**[](http://www.unict.it/sites/default/files/linee-guida-logo%20(2).pdf)**

Dipartimento di Ingegneria Elettrica Elettronica e Informatica

Corso di Laurea in Ingegneria Informatica

Anno 2020

Marco Francesco D’Alessandro

Elaborato finale

**Il Semaforo Intelligente**

|  |  |
| --- | --- |
|  | Relatore:  Chiar.mo Prof. Giovanni Schembra |

*To my family, my dog, etc…*

**Ringraziamenti**

Questo è il carattere da usare.

I paragrafi sono già giustificati

Thanks to you all.

**Indice**

|  |  |  |
| --- | --- | --- |
|  | **Introduzione** | 1 |
|  | **Capitolo 1 – Smart City** | 2 |
|  | 1.1 ICT | 4 |
|  | 1.2 ICT |  |
|  | 1.3 |  |
|  | **Capitolo 2 – Questo è il capitolo 2** | 18 |
|  | 2.1. |  |
|  | *2.1.1* |  |
|  | *2.1.3* |  |
|  |  |  |
|  | Conclusioni | 111 |
|  | **Bibliografia** | 115 |

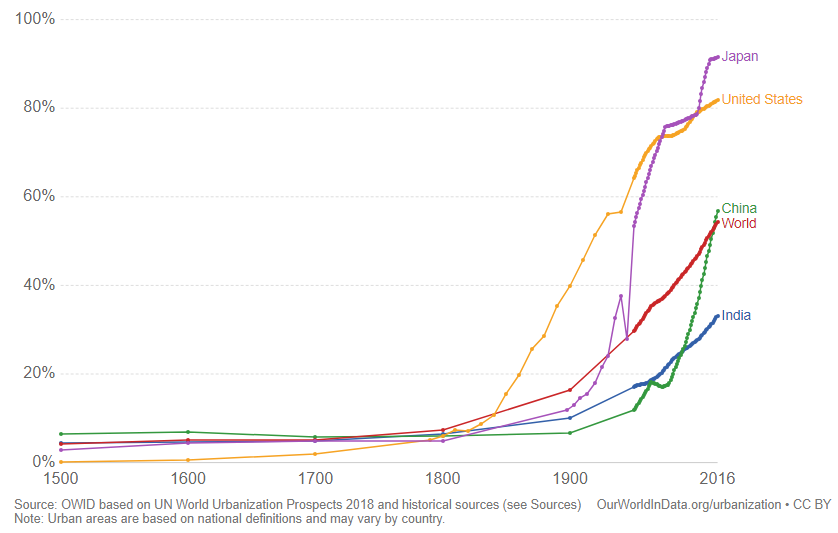
# Introduzione

In un momento storico in cui si ha una crescente urbanizzazione è necessario fare evolvere il concetto di città sia a livello funzionale che strutturale. In particolare, tramite l’ausilio delle nuove tecnologie dell’informazione e della comunicazione (ICT), si cerca di migliorare la qualità della vita dei cittadini ed il loro benessere. E’ cosi che viene introdotto il termine “Smart City”; con esso ci riferiamo a una città vista come un microcosmo di “oggetti” con cui i cittadini possono interagire quotidianamente: trasporti, illuminazione, segnaletica stradale, sensori e molto altro ancora. Ingredienti fondamentali di una Smart City sono quindi la comunicazione e la gestione di una grande mole di dati, entrambi favoriti dall’avvento del 5G. La sfida è quella di [ridurre il traffico](https://www.agendadigitale.eu/mercati-digitali/perche-le-auto-a-guida-autonoma-rischiano-di-peggiorare-il-traffico/), l’inquinamento, ottimizzare l’uso delle risorse, utilizzare i dati immagazzinati da tutti gli elementi di una Smart City per creare soluzioni intelligenti che rispondano alle reali esigenze dei cittadini.

# Smart City ICT

In risposta agli obbiettivi prefissati nel 2015 dall’Assemblea generale delle Nazioni Unite, le città del futuro vengono ormai progettate quali grandi ecosistemi iperconnessi, costellati di sensori e altri device capaci di raccogliere ed elaborare un’enorme quantità di dati.

Tra i vari fattori alla base del mecato delle smart city troviamo l’aumento dell’urbanizzazione, infatti l’incremento costante degli abitanti delle città e il conseguente aumento della dimensione dei centri abitati portano a dei problemi, tra i quali i cambiamenti ambientali e la scarsità di risorse che possono essere risolti tramite delle soluzioni ‘smart’.



**Fig. 1.1:** Urbanizzazione negli ultimi 500 anni.

L’etichetta ‘smart city’ dovrebbe allora indicare soluzioni intelligenti che consentano alle città moderne di prosperare, attraverso il miglioramento qualitativo della produttività.

Si possono allora elencare le caratteristiche che una città deve avere per essere classificata come “smart”:

* Utilizzo di una infrastruttura di rete per migliorare l’efficienza politica ed economica e per consentire lo svoluppo sociale, culturale e urbano. Col termine “infrastruttura” ci si riferisce a servizi per il tempo libero, alloggi, ICTs (telefoni cellulari, tv satellitare, computer networks, e-commerce, servizi internet). Questo punto porta in primo piano l’idea di una città completamente connessa come principale modello di sviluppo e di crescita.
* Forte attenzione all’inclusione sociale dei residenti nei servizi pubblici.
* Profonda attenzione al ruolo del capitale sociale nello sviluppo urbano. Una Smart City è una città in cui i residenti sono in grado di usare la tecnologia e di trarne vantaggio da essa.
* Sostenibilità ambientale come importante componente strategico. Infatti in un mondo in cui le risorse si vanno esaurendo e in cui le città basano il loro sviluppo e la loro ricchezza sul turismo e sulle risorse naturali, si rende necessaria l’adozione di strumenti in grado di garantire la sicurezza e l’uso rinnovabile del patrimonio naturale.

Le Smart City possono offrire un grande numero di servizi, ma a questo proposito si rende necessaria la creazione e la manipolazione di grandi quantità di dati per cui è richiesta l’esistenza e lo sviluppo di un’infrastruttura ICT ampia, solida e scalabile.

Le ICT nelle smart city permettono di migliorare le prestazioni e l’interattività dei servizi urbani, al fine di ridurre i costi e il consumo di risorse e le applicazioni che si basano su questa infrastruttura sono di supporto a tutti i servizi presenti in una smart city, i quali possono includere ad esempio la gestione dei flussi urbani, della sanità e dell’energia.



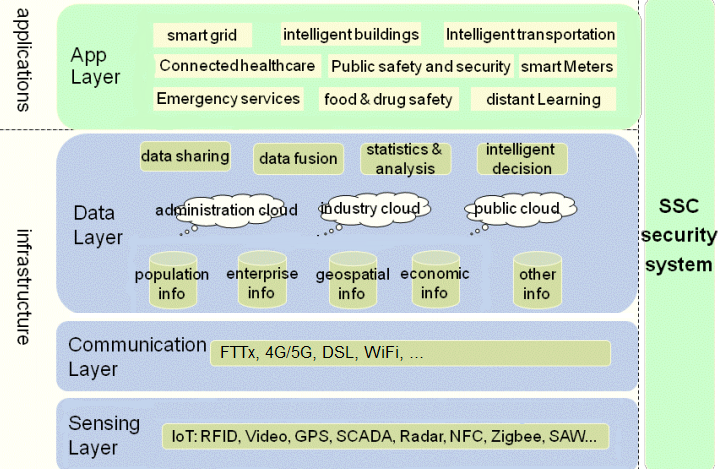
**Fig. 1.2:** Panoramica dei possibili servizi di una Smart City

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*ICT:* Information and Communications Technology

L’architettura di rete richiesta deve essere tale da mettere in comunicazione quanti più possibili servizi, per esempio Governativi, Commerciali, Sociali, e questo deve esser fatto in maniera sicura e veloce.

Viene organizzata in livelli: mentre le applicazioni che forniscono dei servizi lavorano ad alto livello mentre tutti i componenti della rete indispensabili al funzionamento delle applicazioni lavorano a basso livello. Tutta la rete, inoltre, deve essere posta sotto il controllo di un Security System che ne garantisca il funzionamento e la protezione dei dati.



**Fig. 1.3:** Layered Architecture

Verrà ora data una panoramica dell’infrastruttura di rete, evidenziandone le principali caratteristiche e descrivendone i componenti. La trattazione degli applicativi e dei servizi verrà fatta nel capitolo successivo.

### **1.1 Sensing Layer**

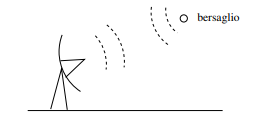
Il Sensing Layer comprende tutti quei dispositivi e relative tecnologie che permettono, in una Smart City, la raccolta delle informazioni dall’ambiente circostante, al fine di fornire dei servizi ai cittadini.

Tali dispositivi vengono di solito installati su strade, ponti edifici e veicoli e la sempre più numerosa presenza degli stessi in una città richiede un continuo sviluppo delle tecnologie tale da garantire una funzionalità continua e affidabile.

**1.1.1 Radar**

**Funzionamento e problematiche**

E’ un sistema che ha come obbiettivo quello di estrarre delle misure da un segnale ricevuto. In particolare, data l’emissione di un segnale s(t) noto, nel caso in cui tale segnale colpisca un bersaglio, parte dell’energia irradiata verrà riflessa e del segnale di ritorno verrà determinato il tempo che impiega per tornare alla sorgente e l’ ampizza del segnale: tali parametri sono, infatti, legati a proprietà del bersaglio e permettono di identificare la sua presenza, la distanza e le sue dimensioni.



**Fig. 1.4:** Radar monostatico (trasmettitore e ricevitore coincidono)

Il dimensionamento di un sistema Radar è complicato, soprattutto dal punto di vista energetico, considerando infatti la potenza ricevuta

emerge che l’attenuazione cresce con la quarta potenza della distanza.

Poiché è impensabile realizzare un Radar che permetta di rivelare qualsiasi bersaglio a qualsiasi distanza, tra le specifiche deve essere valutata la massima distanza Rmax a cui si trova il bersaglio da rivelare e la sezione minima σmin che si deve essere in grado di rivelare a tale distanza.

Il Radar è stato utilizzato prevalentemente in ambito militare, ma in una Smart City sarà sicuramente un dispositivo indispensabile, e molto presto verrà equipaggiato in auto, edifici, e addirittura in orologi da polso. Per la realizzazione di tale scenario, tuttavia, è necessario far fronte alla congestione spettrale, causata dalla presenza in contemporanea di un grande numero di radar. L’insieme delle tecnologie, atte alla risoluzione di questo problema vengono racchiuse dal termine JRC (Joint Radar-Communication). Esse offriranno un’importante opportunità per la riduzione dell’utilizzo dello spettro frequenziale e per la minimizzazione del consumo energetico, e permetteranno la creazione di una nuova piattaforma chiamata IoR (Internet of Radio Detectors And Rangers), che garantirà la simultanea ed efficente connessione di un numero elevato di Radar.

**mmWare**

I maggiori sforzi sono rivolti alla banda mmWare, corrispondente alla gamma di frequenze 30-300GHz, poiché è quella più usata per servizi che richiedono grandi velocità di scambio dati, tra i quali guida autonoma, monitoraggio sanitario, riconoscimento gesti.

