Hardware, Electromagnetic and Localization Security

Pierciro Caliandro

9 marzo 2022

Capitolo 1

Introduzione

1.1 Introduzione

Attacco fisico invece di informatico, viene applicato un attacco di tipo EM: si mandano segnali fisici su un apparato per indurre malfunzionamento o rubare dati.
Si arriva all'impatto sull'elettronica, si cerca quindi di ottenere dei rudimenti di sicurezza fisica: 3 aspetti di livello diverso, dal sistema, alla parte di comunicazione alla parte elettronica.
Aspetti fondamentali:
- short range vulnerabilities: dispositivi medici avranno tutte funzionalità wireless: pacemakers va configurato, quindi in base alla risposta configura il dispositivo con un accoppiamento di tipo NFC, in futuro anche le protesi più "sciocche" come una placca per le ossa saranno wireless, sarà funzionalizzato con diversi sensori per verificare infezioni etc... ed essere letto da fuori.
Qualunque oggetto impiantato sarà funzionalizzato, a seguito di interventi di qualunque tipo (punti di sutura etc...) che sarà provvisto di sensori.
È tutto vittima di attacco informatico, per rubare dati in maniera non intenzionale.
Il corpo diventa quindi un nodo di Internet, si parla di **Internet of the bodies**, ci possono essere diversi tipi di sensori che interagiscono.C'è una lista svariata di oggetti di medica che controllano le attività fisiche.
L'accesso non intenzionale al dispositivo ha un impatto potenzilamente dirompente, lo scenario va a parare in una medicina guidata dai dati dove si mischiano diverse discipline, è il concetto di **medicina di precisione**: parte dalle terapie oncologiche, in ingegneria è la capacità della medicina di apprendere. Se la terapia oggi va bene, il corpo umano cambia e quindi tale terapia può necessitare di essere aggiornata.
Il punto critico è che per rendere questa visione operabile, occorre avere sistemi pervasivi + AI per poter poi tirare fuori una cura.
È una medicina assistiva che può essere integrata con sensori nella casa che controllano l'utente paziente, si parla di 3 tipi di dispositivi, ci interessa capire come questi comunicano e non il loro funzionamento:

- wearable
- epidermici
- implantable

che devono avere la safety by design, quindi non devono fare male quando indossati, la security by design e quindi essere sicuri da progettazione e poi la privacy by design, quindi capire come è possibile che i dati vengano usati impropriamente.
Abbiamo ad esempio strumenti epidermici che rilascia cortisolo quando ad esempio viene misurato

da un sensore che scende sotto soglia una certa misura.
Ci sono quindi 3 tipi di links:

- on-body link
- through-the-body
- off-the-body

Analizzeremo tutto a livello di modello fisico-matematico.
Ci sono poi problemi per quanto riguarda la lettura dei dati, qui c'è la corrispondenza fisica di come si leggono tali dati, ma c'è anche il come si fa per accedere al dispositivo, ad esempio ci sono delle micro-antenne non volute.

1.1.1 Introduzione generale sulla cybersecurity

Si completa il concetto di cybersecurity con gli aspetti fisici e di comunicazione, vi sono delle criticità nelle comunicazioni sulla rete. Ce ne sono però alcune che non vengono prese in considerazione spesso, che è opportuno non tralasciare come appunto la comunicazione a corto raggio: si viaggia in ambienti affollati per rubare dati da cellulari ad esempio se è abilitato il sistema NFC. Normalmente la distanza è dell'ordine del metro, ma su un posto affollato è fattibile, il lettore viene posto vicino al cellulare e ruba dati.
Per le reti ad ampio raggio, ci sarà la sicurezza delle reti da cui però rimangono fuori tutta una serie di apparati che sono ad esempio i sistemi di localizzazione. Ormai quasi tutte le applicazioni usano la posizione per fare delle operazioni, usano EMF per portare dati e sono attaccabili: è "facile" far credere ad un device di trovarsi in un luogo anzi che in un altro.
È stato dimostrato che era possibile controllare uno yatch di lusso semplicemente ingannando il sistema di navigazione, ad esempio.È ancora più semplice inibire i servizi, quindi fare in modo che il servizio non funzioni e basta, un'altra applicazione è quella di sfruttare le EMF usate nei radar per capire dove si trova qualche oggetto, quindi disturbare un radar vuol dire interrompere il funzionamento di un sistema target a bassi rischi.
Cerchiamo quindi di capire come disturbare o difendere un sistema di navigazione o un radar, per cercare di capire come proteggerli nel mondo reale.
Entreremo poi nell'hardware, vedendo vari metodi su come attaccare l'hardware stesso: anche qui, si da per acquisito che il chip sia sicuro in quanto non si può aprire ed occorre per forza passare per il software, ma in realtà negli anni vi sono stati una serie di side channel, come ad esempio isolare termicamente un device.
Ma se si può monitorare la temperatura del device, è possibile capire che elaborazioni sta facendo e quindi capire le attività dell'utente, questo vale anche per le RAM etc... ad esempio vedere quanto sono frequenti le rotture delle singole celle della RAM etc...

