, come stato della batteria, temperatura del dispositivo, conteggio dei pacchetti inviati;
- **Eddystone-EID:** utilizzato per applicazioni che richiedono maggior livello di sicurezza. L'ID che viene trasmesso è temporaneo e criptato, varia dopo un certo periodo di tempo impostabile in fase di configurazione. Questo identificatore può essere decriptato utilizzando il servizio usato per la configurazione.

Questi profili di Eddystone sono trasmessi in modo indipendente tra loro, quindi un beacon compatibile con lo standard Eddystone, può trasmettere tutti e 4 i profili, in intervalli di advertising prefissati.

### 3.3.3 Protocollo AltBeacon

È un protocollo Beacon che definisce un formato per pacchetti di advertising di prossimità [22]. Il pacchetto trasmesso dal beacon contiene delle informazioni che il dispositivo ricevente utilizzerà per identificare il beacon e per calcolare la distanza.

La struttura di un pacchetto AltBeacon è la seguente:

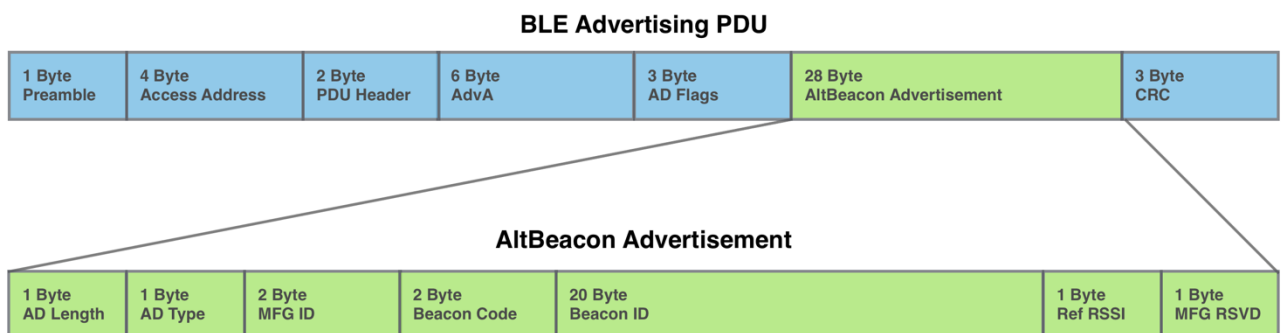


FIGURA 30: PACCHETTO ALTBEACON



#### Descrizione dei campi:

- **AD Length:** lunghezza del tipo e della porzione dei dati della struttura dati indicata dal produttore;
- **AD Type:** il tipo di rappresentazione della struttura dati indicata dal produttore;
- **MFG ID:** il codice identificativo dell'azienda produttrice del beacon, assegnato dal Bluetooth SIG;
- **BEACON CODE:** il codice di advertising di AltBeacon (0xBEAC)
- **BEACON ID:** codice che identifica in modo unico un beacon;
- **REFERENCE RSSI:** rappresenta l'RSSI medio alla distanza di 1m dall'advertiser;
- **MFG RESERVED:** spazio riservato all'implementazione di nuove features da parte del produttore.

#### 4 Algoritmi di localizzazione e stato dell'arte

Esistono diversi modi di calcolare il dato di posizione in un sistema IPS. Ognuno di essi ha i suoi pro ed i suoi contro e possono consentire di raggiungere diversi livelli di accuratezza. In seguito, verranno descritti gli algoritmi di localizzazione utilizzati dalle tecnologie Bluetooth e UWB. La ricerca degli articoli è volta ad individuare le migliori applicazioni rispetto al caso d'uso considerato.

Per questa tipologia di progetto, non è necessario raggiungere un livello di accuratezza molto alto, è tollerabile un errore di posizionamento di 2 m circa, inoltre, una specifica molto importante è il costo della soluzione che dev'essere preferibilmente basso. Bisogna anche individuare un sistema che non interferisca con altri macchinari elettrici in azione nelle linee produttive e che si possa facilmente interfacciare con la rete WiFi già esistente, per l'aggregazione dei dati diretti ai servizi Cloud.

In vista delle specifiche, la tecnologia che più si avvicina al loro soddisfacimento è il Bluetooth Low Energy. Nel capitolo corrente, saranno presenti anche articoli

che discutono dell'utilizzo della tecnologia UWB, poiché è una degna avversaria della tecnologia BLE, fornisce un livello di accuratezza del centimetro ed ha buone prestazioni in ambienti difficili per la propagazione delle onde elettromagnetiche, per l'appunto in un plant di produzione.

#### 4.1 Articoli del BLE

Nell'articolo [24] viene utilizzare la trilaterazione, quindi bisogna avere a disposizione 3 coordinate note per trovare la posizione. I 3 punti di riferimento sono i centri delle aree di copertura, solitamente approssimate a dei cerchi e le distanze calcolate del dispositivo target sono i raggi di questi cerchi. La posizione del target è ottenuta trovando il punto di intersezione delle 3 equazioni dei cerchi. Siccome la posizione del target è sconosciuta, i valori dei raggi sono calcolati così:

$$d = 10^{\frac{A-RSSI}{10n}} \quad (16)$$

Invece la formula per trovare le distanze tra gli access points e il target, considerando il calo tridimensionale è:

$$r_i^2 = (x_i - x_b)^2 + (y_i - y_b)^2 + (z_i - z_b)^2 \quad (17)$$

I valori  $x_b, y_b, z_b$  formano le coordinate spaziali del beacon e  $x_i, y_i, z_i$  sono coordinate spaziali note degli access points.

Se queste sfere sono sullo stesso piano, le equazioni si semplificano e diventano equazioni di cerchi:

$$\begin{aligned} r_1^2 &= (x_1 - x_b)^2 + (y_1 - y_b)^2 \\ r_2^2 &= (x_2 - x_b)^2 + (y_2 - y_b)^2 \\ r_3^2 &= (x_3 - x_b)^2 + (y_3 - y_b)^2 \end{aligned} \quad (18)$$

Poi si riducono in un set lineare di equazioni che possono essere scritte in forma matriciale:

$$2 \begin{bmatrix} x_3 - x_1 & y_3 - y_1 \\ x_3 - x_2 & y_3 - y_2 \end{bmatrix} \begin{bmatrix} x_b \\ y_b \end{bmatrix} = \begin{bmatrix} (r_1^2 - r_3^2) - (x_1^2 - x_3^2) - (y_1^2 - y_3^2) \\ (r_2^2 - r_3^2) - (x_2^2 - x_3^2) - (y_2^2 - y_3^2) \end{bmatrix} \quad (19)$$

Si è scelto di utilizzare la tecnica di calcolo della multilaterazione, cioè una trilaterazione con più di 3 punti di riferimento.

Il Linear Least Squares è un metodo di multilaterazione, col quale si può stimare la posizione del target, linearizzando il problema mediante un vincolo, con la stima delle distanze e le coordinate degli access points.

La differenza tra i valori delle coordinate degli access points e le coordinate di un access point di riferimento, compongono la matrice A.

$$A = \begin{bmatrix} x_2 - x_1 & y_2 - y_1 \\ x_3 - x_1 & y_3 - y_1 \\ \vdots & \vdots \\ x_n - x_1 & y_n - y_1 \end{bmatrix} \quad (20)$$

La distanza euclidea tra le coordinate dell'i-esimo e j-esimo access point è detta  $d_{ij}$ :

$$d_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \quad (21)$$

Dove “j” è il numero dell’access point di riferimento. In totale ci saranno “n” access points, perciò ci sarà un sistema lineare di (n-1) equazioni. L’equazione successiva è usata per calcolare il vettore dei termini noti:

$$\vec{b} = \begin{bmatrix} b_{21} \\ b_{31} \\ \vdots \\ b_{n1} \end{bmatrix} = \begin{bmatrix} \frac{1}{2}(r_1^2 - r_2^2 + d_{21}^2) \\ \frac{1}{2}(r_1^2 - r_3^2 + d_{31}^2) \\ \vdots \\ \frac{1}{2}(r_1^2 - r_n^2 + d_{n1}^2) \end{bmatrix} \quad (22)$$

La posizione stimata del target è data da:

$$A^T A \vec{x} = A^T \vec{b} \quad (23)$$

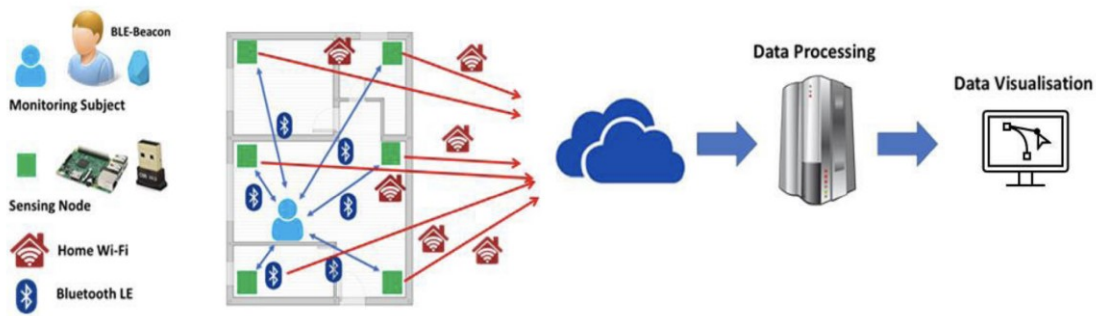
Le coordinate del beacon saranno quelle date dal vettore  $\vec{x}$ .

Poi viene applicato il metodo di Newton Raphson per migliorare la somma dei quadrati minimi.

Invece in [25] si promuove una soluzione a basso costo rispetto gli altri sistemi di localizzazione, prevede l'utilizzo del BLE per la localizzazione indoor.

Per migliorare l'accuratezza di posizione, vengono usati i filtri di Kalman e il Particle Filter, per ridurre la variazione dell'RSSI. Le tecniche utilizzate sono la triangolazione e il fingerprinting.

Per prima cosa sono stati scelti dei Beacon low cost per tracciare i target, essi inviano un segnale beacon in broadcast regolarmente (ogni 100 ms fino a 1000 ms). il sistema è composto da Raspberry Pi con un modulo aggiuntivo BLE, integrato tramite porta USB. I dati trasmessi dai beacon vengono captati dalle Raspberry che individuano quale è l'RSSI di quell'indirizzo MAC corrispondente allo specifico beacon. Le Raspberry sono connesse a un server locale e si occupano, una volta ricevuti i dati, di fare data processing, inclusi anche il training per il classificatore di machine learning.



**FIGURA 31: ARCHITETTURA OPERATIVA**

I beacons BLE sono di Estimote e JAALee e sono stati progettati per poter fare localizzazione. Essi hanno un intervallo di broadcast di circa 1 secondo che può essere modificato con l'apposita applicazione mobile. La loro batteria può durare da pochi mesi a diversi anni.

Le Raspberry pi per captare i pacchetti BLE ha bisogno di un modulo BLE, integrato tramite USB. Essa usa la libreria BlueZ per captare i dati RSSI dai beacons. I dati sono salvati localmente nella Raspberry e viene fatto l'upload regolarmente al web server.

Per identificare il beacon si usa il MAC address suo e solo i valori di RSSI vengono memorizzati nella memoria.

La tecnica per il calcolo della posizione scelta è basata l'RSSI e la distanza. Per localizzare il target, questo metodo utilizza i cambiamenti del segnale RSSI rispetto alla distanza ottenuta dal modello di propagazione del segnale. Il calcolo della distanza avviene come nell'equazione (16).

Poi viene implementato un algoritmo di trilaterazione basato sulle coordinate fisse e note di 3 Raspberry e le equazioni che ne conseguono consentono il calcolo della posizione del beacon.