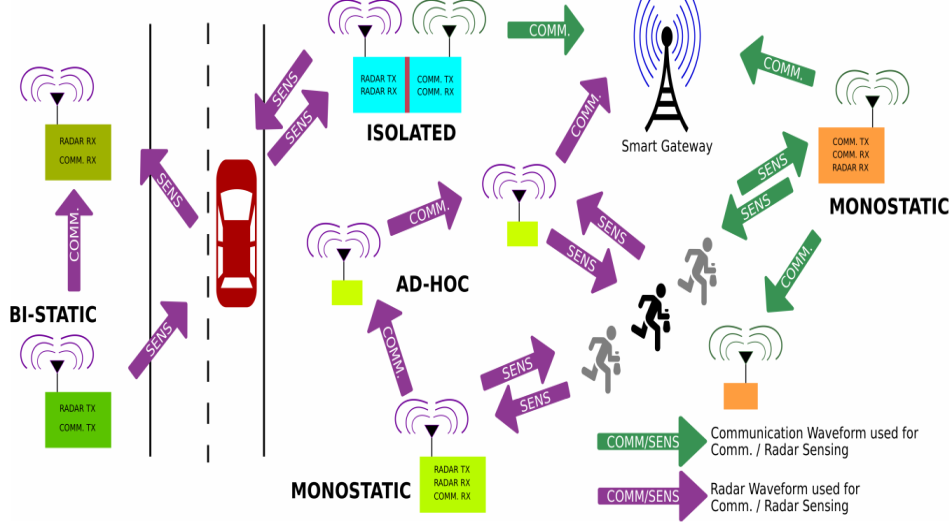
Verranno ora esposte le principali caratteristiche del canale mmWare.

* Forte Attenuazione: in contrasato con i segnali che si propagano a bande inferiori ai 6GHz i segnali mmWave hanno un basso potere penetrante con conseguente importante riduzione della potenza in ricezione. I radar mmWave, quindi, necessitano canali di comunicazione liberi e piccole aree di copertura.
* Grande larghezza di banda: la banda mmWave permette grandi data-rate per la comunicazione, ma ciò implica l’uso di complessi algoritmi per la trasmissione e per la ricezione.
* Basso tempo di coerenza: gli applicativi facenti utilizzo della banda mmWave presentano tempi di coerenza di pochi nanosecondi, e ciò porta all’esigenza di adattare la forma d’onda tramite feedback quando le caratteristiche del canale di trasmissione variano nel tempo.

**Topologie**

In uno scenario IoR si possono trovare radar di diversa tipologia, dimensione e funzionalità, tuttavia la maggior parte di essi richiede il collegamento ad Internet per inviare i dati raccolti ai server. Ogni radar, quindi, oltre ad avere una sezione di rilevamento necessita anche di una sezione che permetta la comunicazione. La relazione tra le due sezioni e quella tra il ricevitore e il trasmettitore è differente in relazione alle esigenze. Le topologie più frequenti sono:

* Isolamento: tale soluzione è abbastanza recente e consiste nella separazione tra la parte di rivelamento e quella di comunicazione. Questo approccio permette di risolvere i problemi di interferenza.
* Monostatica: la maggior parte delle tecnologie JRC sono proposte per il caso in cui il trasmittore e il ricevitore sono posti nello stesso dispositivo, e tale soluzione è la più semplice da realizzare.
* Bistatica: In questo approccio il trasmettitore e il ricevitore si trovano in dispositivi diversi e distanti tra loro. Il vantaggio di questa topologia è quello di avere un ridotto consumo energetico.
* Ad-Hoc: è la soluzione che viene adottata quando i dispositivi hanno delle limitazioni come per esempio una notevole distanza da un gateway, e consiste nella collaborazione tra piu radar al fine di migliorare le proprie capacità di rivelamento. Una WRSN (Wireless radar sensor network) usa spesso questo tipo di topologia.



**Fig. 1.5:** possible topologies for the IoR

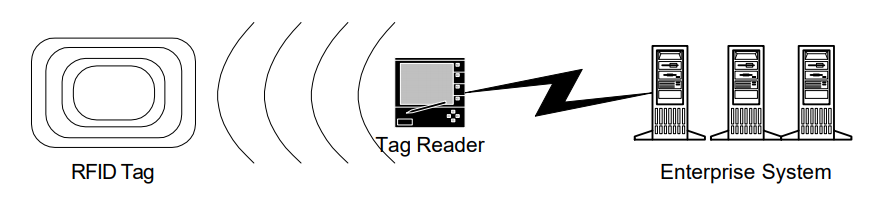
**1.1.2 RFID**

RFID, acronimo di Radio Frequency Identification, è una tecnologia per l’identificazione e/o memorizzazione automatica di informazioni riguardanti oggetti o persone. E’ in uso dal 1970 e rappresenta un miglioramento del rivelamento dei codici a barre, in termini densità di informazioni scambiate e capacità di comunicazione bidirezionale.

**Architettura**

Ci sono molti metodi di identificazione, ma il più usato consiste nell’assegnazione di un RFID tag ad un oggetto o persona. Un sistema RFID tipicamente comprende:

* Dispositivo dotato di un tag
* Lettore tag
* Connesione a un sistema informativo



**Fig. 1.6:** RFID system

I dispositivi RFID possono essere suddivisi in tre categorie:

* Attivi: sono alimentati elettricamente, sono dispositivi di lettura e di scrittura e vengono chiamati Trasponder (TRANSmitter/resPONDER).
* Passivi: sono dei dispositivi di sola lettura, vengono chiamati “tag” e sono molto economici. L’energia viene prelevata dal lettore attraverso accoppiamento induttivo, e l’attivazione avviene quindi solo se la distanza tra lettore e tag è molto piccola. I problemi sono la ridotta capacità di archiviazione dati e il bisogno un lettore con un’elevata potenza. Sono sconsigliati inoltre in ambienti elettromagneticamente “rumorosi”.
* Semi Passivi: sono dotati di una batteria che alimenta il circuitito, ma la comunicazione avviene prelevando energia dal lettore.

I tag possono vengono collocati solitamente sotto la pelle degli animali (tag di tracciamento) e nelle carte di credito e hanno dimensioni di pochi millimetri; i più piccoli disponibili in commercio sono più sottili di un foglio di carta.

**Memorizzazione dati**

Possono essere dotati sia di memoria RAM che ROM: la ROM viene usata per salvare dei dati in modo sicuro, come per esempio l’identificativo unico del dispositivo, la RAM per l’archiviazione dei dati durante l’interrogazione e la risposta del transponder.

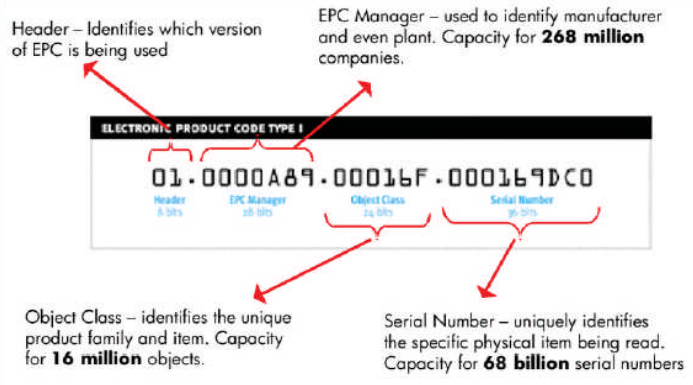
Uno standard per lo storage dei dati è EPC (Electronic Product Code): esso definisce i protocolli e la struttura dati per il salvataggio delle informazioni in un sistema RFID. E’ stato sviluppato al MIT nell’ Auto-ID Center, e nel Novembre 2003 la sua gestione e commercializzazione è stata affidata alla EPCglobal Inc.

Le specifiche EPC definiscono cinque categorie di tag in base alle funzionalità:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Classe | Nickname | Memoria | Alimentazione | Utilizzo |
| 0 | Tags Antitaccheggio | Assente | Passivo | Sorveglianza articoli |
| 1 | EPC | Lettura | Qualsiasi | Identificazione |
| 2 | EPC | Lettura-Scrittura | Qualsiasi | Data logging |
| 3 | Sensor Tags | Lettura-Scrittura | Semi passiva  Attiva | Sensori d’ambiente |
| 4 | Smart Dust | Lettura-Scrittura | Attiva | Networking Ad Hoc |

Viene inoltre definito il formato per l’encode e il decode dai tag RFID a 64 e 96 bit:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Tipo | Header | EPC manager | Object Class | Serial number | Totale |
| 64 bit, tipo 1 | 2 bit | 21 bit | 17 bit | 24 bit | 64 bit |
| 64 bit, tipo 2 | 2 bit | 15 bit | 13 bit | 34 bit | 64 bit |
| 64 bit, tipo 3 | 2 bit | 26 bit | 13 bit | 23 bit | 64 bit |
| 96 bit | 8 bit | 28 bit | 24 bit | 36 bit | 96 bit |



**Fig. 1.6:** EPC Class 1 (96bit) Tag Content

**Utilizzo**

I range di frequenze alla quale lavorano i sistemi RFID vengono gestiti attraverso leggi e regolamentazioni governative, e variano quindi di regione in regione. Attualmente, a livello globale, possiamo individuare tre range di frequenze disponibili per la tecnologia RFID:

|  |  |  |
| --- | --- | --- |
| Range di Frequenze | Caratteristiche | Utilizzo |
| 100-500 kHz | Costi ridotti  Bassa velocità di lettura  Lettura a basso raggio | Identificazione di animali Gestione accessi  Gestione magazzini |
| 10-15 MHz | Costi ridotti  Media velocità di lettura  Lettura a medio raggio | Smart Cards  Gestione accessi |
| 850-950 MHz  2.4-5.8 GHz | Costi elevati  Alta velocità di lettura  Lettura ad alto raggio | Monitoraggio veicoli  Tracciamento veicoli  Monitoraggio container |

I campi di utilizzo dei dispositivi RFID possono essere classificati in 4 categorie:

* EAS (Electronic Article Surveillance): sono dei sistemi usati per percepire la presenza o l’assenza di un oggetto e vengono usati principalmenti per sistemi di anti taccheggio.
* Portable Data Capture: vengono usati in combinazione con lettori, sensori e microprocessori e possono registrare per esempio variazioni di temperatura o eventi sismici.
* Networked Systems: caratterizzati da dei lettori fissi usati per tracciare il movimento di oggetti dotati di un tag.
* Positioning Systems: danno un supporto alla navigazione a veicoli e persone dotati di un tag.

I principali vantaggi nell’utilizzo dei sistemi RFID sono l’assenza di contatto tra tag e lettore e la non necessarietà di una linea visiva: tali caratteristiche permettono a questa tecnologia di essere utilizzata anche in condizioni difficili, quali pioggi, neve e elevate distanze. Inoltre il basso tempo di risposta di circa 100ms permette a un lettore RFID di leggere instantaneamente molti tags, al tal punto da rendere la lettura virtualmente simultanea.

**1.1.3 Zigbee**

E’ uno dei principali standard di comunicazione per le WSN (Wireless Sensor Network), e definisce le specifiche per le WPAN che richiedono un basso transfer rate (LR-WPAN).