1.1.2 Sicurezza informatica e cybersecurity

È un concetto molto ampio, spesso confuso con la cybersecurity, ma la prima vuol dire mantenere in sicurezza l'informazione anche se non è digitale. Non basta quindi proteggersi da attacchi via rete, il concetto è molto più ampio della cybersceurity. Ci sono tantissime definizioni standard per cybersecurity, ma è meglio partire da un approccio che vede il sistema moderno come formato da tante entità, che possiamo dividere in 3 parti:

- hardware, che non è per forza l'hardware del calcolatore, anche un banale pezzo di carta con su scritta una password.

- software, l'hardware visto da un punto di vista informatico è correlato con programmi applicativi che possono avere delle debolezze, occorre quindi anche proteggere l'interno della macchina

- parte di comunicazione, in quanto il mondo moderno di IoT o cloud prevede che l'informazione viaggi fra utente e server o fra vari utenti

La maggior parte delle informazioni continuano a mandare informazioni a qualche server chissà dove (magari in CINA **cit**), in questo modo ci sono diverse facilitazioni.

Questo vuol dire aver venduto parte della privacy a qualcuno o comunque delegato, che non è detto che sia malvagio ma c'è una comunicazione che avviene continuamente e quindi potrebbe interessare a qualcun altro per intervenire sul canale di comunicazione ed entrare in casa.
Questo rimanendo ancora nell'accezione più classica della comunicazione, ma abbiamo anche comunicazione a livello di corto raggio, quindi per gestire queste 3 componenti principali occorre mettere in atto tutta una serie di contromisure che non sono solo quelle che vederemo ma sono molto più ampie:
- procedure di autenticazione, come il controllo di accessi in un edificio, ci possono essere informazioni che vengono classificate come sensibili ed a cui non si può accedere (es. badge per accedere a determinati uffici). Già questo aspetto se ben fatto sarebbe una grossa protezione, soprattutto per software ed hardware security in quanto vorrebbe dire avere degli alti livelli di sicurezza - sicurezza a livelli più bassi, CIA: Confidentiality, Availability and Integrity. Devono valere questi 3 principi nell'information security: - C è un concetto diverso dalla privacy, sta proprio nel non rivelare l'informazione che non dovrebbe essere nota. - I, ovvero la capacità del sistema di non perdere le informazioni che può essere accidentale o anche dovuta ad attacchi, esempi come i ransomware possono portare ad avere dei costi. Ci sono anche altre tipi di compromissione di integrità, che riguardano ad esempio il disturbo di un segnale riguardo la posizione - A, il fatto che l'informazione sia integra non vuol dire che possa essere utilizzata.Ad esempio se si perde la password per accedere a determinati dati, mantenerle ha un suo costo

Vedremo come declinare queste 3 caratteristiche nei casi di studio del corso.

Ci sono delle definizioni da dare:

- vulnerabilità: sfruttate dall'attaccantte, qualsiasi sistema ha una debolezza da qualche parte nella sua progettazione. Se può essere sfruttata per ridurre una delle 3 cose, possiamo chiamare tale debolezza una vulneraiblità

- un cyber attacco sfrutta la vulnerabilità per ridurre la sicurezza.

  Più comuni tecniche di attacco:

- backdoor: vie lasciate aperte dagli sviluppatori, come porte aperte etc...

- DoS: negazione del servizio, si fa in modo che per qualche motivo il servizio sotto attacco divenga indisponibile, come ad esempio richieste di accesso ad un server molteplici volte. Nella parte wireless è molto usato, mediante il **jammer**: è un sistema che trasmette con la massima potenza possibile sul canale usato dal sistema per comunicare, che disturba la comunicazione fino a negare il canale per comunicare. È una tecnologia banale per effettuare DoS

- attacchi ad accesso diretto non autorizzato.