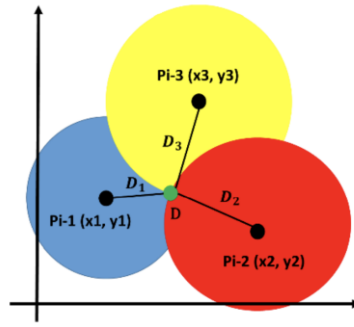


FIGURA 32: TECNICA DELLA TRILATERAZIONE

$$\begin{cases} D_1 = \sqrt{(x - x_1)^2 + (y - y_1)^2} \\ D_2 = \sqrt{(x - x_2)^2 + (y - y_2)^2} \\ D_3 = \sqrt{(x - x_3)^2 + (y - y_3)^2} \end{cases} \quad (24)$$

L'equazione si semplifica se si fanno coincidere le coordinate (0,0) con il sensore  $Pi-1$ :

$$\begin{cases} x = \frac{D_1^2 - D_2^2 + x_2^2}{2x_2} \\ y = \frac{D_1^2 - D_3^2 - 2x_3x + y_3^2 + x_3^2}{2y_3} \end{cases} \quad (25)$$

Per via dei diversi ostacoli in un locale indoor, i dati RSSI grezzi potrebbero risultare molto rumorosi. Può succedere che in tante misurazioni fatte in uno stesso punto, le variazioni di RSSI siano esagerate. È necessario quindi, applicare un filtro che addolcisca queste variazioni, e riesca a far ottenere valori vicini al valore reale dell'RSSI, si utilizza il filtro di Kalman.

Nel testo [26] viene utilizzato un chip Nordic nRF52 che supporta Bluetooth versione 5, che può lavorare sia come nodo periferico che come nodo centrale. Vengono posizionati dei dispositivi in posizioni fisse, che invieranno segnali di advertising. Sarà presente un nodo mobile che funzionerà in modalità scanner ed

estrarrà i valori di RSSI relativi ai nodi periferici. Il dispositivo centrale creerà un database in cui sono memorizzati l'ID del nodo periferico e il suo segnale RSSI ricevuto.

Per calcolare la sua posizione, il nodo centrale utilizzerà la trilaterazione, si serve delle distanze stimate tra lui stesso e 3 nodi fissi attraverso il modello di pathloss:

$$RSSI = RSSI_{d_0} - 10n \log_{10}(d/d_0) \quad (26)$$

Per avere una buona stima della distanza, bisogna migliorare la variabilità dei valori di RSSI attraverso il filtro di Kalman monodimensionale, utile quando si ha un segnale fortemente mutevole. L'alta variabilità è dovuta dall'interazione del segnale con oggetti e pareti interne.

Dopo il filtraggio, viene utilizzato il modello di pathloss per ricavare il fattore di pathloss ad una distanza nota e una volta individuato, viene utilizzato per il calcolo della distanza dal nodo centrale e i 3 fissi come avviene in equazione (24).

In questo articolo la stanza in esame è di dimensioni piccole, 5x5 ed i nodi periferici sono posizionati a 2m da terra, negli angoli della stanza. Viene stimato un "n" diverso per ogni nodo fisso. Il filtro di Kalman è stato applicato 50 volte per ogni posizione.

Nell'articolo [27] viene utilizzato un algoritmo di localizzazione "pesato", ciò significa che vengono introdotti dei pesi per la stima della distanza.

La posizione di un nodo di riferimento è la seguente:

$$P(\bar{x}, \bar{y}) = \frac{1}{N} \sum_{i=1}^N a_i(x_i, y_i) \quad (27)$$

N è il numero di nodi ancora, la posizione del nodo mobile può essere stimata utilizzando l'algoritmo WRL (Weighted Range Localization) in questo modo:

$$P'(\bar{x}, \bar{y}) = \frac{\sum_{i=1}^N w_i \cdot a_i(x_i, y_i)}{\sum_{i=1}^N w_i} \quad (28)$$

Dove:

$$w_i = \sum_{i=1}^N \frac{1}{d_i^g} \quad (29)$$

Il valore  $w_i$  è la distanza pesata tra riferimento e target, “g” è il grado che determina il contributo di ogni nodo ancora. La distanza stimata  $d_i$  può essere calcolata con l’equazione (16). Il valore di pathloss nel modello di pathloss della logdistanza non è accurato nella pratica, perciò viene proposto l’algoritmo RS-WRL (Relative Span WRL) per risolvere il problema del WRL.

Per l’algoritmo RS-WRL la forza del segnale ricevuto dai nodi beacon viene convertito in RSSI ed espresso come:

$$RSSI = 10 \log \frac{P_r}{P_{be}} \quad (30)$$

Dove  $P_r$  è la forza del segnale ricevuto dal nodo target,  $P_{be}$  è la potenza del beacon. L’algoritmo RS-WRL viene espresso così:

$$P''(\bar{x}, \bar{y}) = \frac{\sum_{i=1}^N (1 - \gamma)^{RSSI} \cdot a_i(x_i, y_i)}{\sum_{i=1}^N (1 - \gamma)^{RSSI}} \quad (31)$$

Dove “ $\gamma$ ” è il grado della ponderazione dell’algoritmo RS-WRL.

La stanza nella quale sono eseguiti gli esperimenti ha dimensioni 19.20 x 11.25, settando opportuni valori di “g” e di “ $\gamma$ ” si riesce ad avere un miglioramento rispetto l’applicazione classica di un algoritmo non pesato.



Nel testo [28] viene utilizzato il calcolo dell’AoA per la stima delle posizioni. È una tecnica molto vantaggiosa, in quanto permette di far ottenere il dato della posizione utilizzando le informazioni di solo due nodi di riferimento e non richiede la sincronizzazione tra tag mobile e ricevitori fissi.

Per la stima dell’AoA viene utilizzato l’algoritmo MUSIC (Multiple Signal Classification) che garantisce una buona risoluzione angolare e una buona stima anche a bassi livelli di SNR.

Le info riguardo l’AoA sono misurate in 2 modi differenti, il primo è Switched Beam System (SBS) che usa un numero fisso di beams per scansionare il piano azimutale e trovare la potenza ricevuta più alta o la forza di segnale maggiore. Il secondo modo è l’Adaptive Array System (AAS) che può guidare il beam in ogni direzione desiderata, settando dei pesi attraverso gli M elementi che formano l’array di antenne.

L’algoritmo MUSIC si basa sulla separazione dello spazio di osservazione in 2 sottospazi, uno sorgente e l’altro rumore. La matrice di covarianza di input viene decomposta in autovettori che formano una base per i sottospazi sorgente e rumore. Le forme d’onda ricevute dagli M elementi dell’array di antenna sono una combinazione lineare dei segnali dalle sorgenti S e rumore bianco additivo gaussiano (AWGN). Queste antenne sono separate da una distanza fissa “d”.

Il vettore ricevuto  $M \times 1$  è definito così:

$$x = A(\theta)s + n \quad (32)$$

Dove “s” è il vettore segnale  $S \times 1$  ed “n” è il vettore rumore  $M \times 1$ . Le i-esime colonne della matrice  $A(\theta)$  di dimensioni  $M \times S$ , sono conosciute come steering vectors e sono definite così:

$$\bar{a}(\theta_i) = [1, e^{\beta d \cos(\theta_i)}, \dots, e^{\beta(M-1)d \cos(\theta_i)}]^T \quad (33)$$

$\theta_i$  è l’angolo azimutale della sorgente “s” e varia tra -90 e +90.

$\beta$  invece è il numero d'onda. La funzione di auto-covarianza del segnale ricevuto è denotata con la matrice  $R_{xx}$  di dimensioni  $M \times M$ . Dopo la decomposizione in autovettori, può essere scritta così:

$$R_{XX} = U_s \Lambda_s U_s + U_n \Lambda_n U_n \quad (34)$$

Dove  $U_s$  e  $U_n$  sono i sottospazi di matrici unitarie del segnale e del rumore,  $\Lambda_s$  e  $\Lambda_n$  sono matrici diagonali di autovalori dei sottospazi segnale e rumore.

Lo spettro di potenza spaziale è:

$$P_{MUSIC}(\theta) = \frac{1}{A^H(\theta) U_n U_n^H A(\theta)} \quad (35)$$

Dove  $(.)^H$  indica l'operazione di matrice Hermitiana. Il picco dello spettro indica l'angolo di arrivo. L'accuracy di questo algoritmo dipende dal numero di elementi dell'array  $M$ , dal numero di segnali in arrivo " $S$ ", dalla spaziatura tra gli elementi d'antenna " $d$ " e dal numero di campioni (snapshot) usati per stimare la matrice di covarianza.

Gli esperimenti sono fatti in un'area di laboratorio 6 x 3 m. si assume che il beacon sia statico e le interferenze siano trascurabili. Viene quindi, rilevata la posizione del beacon usando le posizioni note dei dispositivi di riferimento, stimando l'AoA in corrispondenza di ognuno di essi.

Prima di procedere con la misurazione, viene fatta una calibrazione di fase e applicata all'USRP (Universal Software Radio Peripheral). Questa calibrazione definisce le direzioni di riferimento.

Inoltre, per calcolare il Root Mean Square Errore (RMSE) degli angoli predefiniti per una scelta dell'SNR, l'angolo predefinito deve essere prima calibrato a un alto valore di SNR vicino al punto iniziale ipotizzato.

In [29] viene proposto un algoritmo di localizzazione che utilizza tecniche di localizzazione basate su RSSI con fingerprinting e una tecnica chiamata CoO (Cell of Origin).

Nel sistema di posizionamento, i sensori sanno in quale cella essi appartengono ed ogni cella ha una sua area di copertura che non si sovrappone all'area di copertura di un'altra cella. Quando il dispositivo target entra all'interno di una cella, si registrerà la sua posizione come posizione del ricevitore che è al centro della cella. Se il valore di RSSI è inferiore ad una soglia prefissata, il sistema utilizzerà quel valore per il fingerprint, per il calcolo della posizione, altrimenti viene utilizzata la modalità CoO.

Infine, prima di calcolare la posizione del target, viene applicato il filtro di Kalman.

In [30] viene proposto un algoritmo di IPS che ha l'obiettivo di effettuare il tracking di dispositivi in scenario indoor usando BLE.

Nel sistema vengono piazzati  $L$  ricevitori in posizioni fisse che hanno moduli BLE integrati, i trasmettitori saranno beacons mobili.

Per quanto riguarda i ricevitori, sono necessari almeno 3 misurazioni per applicare la trilaterazione, quindi 3 ricevitori per ogni stanza.

L'obiettivo dell'articolo è di realizzare un sistema pienamente funzionante low cost e con errore minimo, definito come distanza euclidea dalla stima della posizione  $p_e$  e la posizione reale  $p_r$ :

$$e = \sqrt{(p_{rx} - p_{ex})^2 + (p_{ry} - p_{ey})^2} \quad (36)$$

Per migliorare i risultati vengono proposti l'uso di frequency channel diversity, un algoritmo pesato basato sul metodo di trilaterazione e filtro di Kalman.

Vengono utilizzati trasmettitori beacon e 3 ricevitori (Raspberry Pi) con 3 sniffers integrati, in ascolto sui canali di advertising del BLE (37,38,39). Ogni sniffer è programmato per processare un solo canale di advertising. Viene implementato un

server che riceve le distanze calcolate da ogni ricevitore e stima con gli algoritmi proposti la posizione del beacon BLE.

Ci saranno delle variazioni del valore RSSI, che dipendono dalla frequenza dei canali usata. I messaggi trasmessi nello stesso beacon interval (uno per ogni canale) hanno lo stesso counter ID quindi il ricevitore può identificarli per applicare la channel diversity di conseguenza. Ogni trasmettitore ha un indirizzo MAC unico usato per differenziare i messaggi da diversi trasmettitori.

Il beacon viene programmato per trasmettere segnali di advertising ogni 100 ms alla potenza massima di 5 dBm. In questo caso si rileva anche se il dispositivo si sta muovendo o no. Se il dispositivo non si muove, cambierà l'intervallo di advertising del beacon a 5 s invece che 100 ms, per il battery saving.

I canali di advertising sono 37,38,39, usati dai beacons per trasmettere, il ricevitore controlla l'RSSI in ogni diverso canale e applica uno schema di combinazione che vedremo dopo, per ottenere i risultati migliori, traendo vantaggio dalla diversità del canale per migliorare le performances del sistema.

Ogni pacchetto di advertisement sono identificati dal MAC del beacon e dal counter ID per effettuare la channel diversity.

I moduli sniffers ricevono i diversi frames e ogni Raspberry estrae i frames individuati e li inserisce in una matrice circolare per ogni trasmettitore identificato.

**TABELLA 13: MATRICE CIRCOLARE**

<b>Counter ID</b>	<b>Channel 37</b>	<b>Channel 38</b>	<b>Channel 39</b>
1	RSSI <sub>37</sub>	RSSI <sub>38</sub>	RSSI <sub>39</sub>
2	RSSI <sub>37</sub>	RSSI <sub>38</sub>	RSSI <sub>39</sub>
...	...	...	...
N	RSSI <sub>37</sub>	RSSI <sub>38</sub>	RSSI <sub>39</sub>

Questa è la matrice di un ricevitore per uno specifico trasmettitore. Ogni valore di RSSI di un canale in ogni riga, corrisponde a un certo counter ID, quindi si può applicare la diversità di canale. Può accadere che per errori di trasmissioni le righe

non siano tutte complete, ad esempio, ho solo l’RSSI del canale 37 e degli altri due no.