Basato sullo standard IEEE802.15.4, il quale definisce il livello fisico e MAC, Zigbee definisce il livello di rete e applicativo di una LR-WPAN.

Un grande vantaggio nell’uso di questo standard è il ridotto consumo energetico, infatti nella maggior parte dei casi usa 1mW o meno.

Fornisce, tuttavia, una portata in esterno di 150m grazie alla tecnologia Direct Sequenze Spread Spectrum (DSSS).

**Architettura**

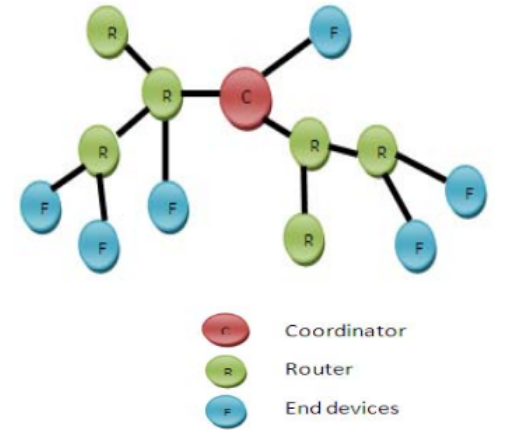
Le caratteristiche di trasmissione sono:

|  |  |  |  |
| --- | --- | --- | --- |
|  | 865Mhz | 915Mhz | 2450Mhz |
| Channels | 1 | 10 | 16 |
| Data Rate | 20Kbps | 40Kbps | 250Kbps |
| Applicability | Europe | USA | World |

Poiché le banda a cui opera sono diverse da quelle usate dalle comuni tecnologie wireless, quali WiFi e Bluetooth, viene garantita la assenza di interferenze con le altre Wireless Network.

I componenti di una rete basata su ZigBee sono:

* Physical Device: si hanno due tipo di physical devices:
* i Full Function Devices (FFD): gestiscono tutte le operazioni, tra cui i meccanismi di routing, di sensoristica e di controllo, e vengono alimentati costantemente.
* Reduced Function Devices (RFD): sono degli end device come ad esempio sensori o attuatori, ed eseguono solo delle operazioni limitate, tra le quali misurazione temperatura, controllo luminosità e controllo di dispositivi esterni. Essi non gestiscono il routing e sono associati a dei FFD.
* Logical Device: vengono divisi in tre categorie:
* Coordinator: crea e gestisce l’albero della rete scegliendo parametri tra i quali frequenza del canale e network identifier, e può anche conservare informazioni di sicurezza.
* Router: è un nodo intermediario, permette lo scambio dati tra tutti i dispositivi e può anche estendere la rete.
* End Devices: possono essere a bassa potenza e alimentati a batteria. Raccolgono varie informazioni dai vari sensori e attuatori, possono comunicare con il Coordinator e i Router ma non possono scambiare dati con gli altri dispositivi. La loro operatività, inoltre, a differenza degli altri due dispositivi, non è richiesta full time.



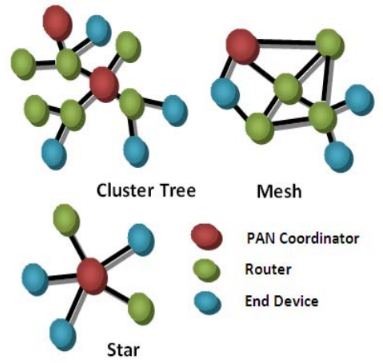
**Fig. 1.7:** Zigbee Network

* Access Modes: possono essere di due tipi:
* Beacon: ogni nodo della rete puà inviare dati quando il canale non è occupato.
* Non-beacon: ogni nodo può trasmettere solo in certi intervalli di tempo che vengono gestiti dal Coordinator.

**Topologie**

Nelle reti basate su Zigbee si hanno tre possibili topologie:

* Star: consiste in un coordinator e un certo numero di dispositivi. Si ha un modello master-slave, il coordinator, cioè un FFD, sarà il master mentre gli altri dispositivi, FFD o RFD saranno gli slave. I dispositivi non saranno collegati tra di loro, ma la comunicazione avviene sempre attraverso il coordinator.
* Cluster Tree: è simile alla Star Topology, con la differenza che in questo caso i dispositivi possono essere collegati a dei Router e ciò permette quindi una possibile espansione della rete.
* Mesh: ciascun nodo può comunicare con qualsiasi altro nodo vicino. La gestione è molto complessa ma la rete è più robusta.



**Fig. 1.7:** Zigbee topologies

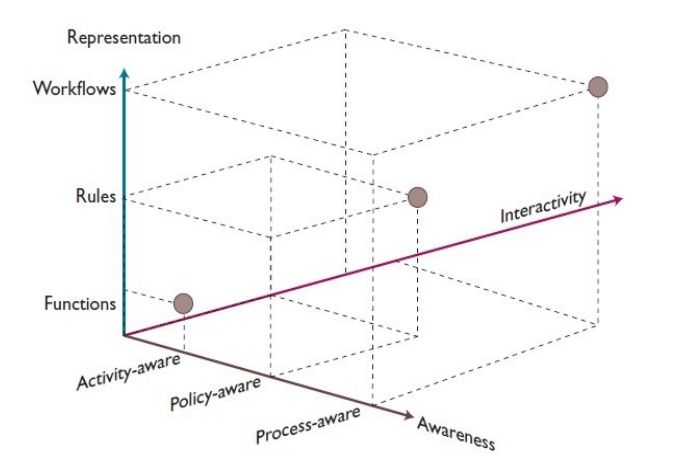
**1.1.4 Smart Object**

Uno Smart Object è un dispositivo di dimensioni di pochi cm cubici, equipaggiato con un sensore o un attuatore, un microprocessore, un dispositivo di comunicazione e una fonte di alimentazione; ingloba inoltre parti di una logica applicativa che gli permette di percepire, memorizzare e interpretare cosa accade nel mondo, infine è proattivo, cioè comunica con altri Smart Object e scambia informazioni con gli utenti.

Per andare incontro alle richieste computazionali ogni Smart Object viene progettato tenendo conto di tre aspetti chiave.

* Awareness: abilità di uno Smart Object di percepire, interpretare e reagire in relazione agli aventi che si verificano nel mondo fisico.
* Rappresentation: abilità di rappresentazione riferita al modello di programmazione dello Smart Object.
* Interactivity: abilità di uno Smart Object di dare un feedback all’utente.

Il giusto bilanciamento tra queste tre dimensioni dipende dalle richieste dello scenario applicativo; progettazioni più complesse non sono sempre le migliori.



**Fig. 1.8:** Le tre dimensioni di uno Smart Object

Da un analisi di vari progetti, si nota che la maggior parte ruota attorno a tre tipi di progetti chiavi:

* Activity-Aware Smart Object: memorizza informazioni sull’uso che ne viene fatto.
* Policy-Aware Smart Object: è in grado di interpretare eventi e attività.
* Process-Aware Smart Object: consente la creazione di tool che possono aiutare i lavoratori, attraverso la comunicazione di informazioni sulle attività di lavoro necessarie.

Si possono inoltre stabilire dei criteri per classificare l’intelligenza di uno Smart Object. In particolare, secondo l’Osservatorio Internet of Things del Politecnico di Milano, la base per stimare il livello di intelligenza di uno Smart Object si ha dall’analisi di alcune principali funzionalità, ciascuna delle quali può racchiuderne altre:

* Self-Awareness: rappresenta tutto ciò che riguarda l’oggetto stesso, quindi la presenza o meno di un identificativo digitale, la capacità di conoscere la propria posizione e di monitorare parametri interni all’oggetto al fine di rilevare malfunzionamenti.
* Funzionalità di interazione con l’ambiente: cioè tutte quelle funzionalità che permettono di acquisire dati dall’ambiente, tramite misure di sensing o di metering (le prime relative a variabili di stato, le seconde a variabili di flusso), o quelle relative alla capacità di eseguire comandi impartiti da remoto.
* Funzionalità di elaborazione dati: si riferisce alla capacità di trattare le informazioni raccolte tramite una elaborazione base, ad esempio tramite filtraggio, conversione, crittografia, o tramite una elaborazione avanzata, ad esempio tramite analisi statistiche.
* Funzionalità di connessione: riguarda le diverse capacità dell’oggetto di collegarsi con utenti o con altri oggetti.

**1.1.5 IoT**

Col termine “IoT”, ci si riferisce ad un’infrastruttura globale di oggetti “intelligenti” interconnessi tra loro, in grado di fornire connettività anytime ed anyplace sia per gli esseri umani che per le cose.

Il temine “IoT” è stato inizialmente usato da Kevin Ashton nel 1999 ed è divenuto ampiamente utilizzato grazie al lavoro di un gruppo di ricerca, Auto-ID Center, che ha lavorato nel campo del RFID e di altre tecnologie sensoristiche emergenti.

Il dominio tecnologico dell’IoT abbraccia diversi campi di sviluppo, ma poiché il principale interesse è rivolto a degli oggetti intelligenti interconnessi, si può orientare maggiore attenzione verso le tecnologie relative alla comunicazione oppure alle tecnologie di miniaturizzazione dei circuiti. Sfide importanti saranno:

* Energia: i dispositivi dovranno consumare poca energia, essendo molte volte alimentati a batteria, e ciò porterà allo sviluppo di nuovi protocolli di comunicazione a basso consumo energetico.
* Scalabilità: Una Smart city sarà composta da milioni di dispositivi, e la sfida sarà quella di organizzarli in sotto domini gerarchici, essendo impossibile collegarli tutti ad una stessa rete.
* Standardizzazione: Così come è stato per lo sviluppo di Internet, sarà necessaria la convergenza su un unico modello di riferimento per permettere all’IoT di affermarsi.
* Abbandono dell’approccio tradizionale: Internet come lo conosciamo oggi si basa su dei principi molto semplici, tra cui il principio dell’end-to-end, che si basa sulla gestione della complessita della rete solo nei dispositivi finali e rendere la rete a basso livello molto semplice. Con l’IoT questo non sarà sicuramente possibile perché gli end point dell’IoT saranno spesso dispositivi economici e a basso consumo e non potranno utilizzare protocolli complessi come per esempio IP. Inoltre ci sono dei possibili applicativi, quali i sistemi real time di frenatura delle automobili che non possono essere basati su un protocollo best-effort, privo di connessione e inaffidabile come lo è IP per definizione.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Banda ISM*: (Industrial, Scientific and Medical) è il nome assegnato dall'[Unione Internazionale delle Telecomunicazioni](https://it.wikipedia.org/wiki/Unione_Internazionale_delle_Telecomunicazioni) (ITU) ad un insieme di porzioni dello [spettro elettromagnetico](https://it.wikipedia.org/wiki/Spettro_elettromagnetico) riservate alle applicazioni di [radiocomunicazioni](https://it.wikipedia.org/wiki/Radiocomunicazione) non commerciali, ma per uso industriale, scientifico e medico.

### **1.2 Communication Layer**

Il Communication Layer è la spina dorsale di una Smart City, e consiste di tecnologie e infrastrutture fisiche che permettono il collegamento cablato e wireless tra tutti i nodi della rete, ma anche tra essi e Internet.