- eavesedropping, dove si ascolta e se ci sono delle informazioni riservate si possono captare. Esempio: canale della DSB, ogni aereo mette la posizione, è un canale in chiaro e quindi ascoltare ed usare quei dati in modo malevolo può creare problemi.
- phishing
- privilege escalation
- social engineering
- reverse engineering
- side channel attack: verificare dei canali correlate con l'informazione da difendere o attaccare, per capire cosa sta succedendo.
- spoofing: attacco che tende a confondere la persona o entità sotto attacco mediante l'invio di falsi dati. Si presta bene alla comunicazione wireless, molto usato nei sistemi di localizzaizone tipo GPS peché è noto a tutti come è standardizato il segnale che arriva al satellite e quindi si può ricostruire e trasmettere. Ma quando lo si ricostruisce si inseriscono delle false informazioni, per far ad esempio cambiare posizione al GPS.
- tampering: alterazione fisica del dispositivo
- malware

È importante inoltre ribadire la differenza fra sicurezza intesa come - safety: concetto che esprime la capacità di mettersi ala riparo da accadimenti dannosi per l'uomo e per la vita umana. Ad esempio la precipitazione dell'aereo, mantenere tale proprietà occorre salvaguardarsi da qualsiasi cosa può accadere. Ad esempio, un aereo può precipitare perché il sistema di comunicazione si danneggia o interferisce con un altro - security: la security è correlata, ma non è sovrapposta bensì è come "un ombrello" che permette di mantenere la safety.
Se installiamo un sistema di sicurezza in casa, veniamo protetti da chi vuole entrare, ma non dal fatto di poter cadere e battere la testa scivolando nella vasca (**super cit**.

Ci occuperemo della security, ma molte delle cose che vederemo possono o non possono essere usate anche per garantire la safety.
È inoltre importante tenere a mente che ormai l'ambiente è pieno di EMF, quindi lo spettro EM è molto pieno e quindi aggiungere qualche altra fonte diventa semplice, quindi vedremo questa cosa.

Parte I

Parte Electromagnetic

Capitolo 2

Lezione 2

2.1 Interazione elettromagnetica col corpo umano

Cosa accade quando una onda EM interagisce col corpo umano: occorre sapere cosa succede perché quando un dispositivo deve essere immesso nel mercato deve garantire la safety: vincolo sulla potenza che rilascia nel corpo umano. È un vincolo di progetto, occorre capire cosa si intende per potenza che entra nel corpo umano, occorre anche sapere che succede quando un dispositivo riceve un'onda EM per non far funzionare il dispositivo.
Quando un onda investe il corpo umano, abbiamo un'onda elettrica ed una magnetica che investono il corpo umano e quindi 3 fenomeni:

- propagazione
- riscaldamento, dovuto all'assorbimento di potenza
- effetti chimico-fisici

Ci interessa come punto fondamentale la propagazione, il riscaldamento è un effetto. In altri contesti, l'obiettivo è scaldare il corpo (come nella fisioterapia), ma comunque occorre capire anche cosa accade perché l'assorbimento di potenza produce dei vincoli che occorre tenere conto.
Questi fenomeni sono legati a:

- materiale
- frequenza: cambierà in base a che tipo di oggetto sta irradiando, come sono fatti i tessuti etc...

Tipicamente,l'esposizione del campo sul corpo produce delle correnti, quando consideriamo l'interazione col corpo umano abbiamo 4 tipi di correnti:

- correnti di conduzione: sono legate alla presenza di elettroni liberi, ad esempio se ci sono dei fluidi.
  Gli elettroni, quando si applica un campo E, tenderanno a muoversi in una determinata direzione secondo la **legge di Ohm**:
  $$\underline{J} = \sigma \cdot \underline{E} \tag{2.1}$$
- correnti di convezione: dovuti alla deriva di ioni. Gli ioni in alcuni casi possono essere disciolti in fluidi corporei (sangue etc...) quindi anche in questo caso s'è c'è un campo le particelle possono spostarsi
- corrente di polarizzazione: la più dominante, legata alla presenza di composti polari, come l'acqua. Tali composti possono oscillare rispetto a posizioni di equilibrio, quindi subiscono una sollecitazione dovuta ad un campo incidente.

- corrente di spostamento:
$$\underline{J_s} = \frac{d\underline{D}}{dt} \Leftrightarrow j\omega D = j\omega\epsilon E \tag{2.2}$$
è quella che ci piace per comunicare con il corpo umano, le altre sono non volute.
Teniamo conto dei fenomeni introducendo una costante dielettrica complessa, è:
$$\dot{\epsilon} = \epsilon' - j\epsilon'' - j\frac{\sigma}{\omega} \tag{2.3}$$
, che deriva dalla
$$\Delta x\underline{H} = j\omega\dot{\epsilon}\underline{E} + \underline{J_0} \tag{2.4}$$
dove j0 è la sorgente (appunti):
  - i termini in j rappresentano la dissipazione
  - i termini reali rappresentano sia accumulo che propagazione di energia.