Nel paper si usa la diversità del canale come modo per incrementare le performances. Si potrà selezionare casualmente oppure usando un certo schema, uno dei canali di advertisement, ed usare quello scelto come riferimento. L’idea del paper è di sfruttare tutte le informazioni che si hanno sui canali e combinarle in uno dei seguenti modi:

- Selezionare il canale che mostra il valore di RSSI più alto, verrà considerato quel canale come il migliore e si prede il suo valore di RSSI per i calcoli:

$$RSSI_{max} = \max (RSSI_{ch\ 37}, RSSI_{ch\ 38}, RSSI_{ch\ 39}) \quad (37)$$

- Prendere la media degli RSSI di tutti e 3 i canali:

$$RSSI_{average} = \frac{1}{3} \sum_{i=37}^{39} RSSI_{ch\ i} \quad (38)$$

- Ottenere il valore di RSSI dall’algoritmo Maximum Ratio Combining (MRC). Con questo approccio viene dato un peso a un canale in modo diverso, viene comunque preso in considerazione il canale con RSSI più alto, poiché è il più fidato, ma si tengono in considerazione anche i valori più piccoli per il calcolo dell’RSSI finale.  $RSSI_{min}$  viene scelto a seconda di quale è la sensibilità degli sniffer di canale:

$$RSSI_{MRC} = \sum_{j=37}^{39} \frac{RSSI_j - RSSI_{min}}{\sum_{i=37}^{39} RSSI_i} RSSI_j \quad (39)$$

Una volta scelto il metodo ottimo di misurazione RSSI usando la diversità di canale, bisogna calcolare la distanza tra trasmettitore e ricevitore. Nel paper sono stati selezionati 3 modelli di propagazione e viene analizzato il più accurato. Viene usato il modello di pathloss basato sulla log-distanza con shadowing, valido per distanze  $d > d_0$ , in cui “ $d$ ” è la distanza da trovare e  $d_0$  è di riferimento:

$$RSSI = RSSI(d_0) + 10n \log\left(\frac{d}{d_0}\right) + X_\sigma \quad (40)$$

$RSSI(d_0)$  è l’RSSI alla distanza di riferimento  $d_0 = 0.8 \text{ m}$  (calcolata con il modello di propagazione in free space), “ $n$ ” è l’esponente di pathloss e  $X_\sigma$  è una variabile casuale che indica una distribuzione Gaussiana a media 0 e deviazione standard che tenta di compensare gli effetti randomici di shadowing.

Un altro modello è quello dato dall’ International Telecommunication Union (ITU) indoor per shadowing:

$$RSSI = 20 \log f + N \log(d) + P_f(n) - 28 \quad (41)$$

Dove “ $f$ ” è la frequenza in MHz, “ $N$ ” è il coefficiente di perdita di potenza per la distanza,  $P_f(n)$  è il coefficiente di penetrazione, questi ultimi 2 sono stati scelti guardando gli scenari e le raccomandazioni dell’ITU.

Il terzo modello è uno empirico:

$$RSSI = 10n \log(d) + A \quad (42)$$

Dove  $A$  è il valore empirico dell’RSSI misurato a 1m di distanza considerando lo scenario LoS (è un valore di riferimento), “ $n$ ” è l’esponente di pathloss. Viene considerato questo modello perché non ha una caratterizzazione spinta e fornisce un livello di performances di riferimento. Assumono che “ $A$ ” rimanga quasi costante, perché si assume che ricevitore e trasmettitore siano vicini e le condizioni sfavorevoli non agiscano a una distanza così piccola.

La trilaterazione classica non è sempre applicabile con precisione, poiché potrebbero esserci casi in cui non si intersecano alla perfezione le 3 distanze stimate, ma si ha un'area nella quale può giacere il beacon.

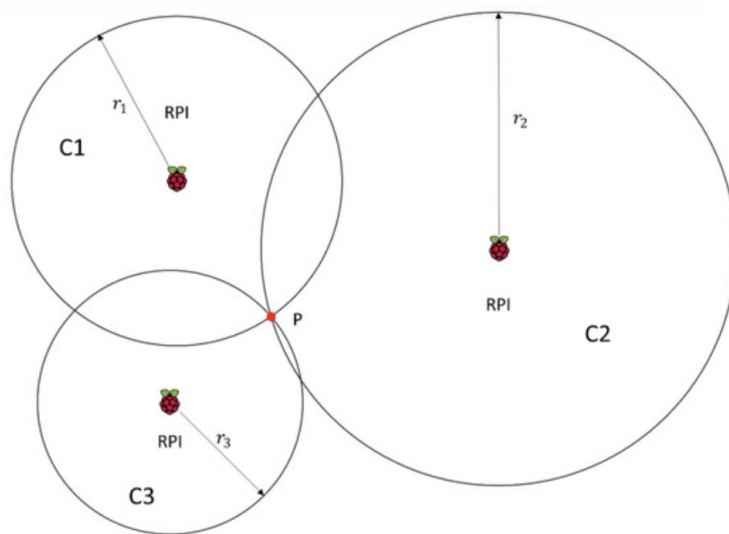
Nel paper viene presentato un metodo che calcola la posizione che dà maggior importanza ai valori ottenuti dai dispositivi che si troverebbero più vicino al beacon, chiamata trilaterazione pesata.

Si possono usare  $L$  ricevitori con  $L \geq 3$ , considerano però, solo i 3 ricevitori che calcolano una distanza tra trasmettitore e ricevitore più piccola. L'utilizzo di più di 3 ricevitori aumenterà l'accuracy del sistema.

Date 3 diverse misure di distanze  $r_1, r_2, r_3$  dai ricevitori  $R1, R2, R3$  al trasmettitore  $S$ . Vengono calcolati i pesi associati a coppie tra i ricevitori  $R1, R2, R3$ :

$$\begin{cases} w_{ab} = \frac{r_a}{r_b} & \text{se } r_a < r_b \\ w_{ba} = \frac{r_b}{r_a} & \text{se } r_b < r_a \end{cases} \quad \text{con } a = 1,2,3; \quad b = 1,2,3 \quad (42)$$

Una volta ottenuti i pesi, si procede con la trilaterazione, il caso ideale mostra che i cerchi si intersecano in un singolo punto:



**FIGURA 33: CASO IDEALE DI TRILATERAZIONE**

Per questi 3 cerchi si hanno 3 equazioni:

$$\begin{cases} r_1^2 = (x - x_1)^2 + (y - y_1)^2 \\ r_2^2 = (x - x_2)^2 + (y - y_2)^2 \\ r_3^2 = (x - x_3)^2 + (y - y_3)^2 \end{cases} \quad (43)$$

I centri delle circonferenze  $(x_j, y_j)$ . Nel caso in cui si hanno  $L$  ricevitori, si avranno  $L$  equazioni e da queste scelgo le 3 che presentano i valori dei raggi  $r_j$  più piccoli, perché indicano una minor distanza tra trasmettitore e ricevitore. Posso ricavare i valori della posizione del beacon:

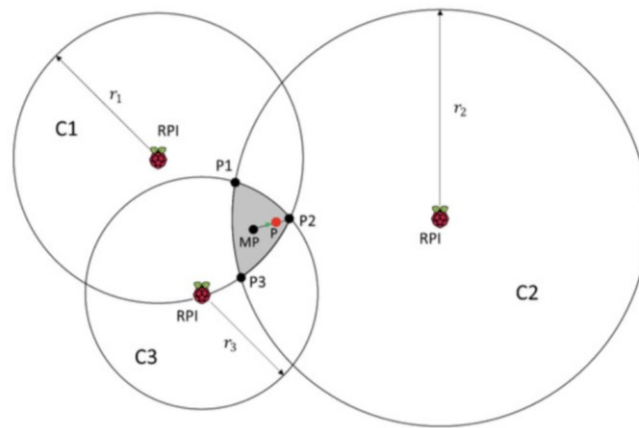
$$x = \frac{\begin{vmatrix} (r_1^2 - r_2^2) - (x_1^2 - x_2^2) - (y_1^2 - y_2^2) & 2(y_2 - y_1) \\ (r_1^2 - r_3^2) - (x_1^2 - x_3^2) - (y_1^2 - y_3^2) & 2(y_3 - y_1) \end{vmatrix}}{\begin{vmatrix} 2(x_2 - x_1) & 2(y_2 - y_1) \\ 2(x_3 - x_1) & 2(y_3 - y_1) \end{vmatrix}} \quad (44)$$

$$y = \frac{\begin{vmatrix} 2(y_2 - y_1) & (r_1^2 - r_2^2) - (x_1^2 - x_2^2) - (y_1^2 - y_2^2) \\ 2(y_3 - y_1) & (r_1^2 - r_3^2) - (x_1^2 - x_3^2) - (y_1^2 - y_3^2) \end{vmatrix}}{\begin{vmatrix} 2(x_2 - x_1) & 2(y_2 - y_1) \\ 2(x_3 - x_1) & 2(y_3 - y_1) \end{vmatrix}} \quad (45)$$

Nel caso in cui i 3 cerchi si intersecano in un unico punto, non c'è bisogno di un algoritmo pesato, basta svolgere semplici calcoli.

Se invece i cerchi che si intersecano non formano un punto, ma c'è un'area di intersezione:





**FIGURA 34: CASO REALE DI TRILATERAZIONE**

Per minimizzare questo errore, l'area viene approssimata a quella di un triangolo formato dai vertici  $P1$ ,  $P2$ ,  $P3$ :

$$P_x = \frac{P1_x + P2_x + P3_x}{3} \quad (46)$$

$$P_y = \frac{P1_y + P2_y + P3_y}{3} \quad (47)$$

Poi verrà fatto un perfezionamento basato sui pesi. Viene prima calcolato un punto di mezzo, detto  $MP$ , poi viene preso il punto di intersezione relativo ai ricevitori più vicini al beacon, ad esempio è dato dall'intersezione dei cerchi  $C2$  e  $C3$  al punto  $P2$ . Poi andiamo da  $MP$  a  $P2$ , la distanza tra essi, moltiplicata per il peso calcolato usando le distanze del ricevitore più vicino (RPI in cerchio  $C3$ ) e l'altro (RPI in cerchio  $C2$ ). Consideriamo la distanza  $r_3$  di  $C3$  invece della distanza  $r_1$  di  $C1$  perché sebbene entrambi si intersecano in  $P2$ ,  $C3$  ha un raggio più piccolo e quindi è più affidabile:

$$w_{32} = \frac{r_3}{r_2} \quad (48)$$

$$\begin{cases} P_x = P_x + (1 - w_{32}) \cdot d \cdot \cos(\theta) \\ P_y = P_y + (1 - w_{32}) \cdot d \cdot \sin(\theta) \end{cases} \quad (49)$$

$\theta$  è l'angolo della linea tra i punti e l'asse x e “ $d$ ” è la distanza tra  $MP$  e  $P2$ .

Quando il raggio degli altri ricevitori va a infinito, ma comunque interseca, il peso è 0 e viene scelto  $P2$  come punto più probabile. Quando stimiamo la stessa distanza dal beacon a tutti i ricevitori, il peso diventa 1 e verrà scelto il punto medio come posizione stimata.

Con questo metodo si tiene conto dell'informazione data da tutti i ricevitori, ma saranno più affidabili quelli più vicini al beacon.

Una volta stimata la posizione con l'algoritmo di localizzazione pesato, verrà usato il Filtro di Kalman per migliorare i calcoli della posizione. Viene implementato un filtro del secondo ordine per fare tracciare la posizione, la velocità e l'accelerazione negli assi x e y.

La scelta dei parametri iniziale non è un fattore critico perché il KF si adatta ai valori nel tempo.

#### 4.2 Articoli UWB

In [31] vengono utilizzati approcci basati sul TDMA che permette di definire una mappa di slots temporali, in modo da organizzare la comunicazione tra i dispositivi. Questo protocollo utilizza comunicazioni bidirezionali, che prima di tutto permettono di determinare la distanza tra due o più dispositivi UWB, usando l'approccio Two-Way Time-of-Flight (TW-ToF). Questo approccio sfrutta i molteplici scambi di informazione tra i nodi ed essi non hanno bisogno di essere sincronizzati temporalmente tra loro.