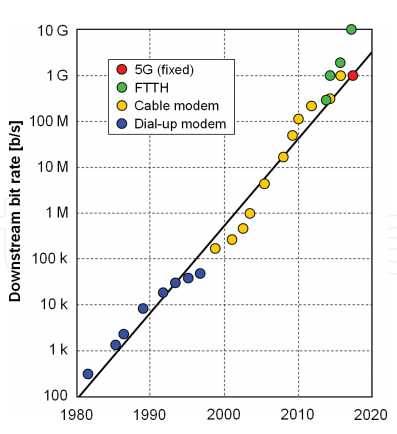
In questo paragrafo verranno esposte le principali tecnologie della Access Network, cioè l’ infrastruttura fisica destinata al collegamento tra i dispositivi e la prima centrale di commutazione.

**1.2.1. FTTx**

Il continuo aumento dei dispositivi connessi in rete e in previsione di una città ricca di serivizi porta all’esigenza di avere un’infrastruttura di rete che garantisca cui una larghezza di banda adeguata, affidabilità e bassi costi.

Per quanto riguarda le reti cablate, la tecnologia FTTx, permettendo bit rate fino a 10Gb/s, è quindi il punto di partenza per garantire tutti i servizi presenti in una Smart City. Un incremento significativo di bit rate oltre i 10Gb/s, nelle reti FTTx, sarà molto difficile, a causa di due problemi fondamentali:

* High Cromatic Dispersion: causa la distorsione del segnale ed è provocata dalla diversa velocità di propagazione nella fibra delle varie componenti spettrali dell’impulso.
* Uso di ricevitori a basso costo con modulazione NRZ e direct detection: con questa tecnologia la distanza di trasmissione è inversamente proporzionale al quadrato del bitrate. Approssimativamente si hanno 10Gb/s a 80Km, 20Gb/s a Km, 40Gb/s a 5Km.



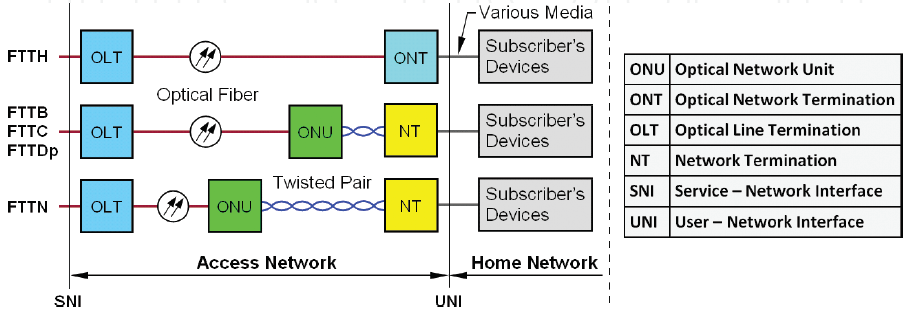
**Fig. 1.9:** Top download rates offered to residential customers in the USA

**Tipi di accesso**

L’architettura di rete definita da ITU-T Recommendation G.984.1 permette l’uso accoppiato di rame e fibra ottica. Poiché esistono diverse soluzioni possibili, questa architettura viene chiamata “fiber to the x” (FTTx).

I principali componenti della rete sono:

* OLT: locato in un central office (CO), funge da end point del fornitore di rete.
* ONT/NT: si trova nella sede dell’utente e si interfaccia con tutti i dispositivi.
* ONU: termina il collegamento in fibra e, utilizzando un mezzo diverso dalla fibra, estende il collegamento verso l’utente.



**Fig. 1.10:** The reference architecture of fiber access network defined by ITU-T .

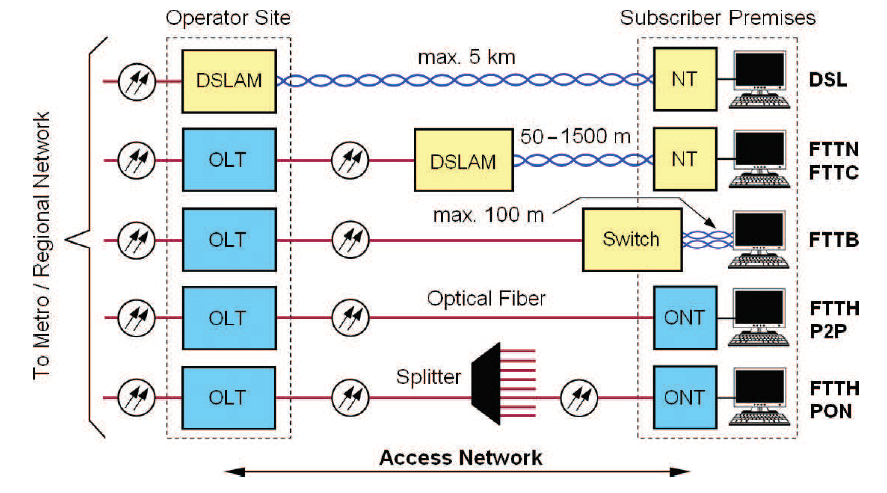
Le più comuni implementazioni di una rete FTTx differiscono per la lunghezza dell’ultimo tratto in rame (se è presente). L’ONU che converte il segnale proveniente dalla fibra e lo immette nel doppino in rame viene chiamato Digital Subscriver Line Acces Multiplexer (DSLAM), oppure Ethernet Switch nel caso di una LAN.

* FTTC (fibre to the cabinet): la rete in fibra ottica viene estesa con un DSLAM. Da quel punto segue una breve rete in rame (50-400m) fino a un NT. Il data rate può essere maggiore di 100 Mb/s.
* FTTN (fibre to node): simile alla FTTC, ma con lunghi tratti di rete in rame (fino a 1500m). Il data rate raggiunge i 40Mb/s.
* FTTB (fibre to the building): il condominio è cablato con cavi UTP al fine di creare una LAN che serva tutti gli abitanti. La terminazione del collegamento in fibra avviene tramite Ethernet Switch. Si hanno data rate da 100 Mb/s a 1 Gb/s.
* FTTH (fibre to the home): la rete in fibra ottica si estede fino ad un ONT posto nella sede del cliente. Può essere di due tipi:
* FTTH-PON: rete FTTH in cui la fibra proveniente dall’OLT viene splittata da 8 a 128 fibre di distribuzione fino a raggiungere la sede del cliente, formando una Passive Optical Network (PON). La larghezza di banda fornita dall’OLT viene quindi condivisa da tutti gli utenti della PON con un Time Division Multiplexing (TDM).

La rete rete tra L’OLT e l’insieme di ONT connesse viene chiamata Optical Distribution Network (ODN).

Gli svantaggi sono la condivisione della banda fornita dall’OLT, la perdita di potenza causata dalla presenza di più ONT, e i diversi ritardi di trasmissione di ogni ONT.

* FTTH-P2P: ogni cliente è collegato direttamente all’OLT. Non essendoci condivisione di rete tra più ONT, il data rate può raggiungere 1 Gb/s. La tramissione full-duplex è possibile grazie a un Wavelength Division Multiplexing (WDM), che è parte di un modulo di transmissione ottica. Verso l’utente, in downstream, si avranno lunghezze d’onda comprese tra 1480nm e 1500nm. Dall’utente, in upstream, si avranno lunghezze d’onda comprese tra 1260nm e 1360nm. Lo svantaggio principale è il costo elevato.
* FTTDp (fibre to the distribution point): rete di accesso basata sulla G.fast technology, con collegamento tramite doppino (10-250m) fino ad un Distribution Point Unit, posto in prossimità della sede del cliente.



**Fig. 1.11:** Basics variants of FTTx broadband access network

**Reti ibride**

Le reti FTTN, FTTC, FTTDp e FTTB, per via della presenza di tratti in rame, vengono chiamate reti ibride, e usano la tecnologia Digital Subscriver Line (DSL) per ridurre al minimo l’uso della fibra ottica. Questo tipo di approccio riduce considerevolmente i costi, tuttavia gli svantaggi sono molteplici:

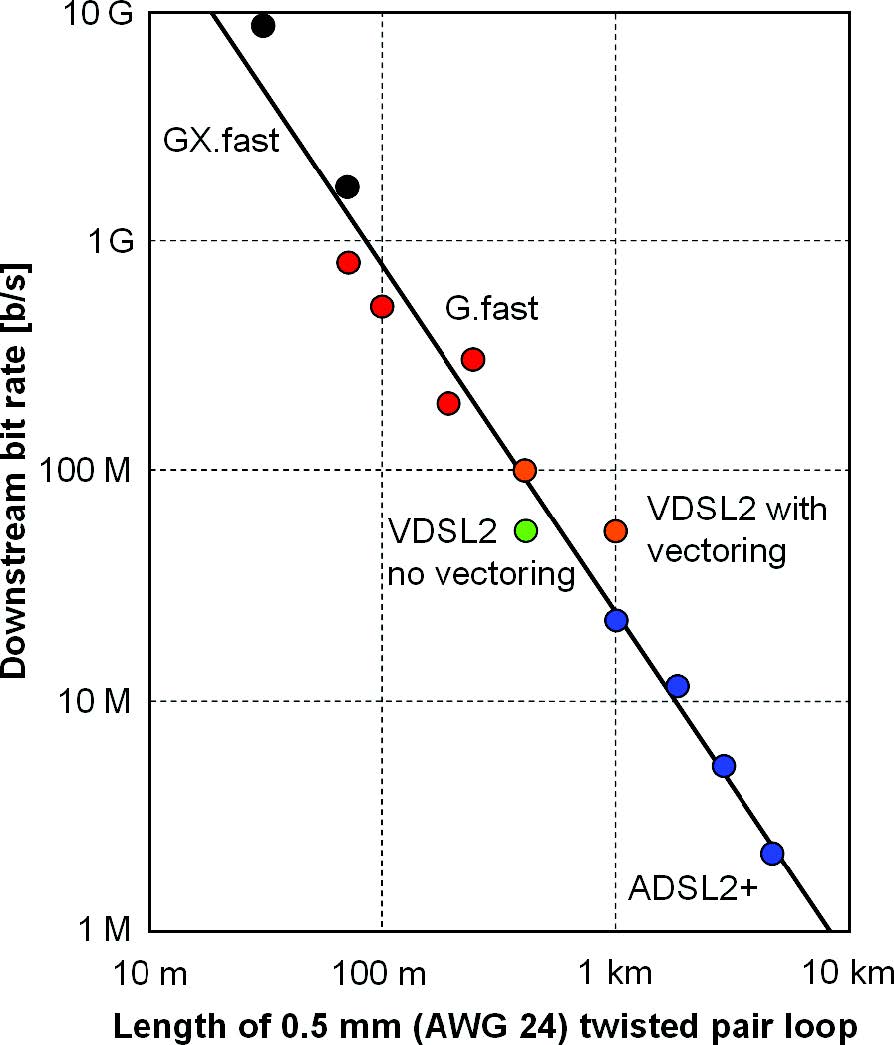
* L’Attenuazione e la diafonia aumentano con la frequenza, riducendo il bit rate e la portata.
* La diafonia tra doppini adiacenti impedisce l’operatività simultanea alle stesse frequenze. Il cavo, quindi, sarà un mezzo con larghezza di banda condivisa. Il problema può essere eliminato con la cancellazione digitale della diafonia, chiamata Vectoring.
* I vecchi cavi telefonici sono spesso in condizioni pessime, e possono causare interruzioni del servizio.