Abbiamo che
$$\epsilon' = \epsilon_0\epsilon_r \tag{2.5}$$
dove ϵ_0 ed ϵ_r sono relativamente costante dielettrica nel vuoto e costante dielettrica relativa, mentre ϵ'' è legata alla dissipazione dei materiali non per la legge di Ohm.
Invece σ ($[\frac{S}{m}]$) è legata legge di Ohm. Nei dielettrici, la dissipazione per effetto Joule non è quella dominante, abbiamo che $\epsilon'' > \frac{\sigma}{\omega}$ (nel corpo umano), quindi possiamo trascurare il termine.
Introduciamo quindi una conducibilità elettrica equivalente
$$\sigma = \epsilon'' \cdot \omega \tag{2.6}$$
$\sigma = \epsilon'' \cdot \omega$, così che ω sia l'inverso ed
$$\dot{\epsilon} = \epsilon' - j\frac{\sigma}{\omega} \tag{2.7}$$
quindi avremo, quando lavoriamo con i tessuti una
$$\bar{\epsilon} = \epsilon_0\epsilon_r - j\frac{\sigma}{\omega} \tag{2.8}$$
Un altro termine importante è la tangente di delta:
$$tan\delta = \frac{\epsilon''}{\epsilon'} = \frac{\sigma}{\omega\epsilon''} = \frac{\sigma}{\omega\epsilon_0\epsilon_r} \tag{2.9}$$
dove, l'ordine di grandezza del tanδ è:

- nel caso di buoni materiali, per fare ad esempio un antenna che irradi bene e scaldi poco, il tanδ deve essere dell'ordine di 10^{-3}
- nel corpo umano abbiamo un ordine di 10^{-1}, quindi non è buono per stabilire una comunicazione.

La complicazione è che il corpo umano non è omogeneo, quindi le costanti cambiano in quanto dipendono dal punto, poi c'è anche la dipendenza dalla frequenza che fa si che l'andamento possa essere molto dipendente dalla frequenza.

2.1.1 Corrente di polarizzazione

È quella dominante, il materiale umano è vincolato, quindi per gli elettroni non c'è movimento libero ma saranno comunque distorti dal campo.
Abbiamo 3 tipologie:

- polarizzazione dipolare
- polarizzazione molecolare-ionica
- polarizzazione elettronica

Polarizzazione dipolare Ci sono alcuni materiali, come l'acqua, che pur essendo elettricamente neutri, hanno una zona positiva ed una negativa. Possiamo immaginare di avere un'addensamento di cariche positive da una parte e di cariche negative da un altra, quindi avremo due cariche Q e $-Q$ a distanza l, quindi abbiamo un dipolo fisico-chimico con associato un momento di dipolo

$$dp = lQ \tag{2.10}$$

È quindi una piccola antennina sensibile ai campi che vi di applicano. Tali molecole sono, per quanto neutre, orientate a caso ma se si applica un campo elettrico E questo tenderà ad allineare tutte queste molecole, in direzione del campo stesso, come mostrato in figura

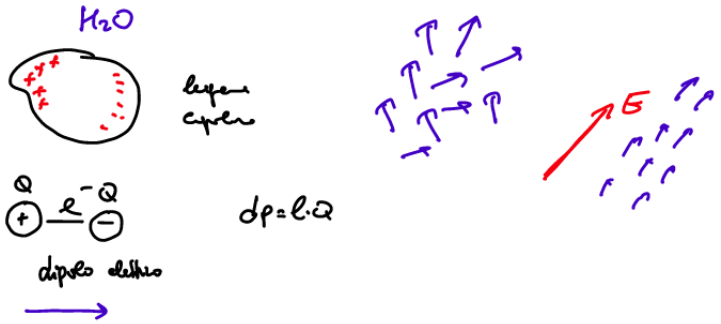

Figura 2.1: Polarizzazione delle molecole a seguito dell'applicazione di un campo elettrico

Il mezzo viene quindi polarizzato per effetto del campo esterno.

Polarizzazione Ionica Nel corpo umano c'è tanta acqua, quindi è molto importante. Ci sono nel corpo altri materiali solidi, in cui è più difficile riconoscere la molecola in quanto sono organizzati sotto forma di reticolo, dove ogni nodo ha una composizione ionica e quindi una parte positiva ed una negativa ad esempio NaCl: l'Na si va ad "appiccicare" al Cl negativo.
Nella singola cella, un pezzo è negativo ed uno è positivo, quando si applica un campo E, l'oggetto non può muoversi poiché vincolato, ma può essere deformato, quindi la poralizzazione ha effetto sulla modifica del reticolo, come riassunto nella figura sottostante

Polarizzazione elettronica Questa agisce direttamente sull'atomo, dove abbiamo il kernel positivo e la nube di elettroni. Anche in questo caso, in presenza di un campo E esterno la nube elettronica si può distribuire, su una forma magari più schiacciata, quindi abbiamo ancora un effetto dovuto allo stimolo esterno