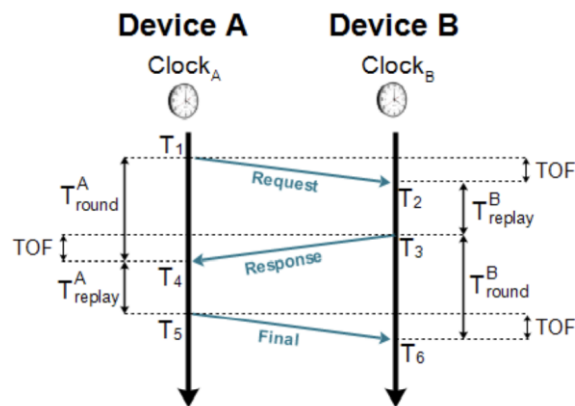


FIGURA 35: RAPPRESENTAZIONE DEL TW-TOF

La seguente formula si chiama “Symmetric double-sided two-way ranging” (SDS-TWR):

$$TOF_{SDS} = \frac{(T_{round}^A - T_{replay}^A) + (T_{round}^B - T_{replay}^B)}{4} \quad (50)$$

Essa si compone di 3 messaggi per determinare il tempo di volo (ToF) tra il dispositivo A e il dispositivo B, che sono Request, Response, Final.

Nella formula:

- $T_{round}^A$ :  $T4 - T1$ ;
- $T_{round}^B$ :  $T6 - T3$ ;
- $T_{replay}^A$ :  $T5 - T4$ ;
- $T_{replay}^B$ :  $T3 - T2$ .

In cui i tempi sono:

- **T1**: invio del segnale di Request da parte di A;
- **T2**: ricezione del segnale di Request da parte di B;
- **T3**: invio del segnale di Response da parte di B;
- **T4**: ricezione del segnale di response da parte di A;
- **T5**: invio del segnale di Final da parte di A;

- **T6:** ricezione del segnale di Final da parte di B.

Moltiplicando il ToF per la velocità della luce, approssimata a  $2.99792458 * 10^8$ , si ottiene l'informazione della stima sul range.

Se assumiamo frequenze di drift fissa  $e_A$  ed  $e_B$ , riferite ai clock dei due dispositivi, l'errore dovuto a questi drift (o scostamenti) è dato da:

$$\widehat{TOF}_{SDS} - TOF_{SDS} = \frac{TOF_{SDS}}{2}(e_A + e_B) + \frac{(T_{replay}^B - T_{replay}^A)}{4}(e_A - e_B) \quad (51)$$

Se  $TOF_{SDS}$  è molto minore rispetto la differenza tra i due tempi di risposta, il secondo termine dell'equazione predomina il primo termine. Più piccola è la differenza tra i due tempi di risposta e più piccolo sarà l'errore nella stima del ToF. I dati di ranging vengono forniti come input per l'algoritmo di posizionamento che si basa su un approccio ai minimi quadrati non lineare, durante un breve periodo di inizializzazione. In seguito, un filtro di Kalman esteso che include un modello di movimento viene utilizzato per determinare la posizione target.

In questo articolo [32] viene utilizzato un sistema basato sul TDoA. Viene utilizzato un hardware customizzato, che dispone di un'antenna UWB con 4 canali. Il luogo è un laboratorio 7 m x 10 m ed alto 3,5 m, tutti i muri sono di metallo, ci sono anche prototipi industriali nella stanza, quindi, può definirsi un piccolo ambiente industriale.

La marcatura temporale  $t_i$  di un segnale ricevuto dal modulo "i", può essere verificata confrontandola con quella di altri moduli.

Una tecnica utilizza le distanze  $d_{i,j}$  tra due antenne e compara questa distanza al time-stamp differenza assoluto:

$$|t_i - t_j| \leq \frac{d_{i,j}}{c} \pm \eta \quad i \neq j; \quad i, j \in [1, 2, \dots, N] \quad (52)$$

In questo paper il numero dei moduli è  $N=4$ , gli indici  $i,j$  indicano il numero del modulo “ $c$ ” è la velocità della luce. La costante  $\eta$  rappresenta il rumore di misura. Poi viene calcolato il valore di timestamp medio  $t_l$ :

$$t_l = \frac{1}{N} \sum_{i=1}^N t_i \quad l \in [1, 2, \dots, M] \quad (53)$$

Questo viene fatto per ognuno degli “ $M$ ” dispositivi fissi e per ogni segnale ricevuto.

ToA necessita di una sincronizzazione wireless, i timers locali di ogni ancora misureranno il ToA. La Central Time Unit (CTU) invia segnali di sincronizzazione ogni  $T= 200$  ms. Una base dei tempi globale viene stabilita collegando i time stamps locali con i messaggi di sincronizzazione globali.

In questo modo le distanze  $\hat{d}_l$ , tra CTU e ogni ancora, sono usate per compensare l’offset del time of flight  $\hat{t}_l$  che è costante nel tempo:

$$\hat{t}_l = \frac{\hat{d}_l}{c} \quad l \in [1, 2, \dots, M] \quad (54)$$

L’accuratezza della base temporale dipende dell’oscillatore cristallino usato del chip UWB. Ogni cristallo ha un’offset di frequenza unico. Questo effetto e la stabilità della frequenza sono compensati usando un fattore di correzione lineare  $v_{l,u}$ :

$$v_{l,u-1} = \frac{T}{\check{t}_{l,u} - \check{t}_{l,u-1}} \quad (55)$$

Dove  $\check{t}_{l,u}$  sono i tempi di sincronizzazione ricevuti all’ancora “ $l$ ” per indice di trama di sincronizzazione “ $u$ ”.

Il time stamp  $t_l$  viene corretto usando  $v_{l,u-1}$  e l'offset di sincronizzazione  $\hat{t}_l$  viene rimosso. Il vettore di time of arrival risultante  $\mathbf{t}_v$  per ogni trama di localizzazione “ $v$ ” viene calcolato così:

$$\mathbf{t}_v = [\tau_{1,v}, \tau_{l,v}, \dots, \tau_{m,v}] \quad \tau_{l,v} = t_{1,v} \cdot v_{l,u} + \hat{t}_l \quad (56)$$

Poi viene calcolato il vettore time difference of arrival TDoA  $\mathbf{t}_v$ , sottraendo il minimo valore di  $\mathbf{t}_v$  a esso:

$$\hat{\mathbf{t}}_v = \mathbf{t}_v - \min(\mathbf{t}_v) \quad (57)$$

La posizione del target in uno spazio multidimensionale può essere calcolata con l'algoritmo di Chan illustrato in [33].

Nel caso di posizioni ottenute non uniche, viene scelta la soluzione che ha la minima distanza rispetto l'ultima posizione nota.

## 5 Progetto: Conteggio pezzi e localizzazione

Il presente lavoro di tesi, inquadrandosi nel settore dell'IIoT, ha riguardato lo sviluppo di due applicazioni di interesse per un contesto industriale. In primo luogo, è stato affrontato il servizio del conteggio e check delle unità di produzione durante un tipico cambio formato industriale, in secondo luogo è stato trattato il servizio della localizzazione indoor. Di seguito vengono riportati i due obiettivi principali del presente lavoro:

- Realizzazione ed implementazione di un'applicazione per il conteggio oggetti.

- Implementazione e testing di un sistema di localizzazione di cose e persone.

Tutte e due le applicazioni funzioneranno in contesto industriale, all'interno di un reparto produttivo, ed entrambe si baseranno sulla stessa architettura di rete.

Nel primo punto viene realizzato un sistema di conteggio pezzi e testato nei pressi della linea di test dove sono stati eseguiti gli esperimenti.

Per il secondo punto, viene testato un sistema di localizzazione commerciale che verrà confrontato con un altro algoritmo realizzato sperimentalmente e già testato presso il Dipartimento di Ingegneria dell'Informazione dell'Università Politecnica delle Marche. Questa tesi servirà a gettare le basi per un possibile confronto tra i due algoritmi, per provare quale dei due restituisce un livello di accuratezza migliore.

### 5.1 Attività di cambio formato e tipologie di oggetti da tracciare

Lo scenario analizzato è il capannone industriale del Fem-Care del “Pescara Plant” della società Fater S.P.A. di Pescara. Si tratta di un luogo dove vengono prodotti articoli di vario genere, relativi ai beni di consumo per la cura personale, come assorbenti intimi, salviette, ecc.

All'interno del reparto sono presenti un gran numero di linee di produzione, nelle quali avviene la realizzazione del prodotto, a partire dalle materie prime.

Una linea di produzione è sostanzialmente divisa in 3 aree:

- **Converter:** ne fanno parte alcuni componenti meccanici ed elettronici che trattano le materie prime, le lavorano e infine realizzano il prodotto finito;
- **Imbustatrice:** i prodotti finiti vengono raggruppati per essere imbustati e realizzare le confezioni;
- **Inscatolatrice:** le confezioni saranno disposte all'interno di scatole, pronte per essere trasferite al magazzino merci.

Un'operazione delicata del processo produttivo è quella del cambio formato, conosciuto anche con il suo nome in inglese "Changeover". Con questa attività si intende che da un articolo di un certo formato, la linea di produzione debba essere riconfigurata per produrre un altro articolo di formato diverso.

La riconfigurazione della linea prevede la sostituzione di alcuni pezzi che servono a generare prodotti differenti. Il cambio formato avviene sempre a linea ferma, rispettando dei tempi di stop programmati.

Esistono 3 tipi di cambio formato:

- **Cambio Count:** da un articolo all'altro varia solo il numero di prodotti che vengono inseriti all'interno delle confezioni;
- **Cambio Tier:** da un tipo di articolo si passa ad un altro tipo di articolo;
- **Cambio Size:** da una taglia di un articolo si passa ad un'altra taglia dello stesso articolo.

L'attività del cambio formato viene organizzata preventivamente ed è prevista dal piano di produzione, un documento nel quale vengono fissate tutte le attività da compiere sulla linea e le quantità prodotte di un certo articolo, per 3 turni lavorativi e per la linea di interesse.



**TABELLA 14: ESEMPIO DI PIANO DI PRODUZIONE**

<b>Giorno x</b>	<b>Turno 1</b>	<b>Turno 2</b>	<b>Turno 3</b>
<b>Linea 1</b>	Cambio count da art. 111 ad art. 124 (ore 8.00) Pulizia (ore 12.00)		
<b>Linea 2</b>	Produzione art. 123 (tutto il turno)	Cambio formato da art. 123 ad art. 133 (ore 15.20)	
<b>Linea 3</b>	Produzione art. 96 (tutto il turno)	Cambio tier da art. 96 ad art. 45 (ore 15.20)	

Gli operai della linea eseguono questo lavoro con l'aiuto di un software che mostra una lista di attività da completare e dunque segnala il loro stato di avanzamento.

L'esecuzione del cambio formato deve essere completata rispettando i tempi nel piano di produzione, dunque, un ritardo che avverrebbe durante questa attività, si traduce come una perdita nella produzione giornaliera.

Per rendere il cambio formato veloce e snello, mezz'ora prima che esso venga effettuato, gli operai predispongono in prossimità della linea tutti gli oggetti che devono essere sostituiti per realizzare un altro prodotto, è la fase di pre-work.

Può succedere che in questa fase, alcuni di questi oggetti non si trovino nelle prossimità della linea nei tempi prestabiliti, per tale motivo, è utile per gli operai conoscere la posizione dei pezzi e di tenerne traccia in caso di smarrimento.

Un ritardo nell'operazione di cambio formato si ripercuoterà sul piano di produzione e di conseguenza sulla produttività di quella linea, poiché riprenderà a funzionare in ritardo.

Per quanto riguarda il cambio count, nella linea di produzione basta sostituire delle parti meccaniche dell'inscatolatrice e dell'imbustatrice, invece per eseguire un cambio size e cambio tier, bisogna sostituire elementi dell'inscatolatrice, imbustatrice e converter.

## 5.2 Oggetti del cambio formato

Per via delle differenze delle dimensioni degli oggetti utilizzati nel cambio formato, è stata fatta una prima distinzione, sono stati divisi in due gruppi:

- **Minuteria:** comprende tutti quei pezzi per il cambio formato di piccole dimensioni, che verranno sostituiti nell'inscatolatrice e nell'imbustatrice;
- **Unità di produzione:** comprende tutti quei pezzi per il cambio formato di grandi dimensioni, che verranno sostituiti nel converter.