La dipendenza tra il bit rate B e la lunghezza L del collegamento tramite DSL viene data dalla seguente formula

Dove k è un fattore che dipende dal diametro e dalle condizioni del cavo. Elevati bit rate richiedono brevi tratti di rete in rame e un gran numero di unità remote .

Lo sviluppo dei sistemi DSL si concentra sull’aumento dei bit rate, combinato con i tentativi di fornire buona parte della capacità di rete anche a lunghe distanze. Necessitano, quindi, tecnologie che permettano l’adattamento dinamico delle caratteristiche di trasmissione del doppino in rame. Una soluzione adottata è l’utilizzo della modulazione DMT (Discrete Multitone Modulation) che consiste nella suddivisione del canale in un determinato numero di sottobande, in ciascuna delle quali il bit rate viene ottimizzato in relazione al SNR (signal-to-noise ratio).

Le performance possono essere migliorate anche tramite l’utilizzo di due o più doppini per una trasmissione parallela, più efficace se accoppiata col Vectoring.



**Fig. 1.12:** Typical reach vs. bit rate in DSL systems using twisted pairs in telephone cables.

**1.2.2. 5G**

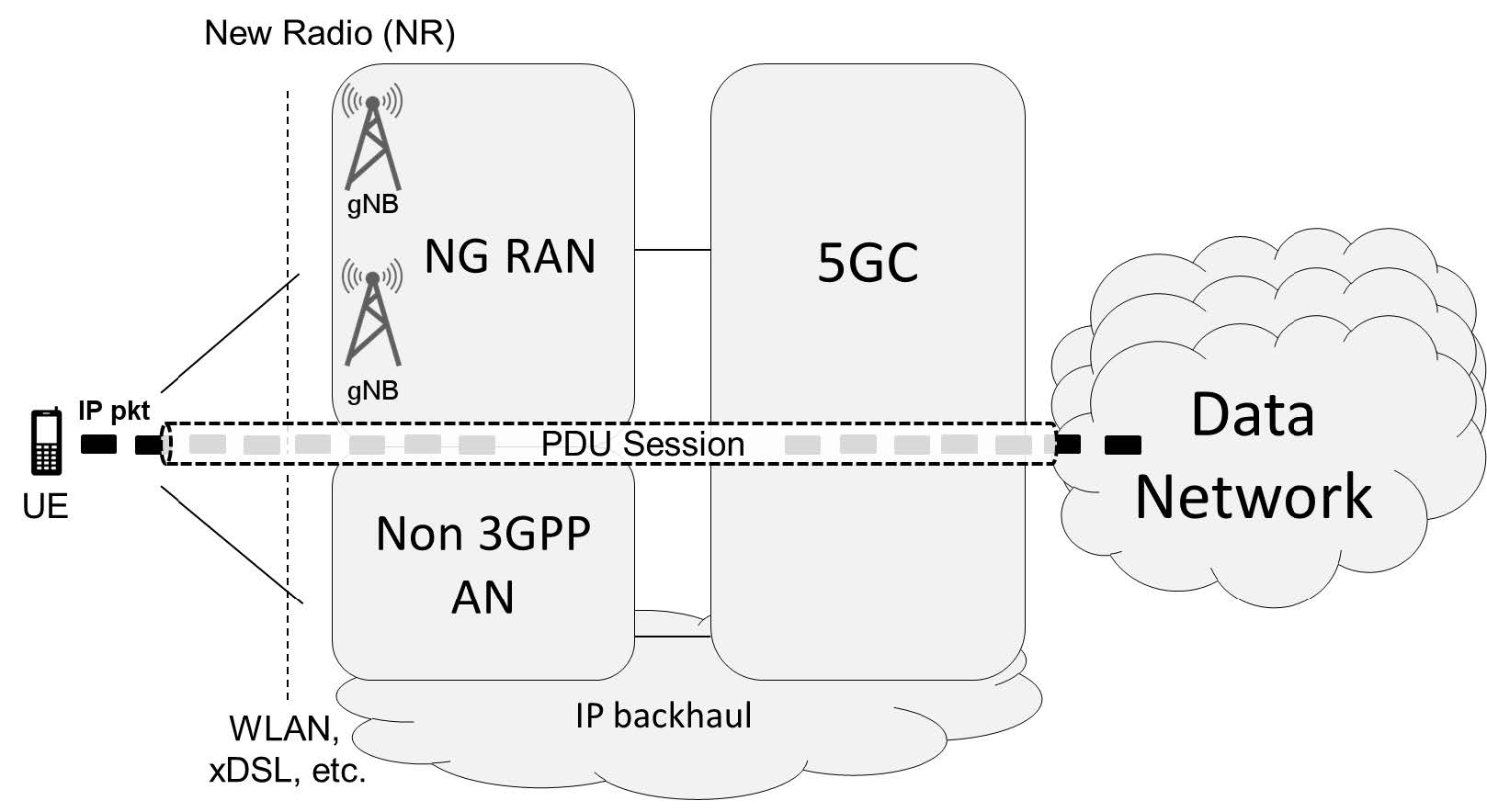
La richiesta di data transfer sempre più alti, e lo sviluppo dell’ IoT e del Machine to Machine (M2M), spingono verso una tecnologia wireless chiamata 5G. Tale tecnologia presenterà infatti numerosi miglioramenti rispetto alle precedenti reti wireless tra cui latenze basse, parecchie connessioni simultanee e copertura migliorata. In accordo con l’Unione Europea la tecnologia 5G è il fattore abilitante per una società pienamente connessa poiché permette ai vertical market di fornire applicazioni abilitanti per molti servizi indispensabili presenti in una Smart City.

Mentre in passato la progettazione dell’architettura della rete mobile era rivolta solo al miglioramento dell’esperienza degli end users, il 5G rappresenta una rivoluzione di questo approccio, e oltre a prevedere migliori caratteristiche comunicative, introduce una nuova categoria di utenti, cioè i Vertical Market, tra i quali la gestione della città, della sanità, dei trasporti e dell’energia.

Per tale eterogeneità, l’architettura 5G è stata progettata per consentire e favorire una softwarizzazione di tutte le funzioni di rete, e di conseguenza la tecnologia SDN e il Cloud Computing sono fondamentali per sfruttare a pieno la potenza di una rete 5G.

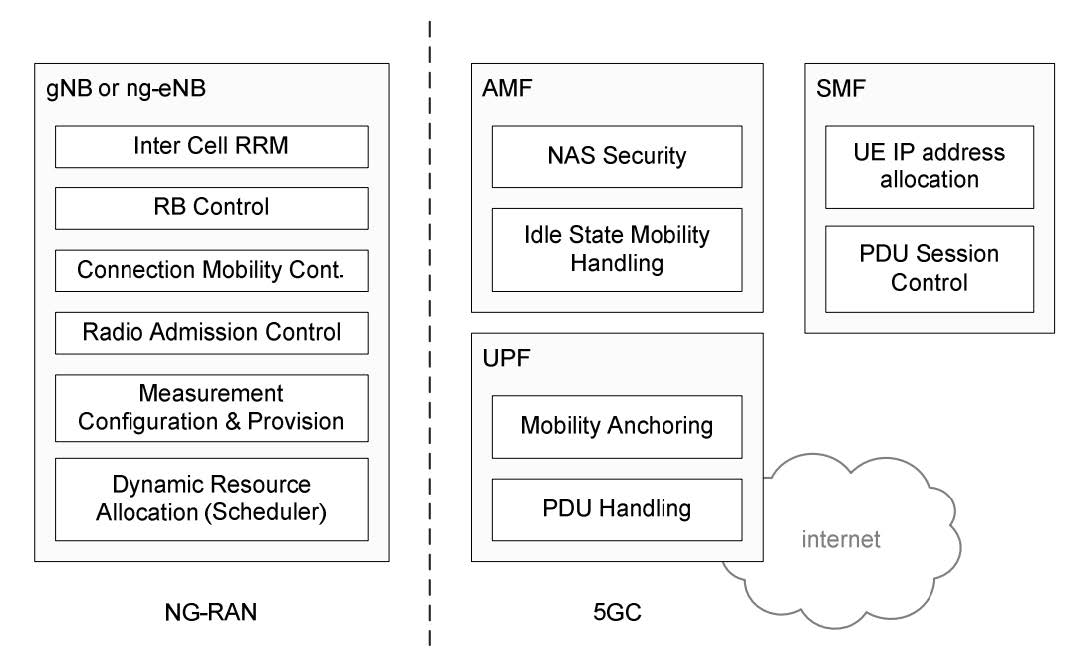
**Archittettura**

Una rete 5G è composta da un 5G Access Network (AN) e da un 5G Core Network (5GC).



**Fig. 1.13:** 5G Network Architecture

La Access Network è costituita da una una Next-generation Radio Access Network (NG-RAN), che usa la nuova interfaccia radio 5G (NR), e/o una rete non-3GPP AN, ad esempio xDSL e WiFi, che si collega al 5GC. Le diverse entità di rete sono connesse da una rete IP sottostante.



**Fig. 1.14:** Functional Split Between NG-RAN and 5GC

L’NG-RAN è formata da una serie di 5G base station, chiamate gNBs, che vengono connesse al 5GC attraverso una serie di interfacce logiche. Così come in LTE, le gNBs possono essere interconnesse attraverso l’interfaccia Xn per migliorare la mobility e le management functions.

Lo stack protocollare è uguale a quello relativo all’LTE ma differisce per la presenza del protocollo SDAP a livello utente. Le funzionalità principali sono:

* Physical layer: contiene le digital and analogue signal processing functions per l’invio e la ricezione delle informazioni. E’ basato su OFDMA, con adaptive carrier spacing delle frequenze e una modulazione adattiva (per esempio da BPSK a 256 QAM).
* MAC protocol: gestisce il controllo del physical layer a basso livello.
* RLC protocol : garantisce la consegna affidabile delle informazioni.
* PDCP: si occupa di funzioni di transporto ad alto livello relative a sicurezza e alla compressione dell’intestazioni
* SDAP: mappa l’interazione tra il pacchetto di un flusso QoS e una portante radio contrassegnando i pacchetti di dati dell’utente in maniera appropriata.
* RRC: è un protocollo di signaling usato nelle procedure che coinvolgono il mobile e il gNB. Include creazione e rilascio della connessione; la trasmissione di informazioni di sistema; la creazione, riconfigurazione e rilascio della portante radio;
* NAS protocol: è il protocollo di signaling usato tra l’ UE e il 5GC per le PDU session management, sicurezza, mobility management etc.

Mentre l’architettura NG-RAN è simile a quella relativa all’LTE, l’architettura del 5GC è innovativa per molti aspetti.

La decomposizione delle funzioni eseguita dai nodi della precedente generazione, nell’architettura 5G viene espressa in termini di Network Functions (NF).

Così come per NG-RAN si ha una separazione tra control e user plane. Nell’user plane si hanno una o più User Plane Function (UPF), che principalmente provvedono al packet forwarding tra differenti NG-U tunnel i quali formano una sessione PDU. Tutte le altre funzioni di rete vengono gestite dal control plane.

Un cambiamento rispetto alla generazione precedente è il diverso modello di interfaccia usato, che si sposta dal “bit-oriented-point-to-point” al “web-oriented service-based”. Le procedure, cioè il set di interazione tra le funzioni di rete, sono infatti definite servizi, e vengono supportate da alcuni strumenti web-oriented come ad esempio HTTP, REST e JSON.