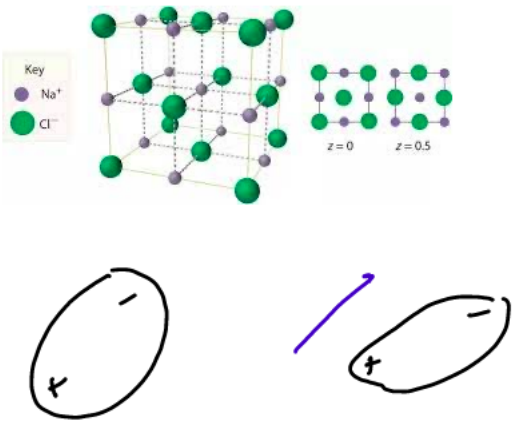

Figura 2.2: Effetti della polarizzazione ionica

Figura 2.3: Effetti della polarizzazione elettronica

La dissipazione risulta nel momento in cui è necessario trasferire informazione, in quanto occorrono dei segnali sinusoidali, avremo che il campo esterno ha la seguente forma

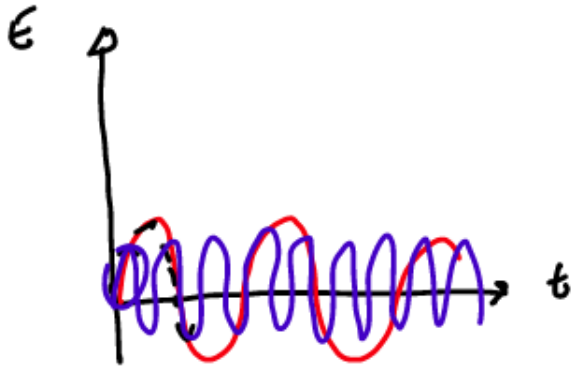

Figura 2.4: Andamento nel tempo del campo elettrico generato da un segnale sinusoidale

questa applicazione di una forza elettrica alla struttura produce lavoro, siccome la materia vuole stare in un certo modo, la struttura tenderà ad opporsi allo stimolo e quindi ci sarà inerzia che produce attrito e che quindi conseguentemente verrà prodotto un riscaldamento.
La dissipazione è quindi dovuta alla coesione complessiva dell'organismo che tende a non far muovere le molecole come vogliono.
È simile a cosa accade con un forno a microonde: se metto del grasso non si cuoce bene, se lo metto in acqua questa cede il calore e lo fa riscaldare più velocemente.
Se ci fosse una frequenza maggiore, ci sarebbe un ritardo in quanto il corpo umano ha del ritardo per capire che sta succedendo qualcosa e quindi le molecole sono sollecitate contro una forza, ci sarà

quindi prima un po' di inerzia per cui ci vuole del tempo prima che la struttura si accorga che sta arrivando un fonte d'onda, ma finché se ne accorge arriva già il fronte negativo e quindi quello che avviene è che l'interazione con la materia è ridotta e concentrata sulla parte esterna.

Occorre ora capire come rappresentare il corpo umano: si usa il modello di Debye, per cui abbiamo

$$\dot{\epsilon} = \epsilon_\infty + \frac{\epsilon_s - \epsilon_\infty}{1 + j\omega\tau} \tag{2.11}$$

dove

- ϵ_s è la costante statica (??)
- ϵ_∞è la costante ottima
- τ è il tempo di rilassamento, legato al tempo che serve alla molecola per sentire lo stimolo e tornare alla condizione iniziale dopo che lo stimolo è finito. È quindi il ritardo con cui viene seguito lo stimolo

Se rappresentiamo consideriamo una rappresentazione grafica:

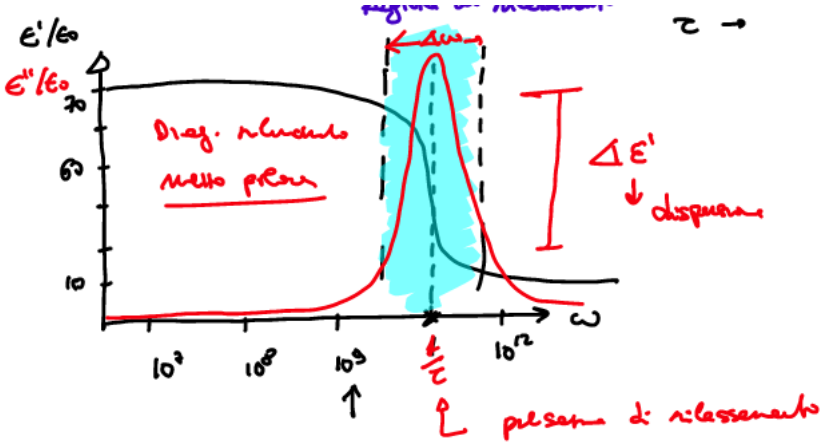

Figura 2.5: Andamento del rapporto $\frac{\epsilon'}{\epsilon_0}$ ed $\frac{\epsilon''}{\epsilon_0}$