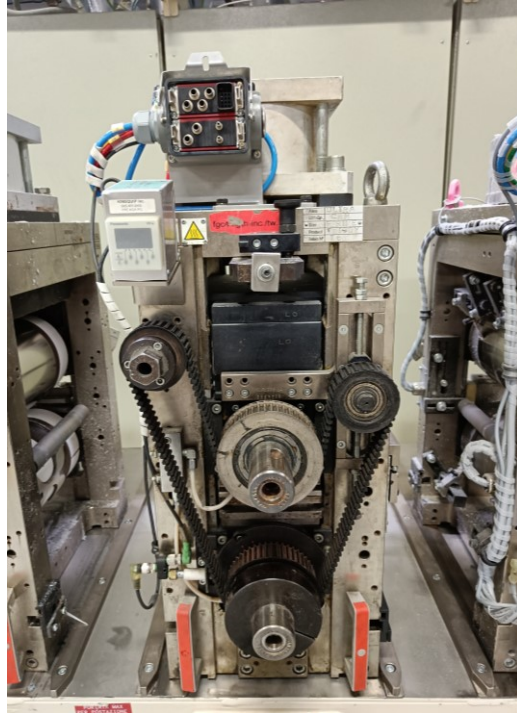
Molti di questi oggetti del gruppo “Minuteria” hanno dimensioni tali da rendere difficile l'applicazione di un tag per il tracciamento. Non è l'unico problema, infatti alcuni di questi pezzi entrano a contatto diretto con il prodotto finito e l'applicazione di un tag su di essi può alterarne la qualità.

Per via delle complicazioni appena descritte è stato deciso di effettuare la localizzazione e il conteggio pezzi soltanto per il gruppo “Unità di produzione”, in quanto hanno dimensioni fisiche maggiori ed alcune parti che le compongono non entrano a contatto diretto col semilavorato. Per tenere traccia di queste unità di produzione e quindi per rilevarle nel sistema di localizzazione, viene applicato un tag attivo sul loro telaio.

### 5.2.1 Unità di produzione

Le unità di produzione appartengono tutte all'area del converter, ad ogni cambio size esse saranno disinserite dai loro slot nella linea e sostituite con altre.

Esse hanno dimensioni medio-grandi, sono composte al loro interno da rulli, coltelli e/o parti saldanti, a seconda della loro funzione ed un telaio sul quale è possibile associare un tag di piccole dimensioni.



**FIGURA 36: ESEMPIO DI UNITÀ DI PRODUZIONE 1**



**FIGURA 37: ESEMPIO DI UNITÀ DI PRODUZIONE 2**

C'è una categorizzazione tra le unità di produzione, esse vengono identificate in modo unico con 3 dati, cioè dal loro modello, dalla size del prodotto e dal codice del telaio:

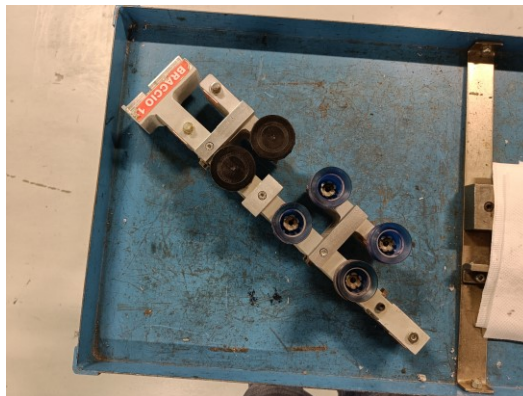
- **Modello:** sono delle categorie di unità, indica quindi, dei gruppi di unità che hanno le stesse funzionalità;
- **Size:** indica qual è la taglia dell'articolo che l'unità produce;
- **Codice del telaio:** è un identificativo di una unità di un certo modello, indica quale è il telaio che forma la struttura dell'intera unità di produzione.

Esempio di nome di un'unità di produzione, Final Knife S3 T1:

- **Modello:** Final Knife;
- **Size:** S3;
- **Numero telaio:** T1.

### 5.2.2 Minuteria

Quando si deve svolgere uno qualunque dei 3 tipi di cambio formato, gli operai devono sostituire alcuni pezzi all'interno dell'inscatolatrice e dell'imbustatrice. Questi pezzi sono molto differenti l'uno dall'altro, sia per le dimensioni che per la forma e solitamente sono di piccole dimensioni, rispetto le unità di produzione, come quelli raffigurati:



**FIGURA 38: ESEMPIO DI MINUTERIA 1**



**FIGURA 39: ESEMPIO DI MINUTERIA 2**

Il loro numero è molto elevato, più di un centinaio per linea produttiva e sono riposti all'interno di armadi metallici. Al momento del cambio formato, i pezzi che dovranno essere sostituiti, nella fase di pre-work, vengono poggiati sopra dei carrelli mobili, che per comodità sono avvicinati alle parti della linea di interesse.

### 5.3 Tecnologia utilizzata

Dopo uno studio dello stato dell'arte, considerando i pro e i contro degli IPS in contesti industriali, la tecnologia utilizzata è il Bluetooth, nella sua versione Low Energy (BLE). Alcuni dei più importanti motivi della scelta del BLE:

- **Costi implementativi bassi:** sia i gateway che i beacon Bluetooth hanno un costo più o meno basso, a seconda del produttore, rispetto agli altri IPS;
- **Semplicità dei dispositivi:** secondo lo standard del BLE, i chip all'interno dei beacons sono molto semplici, poiché svolgono soltanto la funzione di broadcast del segnale. I gateways saranno elettronicamente più completi, predisporranno di un modulo Bluetooth per effettuare lo scanning dei pacchetti ed un modulo WiFi che verrà utilizzato per aggregare i dati ricevuti dai beacons in Cloud o in servers locali;
- **Consumo energetico:** sia i gateways che i beacons sono dispositivi che operano a bassa potenza. I beacons hanno una potenza trasmittiva che tipicamente va da -100 dBm a 4 dBm, alimentati a batteria. La durata di

vita dei beacons dipende dai parametri di trasmissione impostati e dal modello e tipo della batteria. Lo standard BLE permette di trasmettere segnali a potenza minima;

- **Dimensioni piccole dei tag:** i beacon sono dispositivi alimentati da batteria, progettati con lo scopo di avere dimensioni ridotte. La loro dimensione dipende soprattutto dal tipo di circuito della board elettronica e dal tipo di batteria. Ad esempio, un beacon che ha un'alimentazione con batteria a bottone può avere dimensioni di poche unità di centimetri;
- **Interoperabilità con il WiFi:** il Bluetooth lavora alle stesse frequenze del WiFi nella banda libera dei 2,4 GHz ma non genera interferenze con esso. Inoltre, è molto facile trovare in commercio dei dispositivi, come ad esempio degli access point, che integrino entrambe le tecnologie WiFi e Bluetooth Low Energy.

Ciò che si vuole ottenere è un sistema che restituisca una stima della posizione di un'unità di produzione con un errore tollerabile, per questa applicazione non è necessario ottenere un errore del livello del centimetro.

La stessa tecnologia viene utilizzata per effettuare il conteggio dei pezzi al momento del cambio formato.

#### 5.4 Database per cambio formato

È stato realizzato un database su MySQL contenente le informazioni maggiormente importanti riguardo il cambio formato. In special modo al suo interno sono presenti i dati delle unità di produzione, dei tag bluetooth e di tutti gli articoli che la linea di produzione di test realizza.

Segue una descrizione dettagliata delle tabelle del database.

## Tabella “lista\_unità”

**TABELLA 15: TABELLA "LISTA\_UNITA"**

	ID_Unita	Numero_telaio	ID_modello_unita	Denominazione_modello	Nome_unita
▶	1	4	1001	OPT CUT&SLIP	OPT C&S S3 LW
	2	3	1001	OPT CUT&SLIP	OPT C&S S3 LW
	3	21	1001	OPT CUT&SLIP	OPT C&S S3 LW
	4	C8	1002	STS C&L	STS C&L LW
	5	10	1003	STS C&L	STS C&L Seta GEN1X
	6	42	1004	TAGLIO FINALE	FK S3 SW
	7	4	1005	TAGLIO FINALE	FK S3 LW
	8	T3	1006	TAGLIO FINALE	FK TWIGGY
	9	F8	1007	FUSION BOND	FB S3 Petalo-Idea
	10	5	1008	FUSION BOND	FB S3 Seta GEN1X
	11	143	1009	SALDANTE	CRM S3 SW

Sono state censite all'interno di questo file tutte le unità di produzione che si utilizzano nella linea di test FGC2, per avere una lista totale e ordinata di tutte le unità:

- **ID\_unita**: numero incrementale che identifica in modo unico un'unità;
- **Numero\_telaio**: il numero del telaio che compone un'unità;
- **ID\_modello\_unita**: un codice assegnato al tipo di modello dell'unità;
- **Denominazione\_modello**: il nome del modello dell'unità;
- **Nome\_unita**: il nome completo di un'unità, formato dal nome del modello, il tipo di size e il tipo di prodotto che essa produce, come spiegato nel sotto-capitolo “oggetti del cambio formato”.

## Tabella “prodotti”

**TABELLA 16: TABELLA "PRODOTTI"**

	ID_prodotto	Cod_prodotto	Nome_prodotto
▶	1	2740498	INTERVALLO LADY PLUS MAXI LONG X28
	2	2740499	INTERVALLO LADY PLUS MAXI LONG x34
	3	2740536	LINES PETALO ULTRA LUNGO ALI x10
	4	2740540	LINES PETALO ULTRA LUNGO ALI x20
	5	2740543	IDEA ULTRA NOTTE ALI x10
	6	2740547	LINES IDEA ULTRA DWCT NOTTE ALI x 8
	7	2740550	LINES IDEA ULTRA DUO DWCT NOTTE x16
	8	2740554	Lines Cotone BIO Ultra Notte x8+2
	9	2740558	LINES SETA ULTRA LUNGO ALI x11

Nello schema mostrato, sono state salvate le informazioni più importanti riguardanti i prodotti o articoli:

- **ID\_prodotto**: numero incrementale che indica un singolo prodotto;
- **Cod\_prodotto**: il codice di un prodotto secondo la categorizzazione nei database aziendali di Fater;
- **Nome\_prodotto**: il nominativo corrispondente a un certo codice prodotto.

## Tabelle “prodotto”

Sono state realizzate 18 tabelle, ognuna relativa ad uno specifico prodotto. Il loro nome è composto da “prodotto” più il numero dell’”ID\_prodotto”, ad esempio prodotto1, prodotto2, ecc.

Come esempio viene illustrata la tabella “prodotto1”:

**TABELLA 17: TABELLA PRODOTTO 1**

	ID_prodotto1	ID_unita	unita	mac_address	presente
▶	1	14	FK TWIGGY T3	AC233FA27B5B	no
	2	19	CC&S TWIGGY 1	AC233FA27B5C	no
	3	26	PERIMETRAL CRM T6	AC233F58A67F	no
	4	18	KPC TWIGGY T2	AC233F58A589	no
	5	43	VISUAL CRM T5	AC233FE6470F	no



- **ID\_prodotto1**: numero incrementale;
- **ID\_unita**: è l'identificativo di una unità, relativo ai dati della tabella "lista-unità";
- **Unita**: è il nome dell'unità costituito da alcuni dati della tabella "lista-unità"
- **Mac\_address**: il mac address del beacon che è stato associato ad una certa unità;
- **Presente**: un campo che assume solo i valori "si" e "no" ed indica la presenza di un'unità sul posto al momento del conteggio.

## 5.5 Primo caso d'uso: Conteggio pezzi

Per eseguire al meglio il controllo dei pezzi del cambio formato, è stato deciso di implementare la funzione di conteggio pezzi, che restituirà un feedback riguardo al numero di pezzi presenti nelle vicinanze e il numero di pezzi mancanti.

Viene predisposto un gateway WiFi-Bluetooth in prossimità della linea con la funzionalità di Scanner BLE:

- **Scan interval**: 100 ms;
- **Scan window**: 100 ms.

I beacons che trasmettono il segnale sono configurati con i seguenti parametri:

- **Adv interval**: 500 ms;
- **Rssi 1 m**: -36 dBm;
- **Tx Power**: 0 dBm

### 5.5.1 MQTT

Per questo progetto, è stato deciso di utilizzare il protocollo MQTT per consentire la comunicazione tra il gateway BLE e il terminale sul quale viene fatto girare il programma per il conteggio pezzi.