Mentre nel modello point-to-point le interfacce collegano due entità definite, in un service-based le interfacce relative a un’entità sono delle API che le altre entità possono usare. Si ha così il vantaggio di poter aggiungere nuove entità di rete ad un set di N entità senza la necessità di creare N interfacce con i relativi protocolli. Sarà necessario dunque soltanto standardizzare le API della nuova entità.

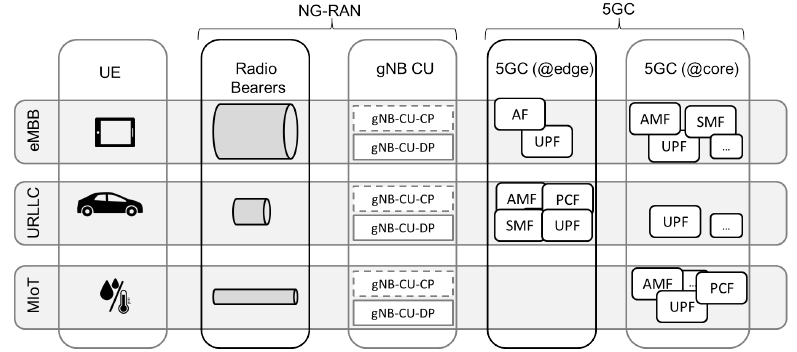
I principali ruoli delle NF sono:

* UPF gestisce il forwarding del tunnel NG-U e i relativi servizi di data path. Contiene funzionalità del 4G MME e del PGW.
* AMF gestisce il signaling proveniente e verso l’UE[[1]](#footnote-1).
* AUSF è il componente interiore del 5GC e e supporta l’autenticazione per accessi 3GPP e non-3GPP. Contiene funzionalità del 4G HSS.
* UDM può essere considerata un archivio per le informazioni relative all’UE.
* PCF controlla le funzioni del control panel, ad esempio SMF. Contiene funzionalità del 4G PCRF.
* NSSF fornisce informazioni tra cui la capacità di rete ed eventi di rete ad applicazioni di terze parti. Non è presente nel 4G.
* NRF fornisce le istanze delle NF quando gli viene effettuata una richiesta di istanza da parte di un’altra NF. Non è presente nel 4G.
* AF funge da application server che può interagire con le NF del control panel.

L’architettura basata su funzioni di rete permette la sua distribuzione tramite strumenti software e cloud. Si ha così un completo disaccoppiamento delle NF sia dall’hardware che dall’infrastruttura di rete. Ciò permette agli operatori di rete di distribuire più sezioni di rete con diverse funzionalità o per gruppi diversi di UE. Ogni sezione possiede un identificatore unico che include il tipo di sezione/servizio (SST). Gli SST standardizzati più comuni sono:

|  |  |  |
| --- | --- | --- |
| Slice/Service Type | SST value | Characteristics |
| eMMB | 1 | Per la gestione della rete mobile 5G |
| URLLC | 2 | Per la gestione dei servizi a bassa latenza |
| MIoT | 3 | Per la gestione dell’IoT massivo |

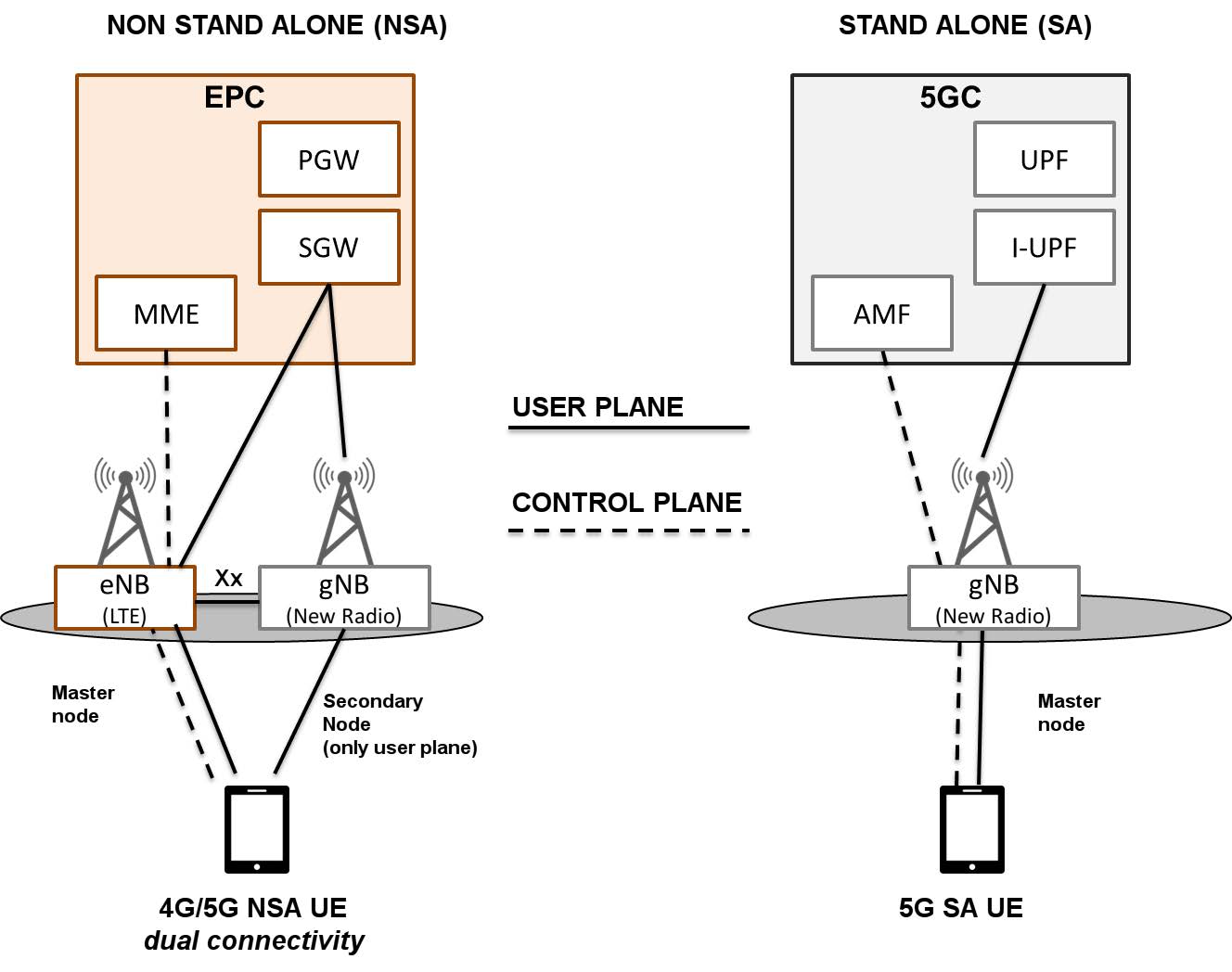
Ogni sezione differisce dall’altra per la diversa configurazione, e ciò dipende dalle vertical application che usano tale sezione. Il servizio eMMB usa portanti radio ad alta capacità e ha due UPF, uno nell’edge e l’altro nel cloud, per favorire la mobilità degli utenti. Nell’URLLC si usa una portante radio a bassa latenza e una capacità di rete media. Molte funzioni di controllo sono spostate nell’edge per ridurre la latenza. Nell’ MIoT si possono avere portanti radio a basso bit-rate e un singolo UPF, assumendo poca mobilità dei dispositivi.



**Fig. 1.15:** 5G slices

5G è progettato per funzionare con le precedenti tecnologie, specialmente con 4G. Si ha, tuttavia, un nuovo approccio di interconnessione, e ciò permetterà un rilascio più veloce del 5G.

Il completo disaccoppiamento tra radio access e core network permette il temporaneo uso del 5G radio access e il riuso del già esistente 4G Evolved Packet Core. Questa configurazione viene chiamata Non-Stand-Alone (NSA), mentre la configurazione definitiva comprendente l’uso del 5G Core è chiamata Stand Alone (SA) è sarà disponibile tra alcuni anni.



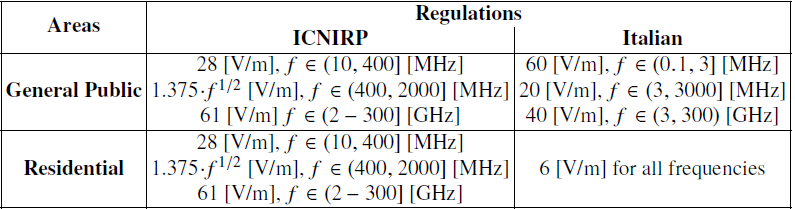
**Fig. 1.16:** 5G configuration options

**Rischi per la salute**

Il rilascio di una rete mobile di nuova generazione richiede l’installazione di una infrastruttura radio dedicata. Nel caso del 5G, si sono create delle controversie a proposito dei potenziali problemi per la salute pubblica che si possono avere con l’installazione delle nuove stazioni radio. Verranno ora presentate le principali questioni:

*Collegamento tra insorgenza di tumori e l’esposizione ai campi elettromagnetici (EMFs) generati dal 5G*

Il fatto che elevati livelli di EMFs provochino danni alla salute è provato da numerose pubblicazioni scientifiche. Proprio per questa ragione esistono delle regolamentazioni che indicano il quantitativo massimo di EMFs a cui i cittadini possono essere esposti in luoghi pubblici. Osservando i limiti previsti in Italia si nota che essi sono più restrittivi rispetto a quelli forniti dal ICNIRP[[2]](#footnote-2).



Una differenza importante è la distinzione tra spazi residenziali e spazi pubblici generici, cioè quelle aree dove i cittadini non risiedono per molto tempo. Inoltre molte città, come ad esempio Roma impongono delle limitazioni aggiuntive sulla posizione delle stazioni radio.

Il fatto che l’Italia abbia dei limiti più severi di quelli imposti dal ICINRP, i quali sono già abbastanza restrittivi, deriva dal fine di prevenire impatti sulla salute umana ancora sconosciuti.