teniamo conto che i GHz sono nell'ordine 10^9, mettiamo ad $\frac{1}{\tau}$ la pulsazione di rilassamento.
Avviene che la parte reale, quindi la capacità di immagazzinare energia e trasmetterla, in prossimità della frequenza in rosso ha un passaggio brusco, in un range di frequenza abbastanza stretto, la regione celeste che è la regione di rilassamento. La parte immaginaria ha un andamento totalmente opposto, in quella finestra c'è un assorbimento importante, le perdite sono elevate e quindi la potenza ceduta viene dissipata dal corpo. Questo è il digramma di rilassamento in un mezzo polare, le conseguenze da un punto di vista di comunicazione è nel che lavorare nella finestra celeste ci sono due fenomeni negativi:

- molte perdite, se mando 1W di potenza buona parte del segnale è propagato;
- guardando alla permettività, mandando un segnale con una banda importante avrà ogni componente spettrale con una diversa velocità di propagazione e quindi avremo informazione dispersa

Quindi tutti i mezzi biologici sono dispersivi, quindi occorre lavorare distanti dalla zona di rilassamento perché il segnale ha effetti dispersivi e distorcenti.

Visto invece dal punto di vista della fisioterapia, conviene lavorare in quella fascia perché c'è dissipazione e quindi riscaldamento.
L'acqua ha una pulsazione di rilassamento dell'ordine di 20GHz, quindi il forno a microonde che funziona a 2450 MHz non è molto lontano.
Questo avverrebbe se ci fossero solo composti polari come l'acqua, ma l'espressione quando consideriamo un corpo umano va adeguata a composti come proteine etc... ottenendo

$$\dot{\epsilon} = \epsilon' - j\frac{\sigma}{\omega\epsilon_0} = \epsilon_\infty + \frac{\epsilon_s - \epsilon_\infty}{1 + (j\omega\tau)^{1-\alpha}} \tag{2.12}$$

(dove $0 < \alpha < 1$), ottenendo **l'espressione di Cole-Cole**.
Mettendo tutto insieme, si è visto che tutto il corpo umano si può rappresentare con 4 di queste espressioni

$$\dot{\epsilon} = \sum_{i=1}^{4} \frac{\epsilon_{si} - \epsilon_\infty}{1 + (j\omega\tau_i)^{1-\alpha_i}} + \epsilon\infty - j\frac{\sigma_0}{\omega} \tag{2.13}$$

dove tutti i parametri con la i e σ sono dipendenti dai tessuti del corpo considerato.
Rappresentando la finestra di dispersione, abbiamo 3 finestre per i vari parametri:

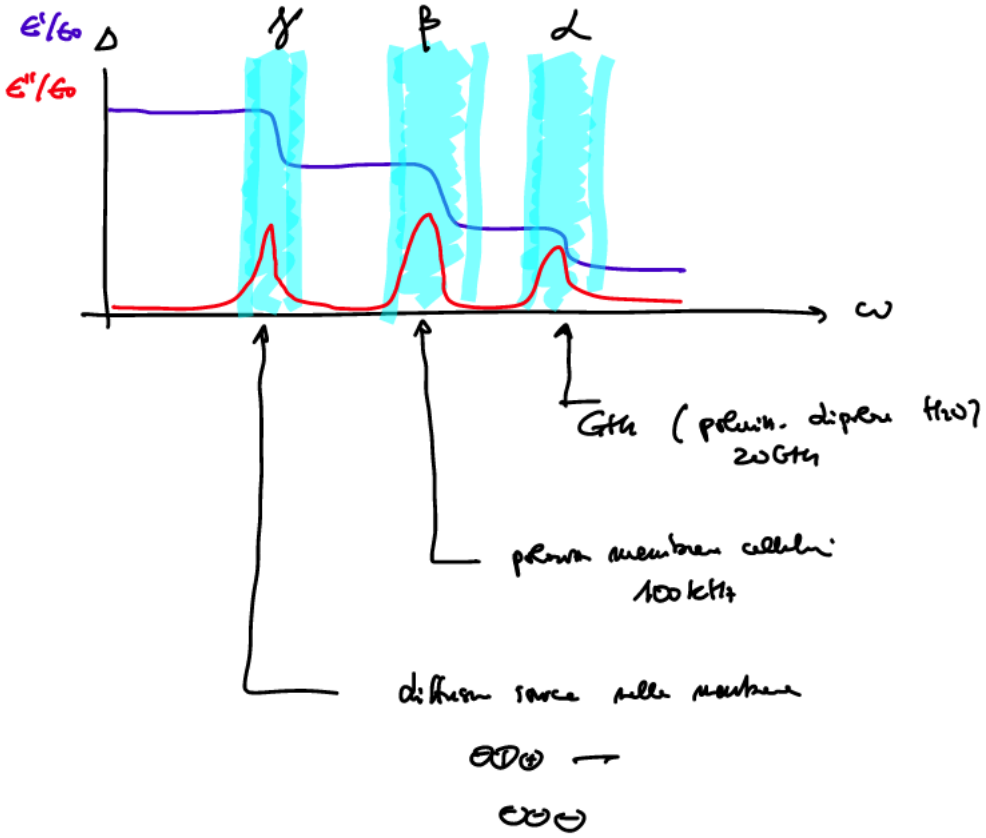

Figura 2.6: Finestre di dispersione

nelle varie finestre ci sarà un incremento di perdite locale, questa è la risposta del corpo umano tessuto per tessuto (grasso, pelle, ...) in termini di riscaldamento, ed hanno nomi γ, β α, dove comandano diversi effetti

- γ comanda la polarizzazione dipolare dell'acqua
- β comanda la polarizzazione delle membrane cellulari

Tessuto	10 Mhz ($\frac{\epsilon_r}{\sigma}$)	434 Mhz	915 Mhz	2450 Mhz
Grasso	54 205	15 60	5 820	12 341
Muscolo	283 715	57 1120	55 1450	50 2272

α diffusione ionica nelle membrane

Immaginando di avere delle cariche libere: applicando il campo questi ioni entrano, poi applicandone un altro escono e quindi c'è assorbimento che produce delle perdite.

2.1.2 Come caratterizzare i materiali

Negli anni 90, sulla spinta dell'evoluzione della telefonia mobile, si è studiato l'impatto del telefono sulla testa e molti gruppi hanno studiato come caratterizzare i tessiti (sugli animali), usando l'espressione come interpolatore ed hanno estratto i parametri che sono di interpolazione. Ci sono dei DB dove in base alla frequenza ed al materiale c'è la lista dei parametri e quindi introducendola nella Cole-Cole generalizzata si ottiene la $\dot{\epsilon}$.
Uno dei DB è Italiano, del CNR: niremf.ifac.cnr.it/emfref o /tissprop: si possono scaricare direttamente i parametri oppure avere i valori di permetività e conducibilità: otteniamo diversi valori tra cui la lunghezza d'onda ($\lambda = \frac{\lambda_0}{\sqrt[2]{\epsilon_r}}$). Prendendo ad esempio il muscolo, all'aumentare della frequenza, la conducibilità aumenta, la permettività diminuisce. Più c'è presenza di acqua, più permettività e conducibilità sono elevate.Ne riportiamo alcuni: la differenza di conducibilità è importante, quindi il muscolo dissiperà sicuramente più potenza del grasso. Cerchiamo ora di caratterizzare tutto da un punto di vista ingegneristico

Assorbimento

Un'onda arriva su un materiale: una grandezza importante è la densità di potenza dissipata nel corpo

$$p_j = \frac{1}{2}\sigma|E|^2 \tag{2.14}$$

e si misura in $\frac{W}{m^3}$.
Per le norme di emissione si considera la SAR (Specific Absorption Rate), data da:

$$SAR = \frac{p_j}{p} \tag{2.15}$$

misurato in $\frac{W}{kg}$ e che indica quanta potenza viene assorbita per unità di massa del dispositivo, ed è quindi data da

$$\frac{\partial P}{\partial m} = \frac{1}{2\rho}\sigma|E|^2 \tag{2.16}$$

e si usa in quanto è più facile da misurare.
Se abbiamo un organo e vogliamo calcolare la potenza avremo quindi:

$$P(\Omega_m) = \int_{\Omega_m} P(r')SAR(r)dr' \tag{2.17}$$

dove

$$SAR(\underline{r}) = \frac{1}{2\rho(r)}\sigma(r)|E(r)|^2 \tag{2.18}$$

Le misure vengono fatte su dei "fantocci" che simulano le caratteristiche EM del corpo, il modo più semplice è usare acqua zucchero e sale:

- l'acqua ha una permettività intorno a 70 Ghz
- il sale abbassa la ϵ_r
- lo zucchero aumenta la σ

Ci sono delle ricette per ricostruire ogni organo e poter quindi misurare il SAR, altrimenti si usano fantocci da "macellaio", pezzi di carne etc...