È stato introdotto da IBM nel 1999 ed è un protocollo a livello applicazione che differisce leggermente dal modello client/server del più noto protocollo applicativo HTTP.

Si basa sul modello publish/subscribe nel quale il mittente dei messaggi, detto publisher, li pubblicherà su uno specifico topic, sul message broker, cioè un programma che permette di gestire il flusso di dati in ingresso e in uscita al terminale sul quale è installato. Come message broker viene utilizzato il software open-source Mosquitto.

I subscribers, cioè i destinatari dei messaggi, si iscriveranno sotto il topic di interesse. Dunque, ogni volta che il publisher trasmette i messaggi, il broker si occuperà di distribuirlo a tutti i subscribers, iscritti ad uno stesso topic. Questo è un tipo di comunicazione asincrono.

### 5.5.2 Calcolo della distanza tra gateway e beacons

Nel momento in cui avviene il conteggio dei pezzi, bisogna avere una stima della distanza tra i beacons e il gateway, per capire se le unità di produzione (quindi i beacons associate ad esse) siano ad una distanza ragionevole dal gateway che viene predisposto vicino la linea di produzione.

Per il calcolo della distanza si utilizza il classico modello di pathloss a larga scala:

$$d = 10^{((RSSI_{1m} - RSSI)/10n)} \quad (58)$$

- **RSSI**: valore ricevuto dal gateway;
- **RSSI\_1m**: parametro del beacon, impostato in fase di configurazione;
- **n**: esponente di pathloss, impostato con il valore 3.

Prima di eseguire il calcolo della distanza stimata, il sistema raccoglie 30 valori di RSSI relativi al singolo beacon ed applica il Filtro di Kalman a singolo stadio per linearizzare questi valori [35].

Dopo aver ricevuto il 30-esimo segnale, viene calcolato il valore di RSSI medio necessario per il calcolo della distanza stimata:

$$d = 10^{((RSSI_{1m} - RSSI_{medio}) / 10n)} \quad (59)$$

Solo i beacon, che presentano una distanza dal gateway minore di una certa soglia prefissata di 7 metri, saranno conteggiati come presenti nelle prossimità del gateway.

### 5.5.3 Architettura dell'applicazione

Per ciò che riguarda l'applicazione di conteggio pezzi, i messaggi trasmessi dai beacon che si trovano nell'area di copertura del gateway, vengono pubblicati dal gateway stesso su un topic, ogni secondo, attraverso il protocollo MQTT. Il broker Mosquitto consente la lettura dei messaggi alle applicazioni iscritte al topic di interesse. Nel caso in esame, un programma scritto in codice Python si occuperà di gestire i messaggi trasmessi dai beacon e il filtraggio dei valori di RSSI. Il codice interagirà con i dati nelle tabelle del database MySQL.

Nell'immagine viene mostrata la configurazione del sistema di conteggio pezzi:

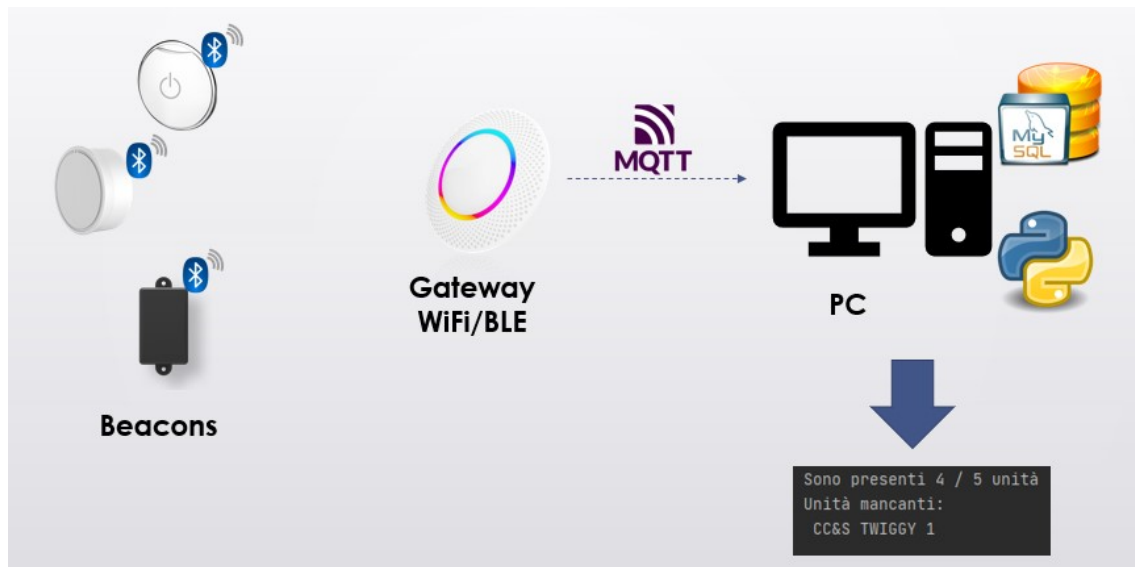


FIGURA 40: ARCHITETTURA CONTEGGIO PEZZI

#### 5.5.4 Step del conteggio pezzi

I beacons trasmettono pacchetti di advertising, il gateway li riceve solo dai beacons entro la sua area di copertura.

Tramite il protocollo MQTT, il gateway pubblica su un topic i dati dei beacon ricevuti, ogni secondo. Questi dati sono strutturati in formato JSON, i loro campi sono:

- MAC address del beacon;
- Dati del protocollo iBeacon (UUID, major, minor);
- Valore di RSSI ad 1 metro.

Il codice Python utilizza la libreria “paho.mqtt” che permette di sfruttare le funzionalità di questo protocollo. Nel caso specifico, il codice Python si sottoscrive al topic pubblicato dal gateway.

Una volta avviato il codice, viene richiesto all’utente di digitare il numero corrispondente al codice prodotto di cui si vuole eseguire il conteggio pezzi. A seconda del numero digitato, il sistema farà riferimento alla tabella corrispondente al codice prodotto scelto.

Si esegue un confronto tra i dati ricevuti dai beacon e quelli contenuti nel database. Viene fatto un primo controllo sulla distanza stimata di un beacon, se essa è maggiore rispetto una certa soglia, i dati trasmessi da quel beacon saranno ignorati. Un secondo controllo si effettua sul mac address. Se viene rilevato un messaggio trasmesso da un beacon che abbia il valore del mac address uguale ad uno di quelli memorizzati nella tabella del prodotto, verrà aggiornato il campo corrispondente della colonna “presente”, con il valore “si”.

La tabella viene aggiornata ogni secondo, per un tempo massimo di 2 minuti. Infine, viene stampato a schermo il numero di unità presenti e il numero e il nome delle unità mancanti all'appello.

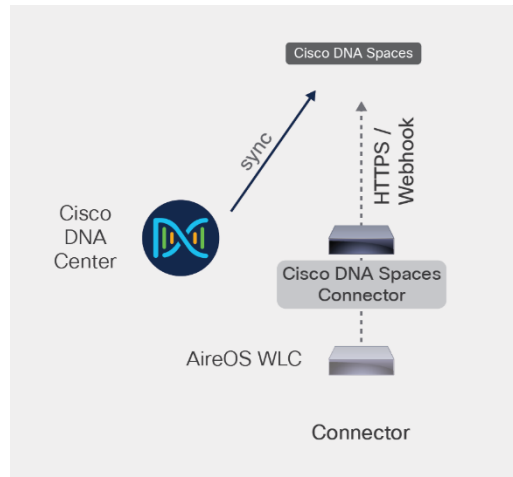
```
Sono presenti 4 / 5 unità  
Unità mancanti:  
CC&S TWIGGY 1
```

**FIGURA 41: OUTPUT DELL'APPLICAZIONE**

## 5.6 Secondo caso d'uso: Localizzazione

In questo progetto il lavoro è stato quello di testare un sistema di localizzazione commerciale (Cisco), di ottenere i dati tramite un codice Python e fornire questi dati in input ad un sistema di localizzazione custom che dovrà essere implementato nella pratica.

Il sistema adottato per la localizzazione è un'applicazione del servizio cloud Cisco DNA Space, chiamata Detect and Locate.



**FIGURA 42: ARCHITETTURA DEL SISTEMA CISCO**

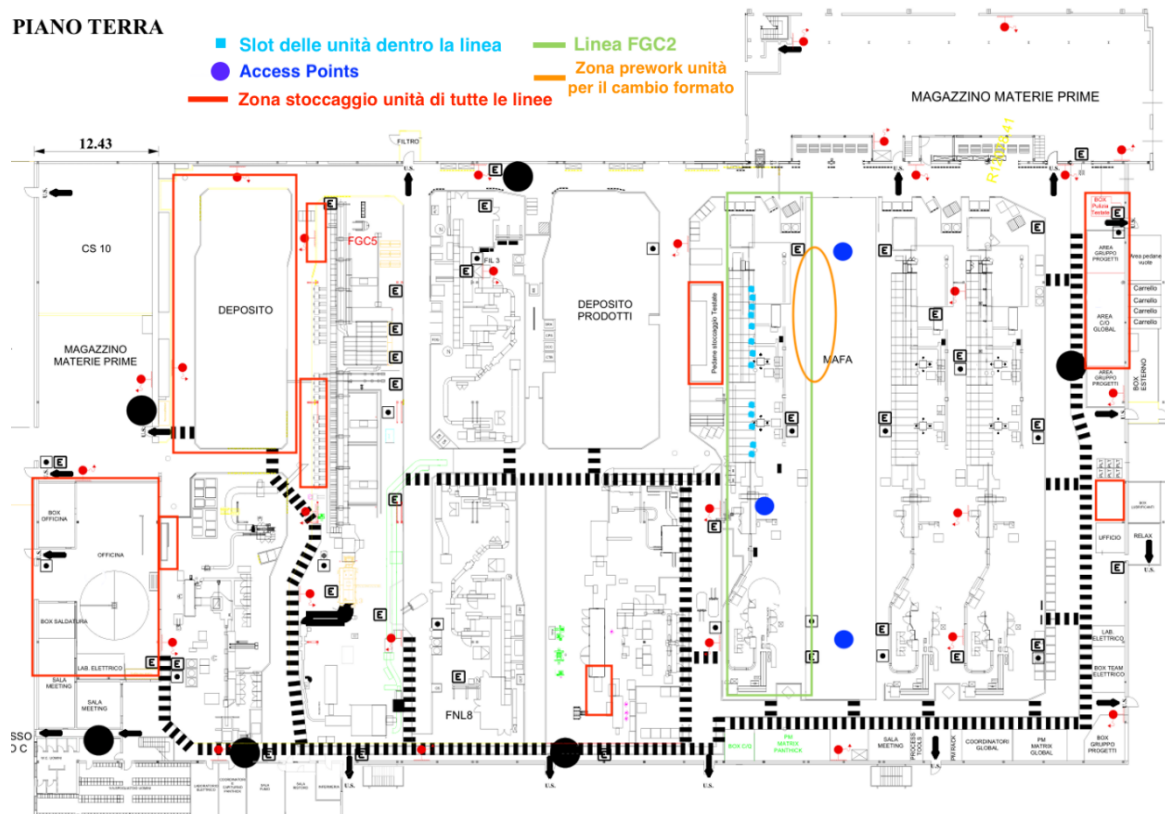
La piattaforma cloud di Cisco consente di utilizzare applicazioni dedicate all'IoT, tra queste, «Detect and Locate» con la quale è possibile localizzare sia client WiFi che tag BLE (quindi beacon BLE) all'interno di una mappa attraverso i segnali RSSI.

L'architettura di rete è composta da access points WiFi, che dispongono di un modulo BLE in modalità scanner, che rileveranno i pacchetti trasmessi dai beacon. Essi saranno gestiti da un WLC (Wireless Lan Controller) e logicamente collegati da un software (Cisco DNA Space Connector) installato su una macchina virtuale, che comunicherà direttamente con il servizio cloud.

Come operazione preliminare, è stato necessario inserire una mappa del luogo, in modo tale da avere delle posizioni degli oggetti relative al posto considerato e una visualizzazione grafica intuibile.

### 5.6.1 Mappa

La mappa del reparto viene caricata sull'applicazione attraverso Cisco Prime Infrastructure.