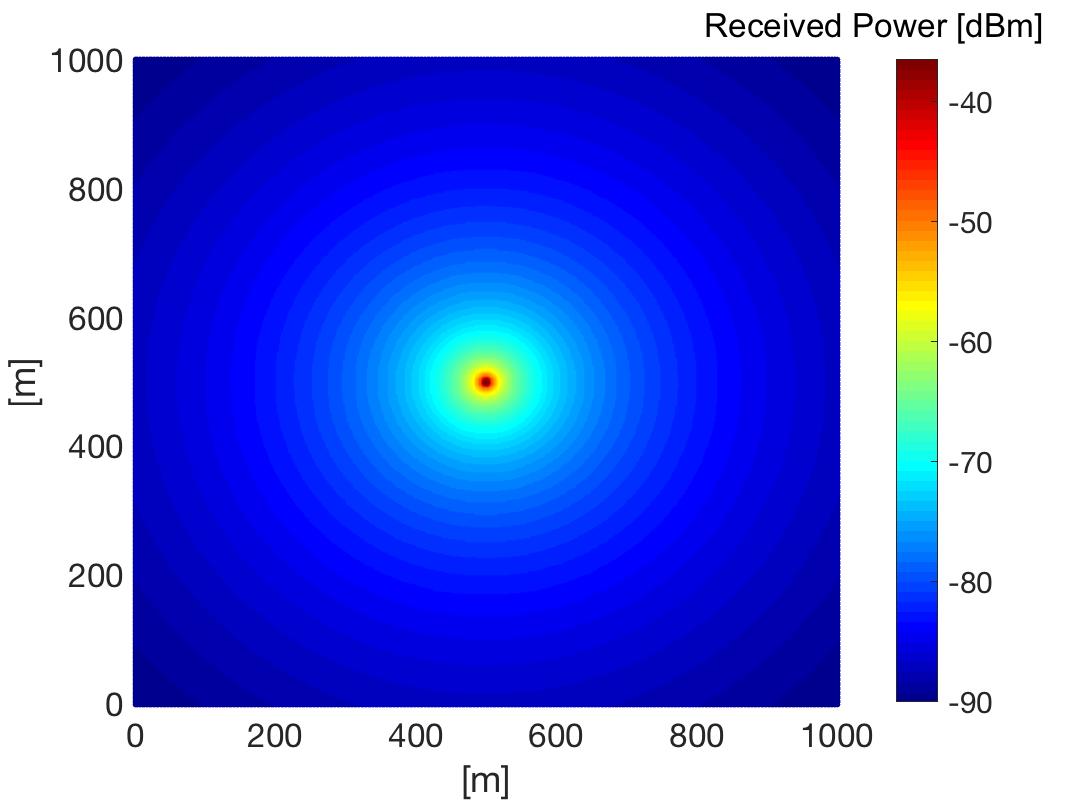
*Aumento dei livelli dei EMFs associato all’installazione di un elevato numero di stazioni radio 5G*

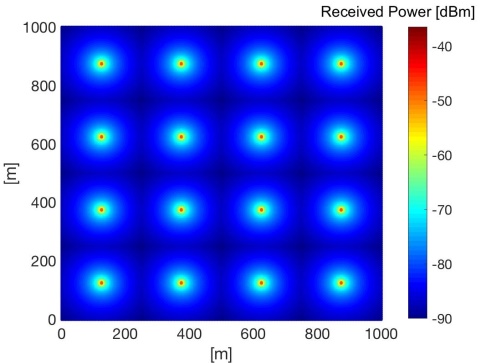
Contrariamente a quanto si crede, nel momento in cui in una porzione di territorio vengono installate una serie di stazioni radio 5G, viene ridotta la potenza di trasmissione di ciascuna antenna. Considerando uno scenario in cui un operatore vuole garantire in ogni porzione del territorio una potenza di ricezione minima . Definendo la potenza ricevuta , l’operatore dovrà garantire > . dipenderà dalla potenza emessa da ciascuna stazione radio e dall’attenuazione delle onde elettromagnetiche nell’aria. Considerando che la potenza di diminuisce con la distanza elevata a un coefficiente di attenuazione si ha:

Si ricava allora:

Dove rappresenta la distanza massima di copertura di una stazione radio. Si considerino adesso due modelli in cui nel primo si hanno un minor numero di stazioni radio rispetto al secondo. Allora per la premessa fatta inizialmente, cioè quella di ridurre la potenza di emissione di ciascuna stazione radio, si ha che (2) < (1). Definendo allora come il rapporto tra (2) e (1) si trova che:

Si ricava quindi che quando il numero di stazioni radio viene incrementato, la potenza emessa di ciascuna viene diminuita di un fattore .





1 base station

16 base station

**Fig. 1.16:** Power radiated over the territory for different number of base station in dBm scale.

*Le stazioni radio 5G useranno le frequenze mm-Wave, ritenute pericolose*

La tecnologia 5G lavora su tre range di frequenze: 700MHz (sub-GHz), 3700MHz (sub-6GHz) e 26GHz (mm-Wave). Attualmente la frequenza 3700MHz viene usata dalle reti 2G/3G/4G mentre la frequenza 700MHz è usata dalle trasmissioni TV.

Le mm-Wave verranno usate solo per dei servizi di nicchia nel 5G, infatti la maggior parte del traffico sarà presente nelle frequenze che vengono giù usate dalle precedenti tecnologie.

Il loro poco utilizzo è dovuto soprattutto dalla presenza di molta attenuazione quando si è in presenza di ostacoli, e ciò si riflette in una bassa copertura.

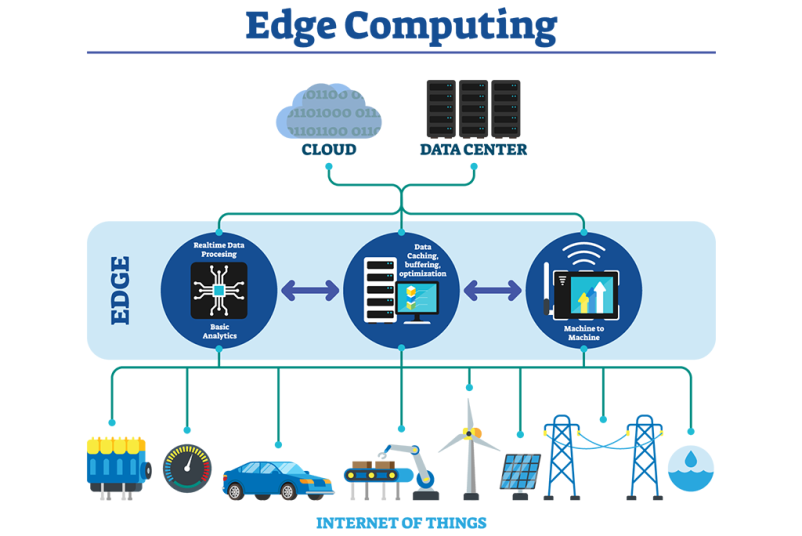
Per quanto riguarda l’impatto sulla salute ci sono degli studi a riguardo i quali affermano che alti livelli di EMFs prodotti dalle mm-Wave coinvolgono soltanto la pelle, e non i tessuti interni, a causa delle deboli proprietà di penetrazione di tali frequenze. Tali effetti vengono comunque eliminati se si considerano bassi livelli di EMFs.

### **1.3 Data Layer**

In una città dotata sempre più di sensori e hardware di nuova generazione si rende necessaria una grande potenza di elaborazione dati. E’ allora indispensabile avere una buona infrastruttura, ricca di datacenter, i quali permettono di raccogliere tutti i dati prodotti da gli elementi smart di una città, quali semafori, lampioni, parcheggi, centrali elettriche, di elaborarli velocemente e di consegnarli in tempo reale. Allora, pur restando parte fondamentale dell’infrastruttura i tradizionali datacenter centralizzati, quelli decentralizzati più piccoli e distribuiti su un’intera area urbana saranno un complemento essenziale per la potenza di elaborazione di una smart city.

In particolare, le città più piccole beneficeranno in genere di più data center periferici per consentire alle aziende di raggiungere meglio gli utenti attraverso una latenza minima.

Per evitare il collasso dell’infrastruttura dovuto alla grandissima mole di dati che richiedono una successiva elaborazione, l’Edge Computing sarà sicuramente una soluzione da considerare. Con tale termine, infatti, ci si riferisce all’elaborazione delle informazioni ai margini della rete, cioè dove i dati vengono prodotti. I benefici principali derivanti dall'utilizzo di queste tecnologie sono la riduzione della [latenza](https://it.wikipedia.org/wiki/Latenza) di elaborazione, che permette risposte in tempo reale, e il risparmio di [banda](https://it.wikipedia.org/wiki/Banda_(informatica)) poiché verranno inviate al [data center](https://it.wikipedia.org/wiki/Data_center) informazioni già elaborate.

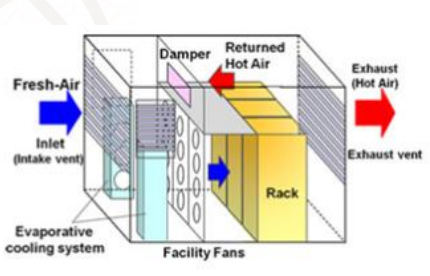


**Fig. 1.5:** Edge Computing

L’aumento dei data center provocherà un maggior consumo elettrico quindi devono essere trovate delle soluzioni che permettano di ridurre il loro impatto ambientale.

Una prima soluzione potrebbe essere quella di migliorare l’efficienza del server, un’altra, invece, quella di trovare fonti di energia alternative. I nuovi progressi nel raffreddamento a liquido e nell’analisi predittiva aiuteranno inoltre i data center a consumare energia in modo più efficiente, riducendo il loro impatto complessivo sull’infrastruttura e migliorandone le prestazioni.

A tal proposito nel “ITU-T Recommendation L-1300”, pubblicato dal FG-SSC, viene illustrato un nuovo progetto di data center che ne prevede una disposizione in un ambiente esterno al fine di ridurne il consumo elettrico dovuto dall’impianto di raffreddamento.



**Fig. 1.6:** Schematic of prototype container-type data center

I dati viaggiano dai dispositivi, attraverso l’infrastruttura, ai datacenter tramite protocolli di trasferimento dati. Due tra i più importanti sono IP ed Ethernet.

- IP: è il protocollo principale del livello 3 dell’architettura TCP/IP. Le sue caratteristiche principali sono la non affidabilità e l’invio dei dati senza l’instaurazione di una connessione. L’inaffidabilità è data dal fatto che il pacchetto inviato può essere perso, duplicato o consegnato fuori sequenza. Sarà compito di altri protocolli appartenenti ad altri livelli provvedere alla correzione degli errori o al rinvio dei dati. La non instaurazione di una connessione fa si che ogni pacchetto venga trattato in maniera indipendente dagli altri, infatti pacchetti diversi aventi stesso mittente e stesso destinatario possono seguire percorsi diversi, e ciò dipende dall’attuale stato della rete.

Attualmente, lo standard è rappresentato dal protocolli IP versione 4 (IPv4), ma dal 1995 è stata proposta una nuova versione del protocollo nota come versione 6 (IPv6). Il sempre maggior numero di dispositivi connessi ad una rete, in previsione di una città sempre più ricca di servizi, rende indispensabile il passaggio al nuovo protocollo.

Esso risolve infatti il numero ormai insufficiente di indirizzi IP disponibili, i quali identificano ogni dispositivo connesso ad una rete, che passano da 232 (IPv4) a 2128 (IPv6).

Inoltre permette di gestire il traffico in modo best-effort, cioè permette di assegnare ai pacchetti delle classi di servizio a cui saranno associate delle certe priorità.

Infine l’IPv6 rende più sicuro il servizio, infatti col nuovo protocollo verranno rese standard e disponibili alcune primitive per l’autenticazione e la cifratura dei dati.

Nonostante questi vantaggi, il protocollo Ipv6 è ancora poco diffuso, e questo perché una completa migrazione al nuovo protocollo constringerebbe a modificare fortemenete gli apparati di rete esistenti.

Esistono tuttavia delle “isole” in cui il protocollo Ipv6 viene usato, e la tecnica più usata per far fronte all’incopatibilità tra le reti Ipv4 e Ipv6 è quella del Tunneling. Con questa tecnica quando si stabilisce un collegamento point to point tra due host i pacchetti IPv6 vengono incapsulati dall'host sorgente in pacchetto IPv4, inviati nel tunnel e, una volta giunti a destinazione, vengono decapsuati dall'host che li tratta come se fossero comunissimi pacchetti IPv4.