Propagazione nei tessuti biologici

Consideriamo il caso più semplice possibile, dove il corpo umano è un mezzo omogeneo, avrà quindi una permettività $\epsilon' - j\frac{\sigma}{\omega}$.
Immaginiamo di avere i due mezzi, (1) e (2) e che arrivi un campo elettrico che sia un'onda piana, si propaghi in direzione z, come mostrato in seguito:

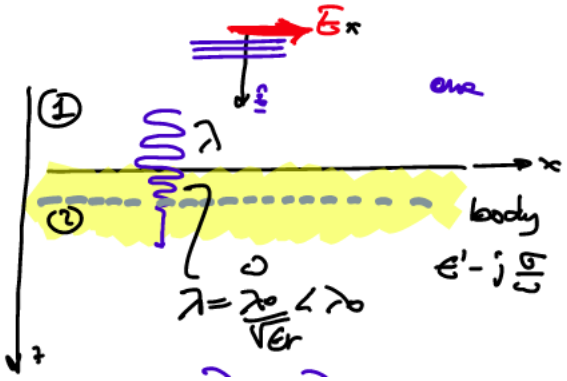

Figura 2.7: Esempio di propagazione di un'onda EM che attraversa due mezzi

Cosa accade al corpo: abbiamo, per un'onda piana

$$E_x(z) = E_0 e^{-jkz} \tag{2.19}$$

dove k è la costante complessa di propagazione

$$k = \beta - j\alpha \tag{2.20}$$

ed α e β sono rispettivamente il fattore di propagazione ed il fattore di attenuazione:

$$\alpha = \omega \sqrt[2]{\mu\epsilon'}\{\frac{1}{2}[\sqrt[2]{1 + (\frac{\epsilon^{\nu}}{\epsilon'})} - 1]\}^{\frac{1}{k}} \tag{2.21}$$

(esponente della quadra forse sbagliata).
Sia α che β dipendono dalla propagazione e dal mezzo.
L'onda entra nel mezzo e man mano tenderà ad attenuarsi per via delle perdite, è importante capire da che punto in poi possiamo dire che l'onda si sia attenuata: definiamo $\delta_s = \frac{1}{\alpha}$ ed è tale per cui z(profondità)= $= \delta_s$:

$$|\frac{E_x(\delta)}{E_y(\delta)}| = \frac{1}{e} \tag{2.22}$$

che è circa del 37%, quindi comunicare sotto questa soglia diventa molto complicato, la densità di potenza proporzionale al modulo di E si è ridotta invece del 13%. Abbiamo un grafico come quello in 2.8:

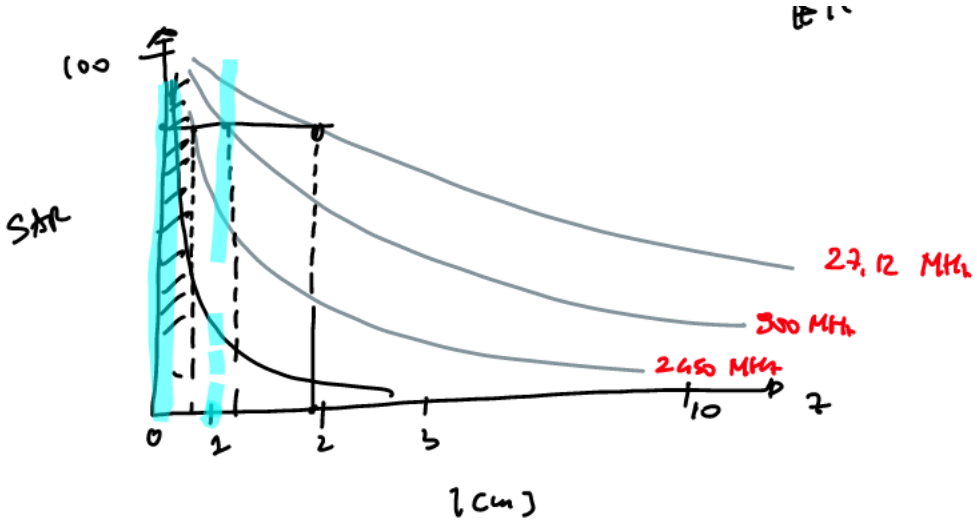

Figura 2.8: Attenuazione del SAR

supponiamo di fissare un valore di riferimento del SAR: questo sarà ottenuto nel mezzo, al variare della frequenza, ad una profondità via via crescente: se la profondità diminuisce lo spessore aumenta, quindi aumentando la frequenza otterremmo una profondità di penetrazione molto sottile. Fissando la profondità, all'aumentare della frequenza, il SAR tende ad abbassarsi quindi le conseguenze sono che volendo arrivare i profondità per comunicare con un dispositivo in profondità occorre usare frequenze basse, per cui il δ_s è basso, aumentando la frequenza l'interazione è sempre più in superficie **(ricorda di smentire i coglioni che dicono che il 5G fa male perché entra nel corpo. COJONI, leggete le frequenze usate COJONI)**.