**FIGURA 43: MAPPA DEL REPARTO**

- **Blu:** Gli access points montati a circa 5 m da terra, su un braccio metallico.
- **Verde:** Nella mappa è mostrata la linea di test, la linea FGC2. Sono stati predisposti 3 Access point in modo tale da coprire tutto il perimetro di interesse della linea di test.
- **Giallo:** È la zona nella quale avviene il pre-work, è anche la zona dove avverrà il conteggio delle unità di produzione.
- **Rosso:** sono le aree nelle quali vengono depositate o entro le quali possono trovarsi le unità di produzione.
- **Azzurro:** gli slots della linea nei quali vanno inserite le unità

Per implementare il sistema di localizzazione sono stati utilizzati degli APs (Access Points) di Cisco. Gli APs sono dei Catalyst 9130 AXE-E, dotati di un modulo Bluetooth 5 integrato e possono agire sia come scanner che come advertiser.

Per implementare il sistema, vengono utilizzati 3 APs messi lungo la linea, in modo da avere una buona copertura di quell'area. Gli APs vengono messi ad un'altezza di circa 5 m da terra e disposti in modo da formare i vertici di un triangolo.

### 5.6.2 Acquisizione e organizzazione dei dati

Vengono fatte delle prove utilizzando dei beacon industriali modello i3 dell'azienda produttrice Minew. Per l'ottenimento dei dati dell'applicazione "Detect and Locate", è stato realizzato un codice Python che esegue delle interrogazioni tramite una REST API. I dati grezzi che l'applicazione di Cisco restituisce, sono in formato Json, quindi è necessaria una loro riorganizzazione. Infine, il codice crea un file .csv, che contiene le informazioni in una struttura tabellare chiamato "dati\_beacon".

**TABELLA 18: DATI DEI BEACONS**

macAddress	deviceType	campusId	buildingId	floorId	zoneId	lastLocatedAt	coordinates	geoCoordinates	AP_1	AP_2	AP_3	profiles	profile	uuid	major	minor
ac:23:3fe6:47:0c	BLE_TAG	3eff4ce4-c20931d7-f914-42e8-99da	cf21d8-5c-86-09T15:31:09.8	050f6f	2022-05-143.4	[248.9, 7836,	[42.44231481283				['84:f1:47:20:bea0',-99]	['profile Mac:']	IBEACON	00001818	3	2
ac:23:3fe6:47:0c	BLE_TAG	3eff4ce4-c20931d7-f914-42e8-99da	cf21d8-5c-86-09T15:31:19.6	050f6f	2022-05-143.4	[248.9, 7836,	[42.44231481283				['84:f1:47:20:bea0',-99]	['profile Mac:']	UNKNO WN	00001818	3	2
ac:23:3fe6:47:0c	BLE_TAG	3eff4ce4-c20931d7-f914-42e8-99da	cf21d8-5c-86-09T15:31:28.5	050f6f	2022-05-143.4	[248.9, 7836,	[42.44231481283				['84:f1:47:20:bea0',-98]	['profile Mac:']	UNKNO WN	00001818	3	2
ac:23:3fe6:47:0c	BLE_TAG	3eff4ce4-c20931d7-f914-42e8-99da	cf21d8-5c-86-09T15:31:39.4	050f6f	2022-05-143.4	[248.9, 7836,	[42.44231481283				['84:f1:47:20:bea0',-98]	['profile Mac:']	IBEACON	00001818	3	2
ac:23:3fe6:47:0c	BLE_TAG	3eff4ce4-c20931d7-f914-42e8-99da	cf21d8-5c-86-09T15:31:43.1	050f6f	2022-05-143.4	[248.9, 7836,	[42.44231481283				['84:f1:47:20:bea0',-100]	['profile Mac:']	IBEACON	00001818	3	2
ac:23:3fe6:47:0c	BLE_TAG	3eff4ce4-c20931d7-f914-42e8-99da	cf21d8-5c-86-09T15:31:49.4	050f6f	2022-05-143.4	[248.9, 7836,	[42.44231481283				['84:f1:47:20:bea0',-99]	['profile Mac:']	IBEACON	00001818	3	2
ac:23:3fe6:47:0c	BLE_TAG	3eff4ce4-c20931d7-f914-42e8-99da	cf21d8-5c-86-09T15:32:00.3	050f6f	2022-05-143.4	[248.9, 7836,	[42.44231481283				['84:f1:47:20:bea0',-98]	['profile Mac:']	UNKNO WN	00001818	3	2
ac:23:3fe6:47:0c	BLE_TAG	3eff4ce4-c20931d7-f914-42e8-99da	cf21d8-5c-86-09T15:32:06.5	050f6f	2022-05-143.4	[248.9, 7836,	[42.44231481283				['84:f1:47:20:bea0',-100]	['profile Mac:']	IBEACON	00001818	3	2
ac:23:3fe6:47:0c	BLE_TAG	3eff4ce4-c20931d7-f914-42e8-99da	cf21d8-5c-86-09T15:32:08.9	050f6f	2022-05-143.4	[248.9, 7836,	[42.44231481283				['84:f1:47:20:bea0',-99]	['profile Mac:']	IBEACON	00001818	3	2
ac:23:3fe6:47:0c	BLE_TAG	3eff4ce4-c20931d7-f914-42e8-99da	cf21d8-5c-86-09T15:32:23.8	050f6f	2022-05-143.4	[248.9, 7836,	[42.44231481283				['84:f1:47:20:bea0',-98]	['profile Mac:']	IBEACON	00001818	3	2

Colonne:

- **macAddress:** del beacon trasmittente;
- **deviceType:** tipo di dispositivo rilevato (se è un beacon Bluetooth sarà BLE\_TAG)
- **campusId, buildingId, floorId, zoneId:** colonne relative ad informazioni sulla mappa;



- **lastLocatedAt:** il momento in cui è stato ricevuto un messaggio di advertising da un beacon (in formato data/ora)
- **coordinates:** coordinate relative, indicano i punti nella mappa;
- **geoCoordinates:** coordinate assolute, longitudine e latitudine;
- **AP1, AP2, AP3:** colonne relative ai diversi access points, contengono una lista di 2 valori, il primo è il mac address dell'AP e il secondo è il valore di RSSI del beacon;
- **Profiles, profile:** colonne che indicano qual è il protocollo che utilizza il beacon (di default i beacon utilizzati trasmettono il segnale con protocollo iBeacon);
- **UUID, major, minor:** dati del protocollo iBeacon.

Una struttura tabellare di questo tipo è stata scelta per fornire le informazioni, in maniera adatta, ad un algoritmo sperimentale basato sulla tecnica del fingerprinting, per eseguire un confronto con il sistema di localizzazione di Cisco.

### 5.6.3 Algoritmo sperimentale

Questo algoritmo non è stato implementato nella pratica, in questa tesi è stato svolto uno studio teorico della sua futura applicazione. Esso è basato sulla tecnica del fingerprinting con valori di RSSI, già descritta sommariamente in precedenza. Sono quindi previste 2 fasi principali:

#### **Fase offline**

Solitamente in questo step avviene la raccolta dati, tuttavia in questo caso vengono utilizzate le informazioni nel file .csv “dati\_beacon” citato precedentemente.

In un database esterno, detto database di fingerprinting, vengono annotati i valori di RSSI del beacon, calcolati da tutti gli AP in visibilità per ogni punto di

riferimento. Un punto di riferimento è una posizione nota nella quale vien posto il beacon e vengono registrati i suoi dati nel database di fingerprinting.

### Fase online

Viene posto un beacon in una posizione ignota all'interno della scena.

Ogni access point calcolerà l'RSSI del beacon e lo confronterà con i valori nel database relativi alle posizioni note. Per eseguire il confronto si utilizza l'algoritmo KNN con distanza euclidea per eseguire i calcoli [34].

Viene quindi calcolata la distanza tra i valori di RSSI e messa in forma vettoriale, ogni elemento del vettore è corrispondente all'i-esimo punto di riferimento. Questa è l'equazione che descrive il problema:

$$D_i = \sqrt{\sum_{j=1}^M (P_{r,dB}(d^j) - P_{r,dB}(d_i^j))^2} \quad \text{per } i = 1, 2, \dots, N \quad (60)$$

M è il numero di APs totale ed N è il numero totale di punti di riferimento nel database di fingerprinting. Il primo termine dell'equazione è l'RSSI acquisito dal j-esimo AP in un punto ignoto e il secondo termine è l'RSSI dello stesso AP al punto di riferimento i-esimo, nel database.

Il vettore conterrà N distanze. In seguito, verranno presi i "k" punti di riferimento che mostrano le distanze minori (bisogna impostare una soglia, es  $k=5$ ).

Vengono utilizzate quindi le coordinate relative ai punti di riferimento che hanno mostrato k distanze minori e di queste si calcola una media:

$$(x, y) = \frac{1}{k} \sum_{i=1}^k (x_i, y_i) \quad (61)$$

$(x_i, y_i)$  sono le coordinate dell'i-esimo punto di riferimento.

Invece WKNN è una variante del KNN. Viene usato un coefficiente di peso:

$$(x, y) = \sum_{i=1}^k w_i (x_i, y_i) \quad (62)$$

Il coefficiente di peso dell'i-esimo RP determinato dalla formula è  $w_i$ :

$$w_i = \frac{1/D_i}{\sum_{i=1}^k (1/D_i)} \quad (63)$$

Dove  $D_i$  si calcola come sopra.

## 6 Conclusioni

Il presente lavoro di tesi si inquadra nel contesto dell'IIoT in particolare viene proposta una architettura di rete in grado di offrire due servizi importanti in un contesto industriale come quello del conteggio pezzi e localizzazione indoor.

Grazie alla collaborazione con l'azienda Fater S.p.A. è stato possibile testare il sistema in un contesto industriale reale che tiene conto di tutte le criticità che entrano in gioco.

Tutte e due le applicazioni consentono una riduzione dei tempi di ritardo, quindi, sono delle ottime soluzioni a problematiche industriali, come la ricerca di oggetti. Per la prima applicazione (conteggio pezzi) è stato utilizzato un solo AP e il sistema è stato sviluppato e testato presso la linea di produzione di test FGC2.

Il sistema rileva correttamente la presenza degli oggetti ai quali sono stati associati i beacons.

La seconda applicazione il sistema proposto è stato implementato e testato presso il DII dell'UNIVPM ottenendo come risultati un errore medio rispetto alla posizione realmente assunta dal target dell'ordine di 1 metro e un errore massimo 1,5 metri. Mentre presso la Fater è stato testato un sistema commerciale già in uso. I risultati hanno mostrato una scarsa precisione, dell'ordine di 5 metri, per via della

densità degli APs lungo la linea di test. Per problemi tecnici di tempistiche non è stato possibile risolvere il problema in questo lavoro.

Sviluppi futuri riguardano il test del sistema di localizzazione proposto nel contesto industriale. Un obiettivo sarà quello di aumentare la densità degli APs nell'area di interesse, in modo da ottenere un errore di localizzazione inferiore ai 2 metri e poter effettuare il confronto con l'algoritmo sperimentale sulla linea di produzione.

Un altro possibile sviluppo riguarda il tracciamento di persone all'interno del reparto. Può essere utile per l'incremento della sicurezza, ad esempio fare in modo che in particolari aree pericolose possa accedere solo il personale che possiede un beacon autorizzato, per prevenire infortuni o danni ai macchinari.

Lo sviluppo delle applicazioni descritte nei precedenti capitoli sono esempi concreti di due casi d'uso che potrebbero beneficiare di quanto sviluppato in questo lavoro di tesi.