- Ethernet: è una suite di protocolli originariamente sviluppati per realizzare LAN (Local Area Network) ed è ufficialmente standardizzata da IEEE con la serie di specifiche denominate IEEE 802.3.

Mentre in origine il data rate era di 10Mbit/s successive standardizzazioni hanno indrodotto:

- Ethernet 100Mbit/s (Fast Ethernet)

- Ethernet a 1Gbit/s (Gigabit Ethernet)

- Ethernet a 10Gbit/s.

Per i diversi bit rate, il protocollo Ethernet ha standardizzato soluzioni sia in rame che in fibra, tuttavia per Gigabit Ethernet la soluzione in fibra è di gran lunga la più utilizzata.

Sia per Fast Ethernet che per Gigabit Ethernet, si hanno due modalità operative:

- Full duplex: la connessione avviene tra due switch, le porte sono dotate di buffer e le collisioni non sono possibili, quindi non viene utilizzato CSMA/CD ( accesso multiplo tramite rilevamento della portante con rilevamento delle collisioni).

- Half duplex: viene usata per connessioni tramite hub, quindi essendoci possibilità di collisione è richiesto l’uso di CSMA/CD per prevenire i conflitti di trasmissione.

### **1.4 Security System**

In una Smart City è necessario che il trasferimento dei dati avvenga in maniera sicura, affidabile, tuttavia la grande complessità dell’infrastruttura, il gran numero dei dispositivi connessi e la grande mole di dati scambiati creano vulnerabilità nel sistema.

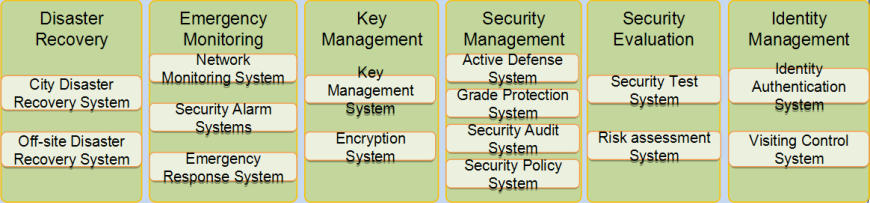
Col termine vulnerabilità ci si riferisce in genere a diversi tipi di problemi:

- Attacchi da parte di malintenzionati: le motivazioni sono molteplici e includono guadagno economico, industrial espionage, cyber-warfare, cyber-sabotage.

- Malfunzionamenti casuali.

- Catastrofi naturali.

L’infrastruttura riguardante la sicurezza informatica in una Smart City costituisce la base dell’intero sistema e consiste di un gran numero di funzioni, tra cui disaster recovery, gestione delle chiavi di sicurezza, identity management e valutazione della sicurezza.



**Fig. 1.7:** Information Security Infrastructure

Il “Technical Report on Cyber-Security, Data Protection and Cyber-Resilience in Smart Sustainable Cities”, redatto dal FG-SSC elenca delle possibili soluzioni da adottare al fine di garantire la continuità di tutti i servizi presenti in una Smart City.

- Protezione proattiva delle informazioni: consiste nella protezione continuata degli endpoint, dei server interni e nell’implementazione di servizi di backup e recupero dati che permettano di garantire la recuperabilità completa dei dati in caso di incidenti.

- Autenticazione utenti: forti regole di autenticazione permettono alle organizzazioni di proteggere i propri dati verificando l’identità di uno smart device, sistema o applicazione. Ciò previene il collegamento di dispositivi non autorizzati all’infrastruttura.

- CERT (Computer Emergency Response Team): Ogni Smart City dovrebbe far affidamento ai propri CERT nazionali, cioè organizzazioni finanziate generalmente da Enti Governativi, incaricate di raccogliere informazioni a proposito di incidenti informatici su larga scala e di fornire informazioni tempestive su potenziali minacce informatiche che possono recare danno a imprese e cittadini.

- Controllo degli accessi ai confini della rete: controllando tutti gli accessi nella rete esterna si può isolare la rete interna da eventuali attacchi. E’ richiesto l’utilizzo di un firewall, cioè un dispositivo per la sicurezza informatica che permette di monitorare il traffico in ingresso e in uscita utilizzando una serie predefinita di regole di sicurezza per consentire o bloccare gli accessi, e che in caso di azioni sospette può generare l’allarme e fornire informazioni dettagliate per la successiva analisi.

Prevenzione dagli attacchi DDoS (distributed denial-of-service attaccks): un attacco DDoS consiste nell’invio di un grande numero di pacchetti di richieste ad un server, da parte di numerose macchine, costituenti una botnet, al fine di saturarne le risorse e rendenderlo instabile.

Le misure atte a contrastare tale attacco prevedono l’aggiornamento dell’infrastruttura di rete al fine di rendere disponibile una grande larghezza di banda, l’aggiornamento dell’hardware di ciascun server, e l’installazione di un firewall specializzato anti-DDoS.

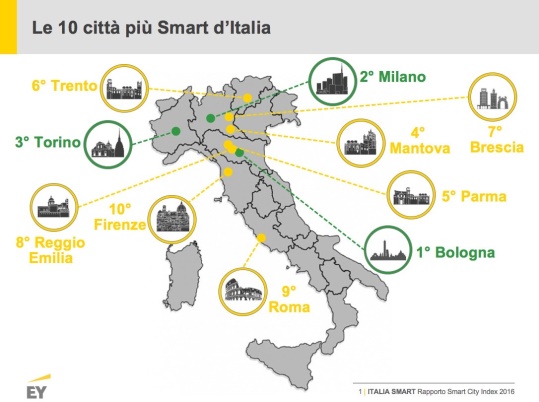
## 1.1 Smart City in Italia

Un quadro dell’italia in ambito Smart City viene offerto da rapporto Smart City Index, di EY, società di consulenza mondiale, la quale ha analizzato le 116 città capoluogo italiane utilizzando oltre 470 indicatori.

Quello che si nota è una grandissima differenza di sviluppo tra nord e sud, infatti le città di Sardegna e Sicilia si classificano tutte, ad eccezione di Palermo, nella terza fascia dell’Indice, mentre delle città del sud solo Napoli si trova in prima fascia, e Cosenza e Lecce sono le uniche a non classificarsi in terza fascia.

Segnali positivi si registrano al centro con città quali Firenze che si trova tra le prime 10, e Bologna, città con il maggior tasso di archiviazione di big data con oltre 1000 data set pubblicati.

La maggior parte dei capoluoghi del Nord Italia è distribuita nelle prime cinquanta posizioni. Il litorale romagnolo, per esempio è considerato il più connesso d’Italiam con più di 50Km di spiagge coperte dal servizio Wi-Fi, Milano costituisce l’80% del mercato di sharing mobility in Italia e Brescia ha il teleriscaldamento disponibile per il 70% degli edifici cittadini.



**Fig. 1.2:** Rapporto Smart City Index 2016.

L’uso dell’ICT e dell’IoT per gestire e coordinare efficacemente le risorse della città viene definito Smart City.

## 1.3 Mobilità e Trasporti

Le soluzioni riguardanti la mobilità e i trasporti sono molteplici ed hanno come obbiettivo soprattutto quello di ridurre l’inquinamento.

In Europa, città molto attive sono per esempio Barcellona, Lione, Manchester, Monaco, Nottingham e le soluzioni più adottate sono:

* Car sharing, in particolare tramite l’utilizzo di veicoli elettrici
* Costruzione dell’infastruttura per favorire l’e-mobility, per esempio l’integrazione di stazioni di ricarica con l’illuminazione pubblica e la costruzione di green parking.
* Test sulla guida autonoma
* Costruzione centri per la consegna merci tramite veicoli elettrici
* Riduzione del traffico tramite l’intervento sui cicli semaforici per gestire la circolazione delle automobili in modo dinamico.

# Capitolo 2

# Titolo

Different strategies have been proposed to describe the working principle of IPMC transducers and efforts have been made to move from black box models toward first principle ones, the rationale being that black box models, obtained on the basis of experimental observations, cannot easily be extended to other devices. First principle models, on the other hand, are generally either too complex to be used in practical applications or too simple to guarantee sufficiently accurate predictions.

.....

.....

The model of the IPMC actuator has been divided into two stages as shown in the block scheme in Figure 2.1.

|  |
| --- |
| fig2_1 |
| **Fig. 2.1:** La didascalia va giustificata allineata a sinistra e giustificata a destra se è più lunga di un rigo, altrimenti va centrata. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | (a) | (b) | | **Fig. 3.13:** Questa è una figura composta fatta da una prima (a); e una seconda parte (b). | | |

Tab. IV è un esembio di tabella:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | |  |  [Kg/m3] |  [Pa s] | | Air | 1 | 0.0001 | | Synthetic fluid | 200 | 0.0002 | | Deionized water | 997 | 0.0008 | | Sea water | 103 | 0.0018 | | Human blood | 1125 | 0.00 | |
| **Tab. IV.** Density and viscosity values of the fluids analyzed in Figure 17. |

|  |  |
| --- | --- |
| (a) |  |
| (b) |
| **Fig. 4.15.** Le misure debbono sempre avere sugli assi le grandezze e le unità di misura corrispondenti. | |

# 

# Conclusioni

In questo elaborato....

**Bibliografia e Sitografia**

*Il sistema radar,* Ciro Cafforio, <http://telematics.poliba.it/images/file/grieco/fondamenti-tlc/dispenseCE.pdf>

Akan, Ozgur & Arik, Muharrem. (2020). *Internet of Radars (IoR): Internet of RAdio Detectors And Rangers.*

A. Hassanien, M. G. Amin, E. Aboutanios and B. Himed, "*Dual-Function Radar Communication Systems: A Solution to the Spectrum Congestion Problem*," in *IEEE Signal Processing Magazine*, vol. 36, no. 5, pp. 115-126, Sept. 2019.

Mishra, Kumar Vijay & Mysore, Bhavani Shankar & Koivunen, Visa & Vorobyov, Sergiy. (2019). *Toward Millimeter Wave Joint Radar-Communications: A Signal Processing Perspective*.

Roberts, C. M. (2006). *Radio frequency identification (RFID). Computers & security*, 25(1), 18-26.

Chellappa, Muthu & Madasamy, Shanmugaraj & Prabakaran, R.. (2011). *Study on ZigBee technology*. 297-301. 10.1109/ICECTECH.2011.5942102.

Kranenburg, Rob & Bassi, Alex. (2012). IoT Challenges. Communications in Mobile Computing. 1. 10.1186/2192-1121-1-9.

Istituto di Calcolo e Reti ad Alte Prestazioni, *Smart Object e forme di cooperazione,*<https://intranet.icar.cnr.it/wp-content/uploads/2016/12/RT-ICAR-CS-14-01.pdf>

Borzycki, Krzysztof. (2018). *FTTx Access Networks: Technical Developments and Standardization*. 10.5772/intechopen.71785.

1. UE: Dispositivo usato da un end-user per comunicare. [↑](#footnote-ref-1)
2. ICNIRP: organismo non governativo che si occupa di ricerca sul tema dei possibili effetti nocivi sul corpo umano dell’esposizione a radiazioni non ionizzanti [↑](#footnote-ref-2)