## Bibliografia

- [1]: Pereira, A.C., & Romero, F. (2017). A review of the meanings and the implications of the Industry 4.0 concept. *Procedia Manufacturing*, 13, 1206-1214.
- [2]: Koh, L., Orzes, G. and Jia, F.(J). (2019), "The fourth industrial revolution (Industry 4.0): technologies disruption on operations and supply chain management", *International Journal of Operations & Production Management*, Vol. 39 No. 6/7/8, pp. 817-828.
- [3]: E. Manavalan, K. Jayakrishna, A review of Internet of Things (IoT) embedded sustainable supply chain for industry 4.0 requirements, *Computers & Industrial Engineering*, Volume 127, 2019, Pages 925-953.
- [4]: B. Tjahjono, C. Esplugues, E. Ares, G. Pelaez, What does Industry 4.0 mean to Supply Chain?, *Procedia Manufacturing*, Volume 13, 2017, Pages 1175-1182.
- [5]: <https://www.redhat.com/it/topics/cloud-computing/iaas-vs-paas-vs-saas>
- [6]: Oztemel, E., Gursev, S. Literature review of Industry 4.0 and related technologies. *J Intell Manuf* 31, 127–182 (2020).
- [7]: Patel, K. K., Patel, S. M., & Scholar, P. (2016). Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges. *International journal of engineering science and computing*, 6(5).
- [8]: Samie, F., Bauer, L., & Henkel, J. (2016, October). IoT technologies for embedded computing: A survey. In *2016 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ ISSS)* (pp. 1-10). IEEE.
- [9]: Jaidka, H., Sharma, N., & Singh, R. (2020, May). Evolution of iot to iiot: Applications & challenges. In *Proceedings of the international conference on innovative computing & communications (ICICC)*.
- [10]: Maddikunta, P. K. R., Pham, Q. V., Prabadevi, B., Deepa, N., Dev, K., Gadekallu, T. R., ... & Liyanage, M. (2022). Industry 5.0: A survey on enabling

technologies and potential applications. *Journal of Industrial Information Integration*, 26, 100257.

[11]: Mainetti, L., Patrono, L., & Sergi, I. (2014, September). A survey on indoor positioning systems. In *2014 22nd international conference on software, telecommunications and computer networks (SoftCOM)* (pp. 111-120). IEEE.

[12]: Liu, H., Darabi, H., Banerjee, P., & Liu, J. (2007). Survey of wireless indoor positioning techniques and systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 37(6), 1067-1080.

[13]: Zafari, F., Gkelias, A., & Leung, K. K. (2019). A survey of indoor localization systems and technologies. *IEEE Communications Surveys & Tutorials*, 21(3), 2568-2599.

[14] Serra, F. A. (2018). *Industria 4.0: la quarta rivoluzione industriale, un'analisi del paradigma attraverso le tecnologie abilitanti e le nuove competenze richieste dal mercato: il caso Colombini Group Spa.*

[15] Cafagna F. (2020). *Industria 4.0: effetti ed opportunità della digitalizzazione sulle imprese.*

[16] Ohtsu T. (January 2019) *Bluetooth® Low Energy Technology that Brings the IoT to Life.*

[17] Rohde & Schwarz (November, 2020) *From cable replacement to the IoT Bluetooth 5.1.*

[18]: Tosi, J., Taffoni, F., Santacatterina, M., Sannino, R., & Formica, D. (2017). Performance evaluation of bluetooth low energy: A systematic review. *Sensors*, 17(12), 2898.

[19]: Townsend, K., Cufi, C., & Davidson, R. (2014). *Getting started with Bluetooth low energy: tools and techniques for low-power networking.* " O'Reilly Media, Inc."

[20]: Chong, C. C., Watanabe, F., & Inamura, H. (2006, August). Potential of UWB technology for the next generation wireless communications. In *2006 IEEE Ninth International Symposium on Spread Spectrum Techniques and Applications* (pp. 422-429). IEEE.

- [21]: Minoli, D., & Occhiogrosso, B. (2018, September). Ultrawideband (UWB) technology for smart cities IoT applications. In 2018 IEEE international smart cities conference (ISC2) (pp. 1-8). IEEE.
- [22]: <https://github.com/AltBeacon/spec>
- [23]: <https://developer.apple.com/ibeacon/Getting-Started-with-iBeacon.pdf>
- [24]: Ture, M., & Hatipoglu, A. (2019, June). Indoor location finding of the transmitter based on Bluetooth received signal strength. In 2019 International Symposium on Networks, Computers and Communications (ISNCC) (pp. 1-5). IEEE.
- [25]: Bai, L., Ciravegna, F., Bond, R., & Mulvenna, M. (2020). A low cost indoor positioning system using bluetooth low energy. *Ieee Access*, 8, 136858-136871.
- [26]: Essa, E., Abdullah, B. A., & Wahba, A. (2019, December). Improve performance of indoor positioning system using ble. In 2019 14th International Conference on Computer Engineering and Systems (ICCES) (pp. 234-237). IEEE.
- [27]: Sangthong, J., Thongkam, J., & Promwong, S. (2020, July). Indoor wireless sensor network localization using RSSI based weighting algorithm method. In 2020 6th International Conference on Engineering, Applied Sciences and Technology (ICEAST) (pp. 1-4). IEEE.
- [28]: Monfared, S., Nguyen, T. H., Petrillo, L., De Doncker, P., & Horlin, F. (2018, September). Experimental demonstration of BLE transmitter positioning based on AOA estimation. In 2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC) (pp. 856-859). IEEE.
- [29]: Li, H. Y., & Ma, H. P. (2018, September). A low complexity low power indoor positioning system based on wireless received signal strength. In 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom) (pp. 1-6). IEEE.
- [30]: Cantón Paterna, V., Calveras Auge, A., Paradells Aspas, J., & Perez Bullones, M. A. (2017). A bluetooth low energy indoor positioning system with

channel diversity, weighted trilateration and kalman filtering. *Sensors*, 17(12), 2927.

[31]: Martinelli, A., Jayousi, S., Caputo, S., & Mucchi, L. (2019, September). UWB positioning for industrial applications: The galvanic plating case study. In 2019 International Conference on Indoor Positioning and Indoor Navigation (IPIN) (pp. 1-7). IEEE.

[32]: Schroerer, G. (2018, September). A real-time UWB multi-channel indoor positioning system for industrial scenarios. In 2018 International Conference on Indoor Positioning and Indoor Navigation (IPIN) (pp. 1-5). IEEE.

[33]: Chan, Y. T., & Ho, K. C. (1994). A simple and efficient estimator for hyperbolic location. *IEEE Transactions on signal processing*, 42(8), 1905-1915.

[34]: Li, M., Zhao, L., Tan, D., & Tong, X. (2019). BLE fingerprint indoor localization algorithm based on eight-neighborhood template matching. *Sensors*, 19(22), 4859.

[35]: Zhang, K., Zhang, Y., & Wan, S. (2016, October). Research of rssi indoor ranging algorithm based on gaussian-kalman linear filtering. In 2016 IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC) (pp. 1628-1632). IEEE.

[36]: Fernández-Caramés, T. M., Fraga-Lamas, P., Suárez-Albela, M., Castedo, L., Crepaldi, P. C., & Pimenta, T. C. (2017). A methodology for evaluating security in commercial RFID systems. *Radio Frequency Identification*.



## **Bibliografia immagini**

**Figura 1:** Chapter 12 - Internet of Things Technologies

**Figura 2:** Patel, K. K., Patel, S. M., & Scholar, P. (2016). Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges. *International journal of engineering science and computing*, 6(5).

**Figura 3:** Samie, F., Bauer, L., & Henkel, J. (2016, October). IoT technologies for embedded computing: A survey. In *2016 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ ISSS)* (pp. 1-10). IEEE.

**Figura 4:** <https://www.presentationpoint.com/blog/data-signals-triggers-industry-4-0/>

**Figura 5:** <https://nickelinstitute.org/en/blog/2020/november/customising-the-future-the-next-industrial-revolution/>

**Figura 6:** Zafari, F., Gkelias, A., & Leung, K. K. (2019). A survey of indoor localization systems and technologies. *IEEE Communications Surveys & Tutorials*, 21(3), 2568-2599.

**Figura 7:** Zafari, F., Gkelias, A., & Leung, K. K. (2019). A survey of indoor localization systems and technologies. *IEEE Communications Surveys & Tutorials*, 21(3), 2568-2599.

**Figura 8:** Zafari, F., Gkelias, A., & Leung, K. K. (2019). A survey of indoor localization systems and technologies. *IEEE Communications Surveys & Tutorials*, 21(3), 2568-2599.

**Figura 9:** Zafari, F., Gkelias, A., & Leung, K. K. (2019). A survey of indoor localization systems and technologies. *IEEE Communications Surveys & Tutorials*, 21(3), 2568-2599.

**Figura 10:** Ibnatta, Y., Khaldoun, M., & Sadik, M. (2021, May). Indoor localization techniques based on UWB technology. In *International Symposium on Ubiquitous Networking* (pp. 3-15). Springer, Cham.

**Figura 11:** Tosi, J., Taffoni, F., Santacatterina, M., Sannino, R., & Formica, D. (2017). Performance evaluation of bluetooth low energy: A systematic review. *Sensors*, 17(12), 2898.

**Figura 12:** Rohde & Schwarz (November, 2020) From cable replacement to the IoT Bluetooth 5.1.

**Figura 13:** Rohde & Schwarz (November, 2020) From cable replacement to the IoT Bluetooth 5.1.

**Figura 14:** Rohde & Schwarz (November, 2020) From cable replacement to the IoT Bluetooth 5.1.

**Figura 15:** Shan, G., & Roh, B. H. (2018). Advertisement interval to minimize discovery time of whole BLE advertisers. *IEEE Access*, 6, 17817-17825.

**Figura 16:** Townsend, K., Cufi, C., & Davidson, R. (2014). Getting started with Bluetooth low energy: tools and techniques for low-power networking. " O'Reilly Media, Inc."

**Figura 17:** Townsend, K., Cufi, C., & Davidson, R. (2014). Getting started with Bluetooth low energy: tools and techniques for low-power networking. " O'Reilly Media, Inc."

**Figura 18:** <https://microchipdeveloper.com/wireless:ble-link-layer-packet-types>

**Figura 19:** <https://it.mathworks.com/help/bluetooth/ug/bluetooth-packet-structure.html>

**Figura 20:** Rohde & Schwarz (November, 2020) From cable replacement to the IoT Bluetooth 5.1.

**Figura 21:** Rohde & Schwarz (November, 2020) From cable replacement to the IoT Bluetooth 5.1.

**Figura 22:** Rohde & Schwarz (November, 2020) From cable replacement to the IoT Bluetooth 5.1.

**Figura 23:** Rohde & Schwarz (November, 2020) From cable replacement to the IoT Bluetooth 5.1.

**Figura 24:** Rohde & Schwarz (November, 2020) From cable replacement to the IoT Bluetooth 5.1.

**Figura 25:** Rohde & Schwarz (November, 2020) From cable replacement to the IoT Bluetooth 5.1.

**Figura 26:** Townsend, K., Cufí, C., & Davidson, R. (2014). Getting started with Bluetooth low energy: tools and techniques for low-power networking. " O'Reilly Media, Inc."

**Figura 27:** Townsend, K., Cufí, C., & Davidson, R. (2014). Getting started with Bluetooth low energy: tools and techniques for low-power networking. " O'Reilly Media, Inc."

**Figura 28:** <https://os.mbed.com/blog/entry/BLE-Beacons-URIBeacon-AltBeacons-iBeacon/>

**Figura 29:** Hernández-Rojas, D. L., Fernández-Caramés, T. M., Fraga-Lamas, P., & Escudero, C. J. (2017). Design and practical evaluation of a family of lightweight protocols for heterogeneous sensing through BLE beacons in IoT telemetry applications. *Sensors*, 18(1), 57.

**Figura 30:** <https://austinblackstoneengineering.com/ble-beacons-ibeacon-altbeacon-uribeacon-and-derivatives/>

**Figura 31:** Bai, L., Ciravegna, F., Bond, R., & Mulvenna, M. (2020). A low cost indoor positioning system using bluetooth low energy. *Ieee Access*, 8, 136858-136871.

**Figura 32:** Bai, L., Ciravegna, F., Bond, R., & Mulvenna, M. (2020). A low cost indoor positioning system using bluetooth low energy. *Ieee Access*, 8, 136858-136871.

**Figura 33:** Cantón Paterna, V., Calveras Auge, A., Paradells Aspás, J., & Pérez Bullones, M. A. (2017). A bluetooth low energy indoor positioning system with channel diversity, weighted trilateration and kalman filtering. *Sensors*, 17(12), 2927.

**Figura 34:** Cantón Paterna, V., Calveras Auge, A., Paradells Aspás, J., & Pérez Bullones, M. A. (2017). A bluetooth low energy indoor positioning system with channel diversity, weighted trilateration and kalman filtering. *Sensors*, 17(12), 2927.

**Figura 35:** Martinelli, A., Jayousi, S., Caputo, S., & Mucchi, L. (2019, September). UWB positioning for industrial applications: The galvanic plating case study. In 2019 International Conference on Indoor Positioning and Indoor Navigation (IPIN) (pp. 1-7). IEEE.

**Figura 42:** <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/dna-spaces/guide-c07-744932.html>