UNIVERSITÀ
DEGLI STUDI
DI PADOVA

DIPARTIMENTO
DI INGEGNERIA
DELL'INFORMAZIONE

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

LAUREA IN INGEGNERIA INFORMATICA

AUTENTICAZIONE A LIVELLO FISICO DI COMUNICAZIONI CON SUPERFICI INTELLIGENTI

Relatore: Prof. Stefano Tomasin

Laureando: Lorenzo Serafini

ANNO ACCADEMICO 2022-2023

Data di laurea 25/09/2023

Indice

1

Introduzione

In questo documento vogliamo studiare un metodo alternativo per l'autenticazione di un dispositivo al ricevitore. Invece di autenticarlo attraverso i classici meccanismi ad alto livello, vogliamo riuscirci analizzando le proprietà del canale di trasmissione. Per questo scopo utilizzeremo una Superficie Riflettente Intelligente (IRS) che, a seconda della sua configurazione, decisa dal ricevitore, modificherà le proprietà del canale. Se il ricevitore identifica il segnale come proveniente dal trasmettitore legittimo, processerà il segnale, altrimenti lo scarterà. Per decidere della legittimità del segnale, faremo affidamento al Generalized Likelihood Ratio Test (GLRT) e studieremo i casi di errore di autenticazione.
Nel capitolo 2 introdurremo il concetto di autenticazione e descriveremo il meccanismo con il quale intediamo proteggere le comunicazioni. Nel capitolo 3 verrà illustrato il modello di canale utilizzato, in particolare ci concentreremo sul caso di antenna singola e analizzeremo un attacco con conoscenza completa dei canali di comunicazione. Nel capitolo 4 studieremo le caratteristiche dell'utilizzo di due densità di probabilità: clipped gaussian e uniforme. Infine le conclusioni saranno discusse nel capitolo 5.

2

Autenticazione

Quando parliamo di sicurezza nell'ambito delle telecomunicazioni, i principali aspetti sui cui ci si concentra sono la confidenzialità e l'autenticazione. Con confidenzialità intendiamo il voler evitare che il messaggio inviato sia intercettato e decifrato da un soggetto terzo, diverso dal ricevente. Con autenticazione, invece, intendiamo il verificare le identità degli utenti, impedendo che utenti non legittimi possano fingersi utenti legittimi.
Tradizionalmente la sicurezza nelle comunicazioni è prerogativa dei livelli più alti delle architetture mediante l'uso della crittografia, ad esempio attraverso metodi cifratura a chiave simmetrica o asimmetrica. Questi metodi necessitano fortemente di complessità computazionale e della segretezza delle chiavi.
Con l'avvento dell'Internet of things, che si prefigge di connettere dispositivi spesso aventi risorse limitate, i classici protocolli di sicurezza, basati su complessi metodi crittografici, diventano impraticabili. [1]
Nonostante i vincoli ai livelli superiori, una soluzione possibile è la physical layer security (PLS), sicurezza a livello fisico, un meccanismo tramite cui è possibile implementare metodi che realizzano la sicurezza delle comunicazioni a livello fisico.
Invece di far affidamento sulla complessità computazionale, la PLS sfrutta la variabilità e la casualità dei canali di comunicazione per garantire sia confidenzialità che autenticazione, limitando l'informazione estratta dagli attaccanti sul messaggio inviato. [1]
Nel nostro caso, puntiamo a verificare l'identità di un trasmettitore, confrontando le proprietà di canale correnti con quelle verificate precedentemente nelle comunicazioni passate.

2.1 Challenge-Response

A questo scopo utilizziamo il meccanismo noto come Challenge-Response (CR). Chiamiamo Alice il trasmettitore, Bob il ricevitore, infine Eve è l'attaccante che vuole fingersi Alice. Nella sicurezza ad alto livello, la CR consiste nella condivisione tra Alice e Bob di una chiave segreta che permette a Bob di fare domande casuali (challenge) ad Alice, che è l'unica in grado di rispondere correttamente (response). Nella vita di tutti i giorni, usare una one-time password, è un metodo di autenticazione challenge-response.

Il metodo per l'autenticazione CR si può applicare alla PLS, ciò avviene tramite il controllo parziale delle proprietà di canale da parte di Bob. Queste proprietà quindi possono essere in parte determinate da Bob. La challenge è rappresentata dalla configurazione delle proprietà di canale scelte da Bob. Questo però non definisce completamente il canale. La response è rappresentata dalle proprietà di canale stimate da Bob, che devono essere corrispondenti, entro una certa soglia, a quelle della configurazione scelta.
Per poter garantire una maggiore sicurezza, nel meccanismo di CR-PLS, le proprietà di canale stimate devono variare lentamente nel tempo, considerando anche cambiamenti dell'ambiente in cui trasmettiamo, e deve mostrare una grande variabilità sia rispetto alla posizione del ricevitore e trasmettitore, sia cambiando la configurazione scelta da Bob. [2]
Il meccanismo di autenticazione challenge-response, si articola in 4 fasi:

1. *Identificazione*

   Alice trasmette a Bob diversi segnali, passando attravarso il canale parzialmente controllabile, configurato diversamente per ogni segnale. Bob così riesce e a stimare le proprietà del canale. Alice viene identificata tramite meccanismi ad alto livello.

2. *Configurazione*

   Bob configura la IRS, questa configurazione potrebbe essere diversa da una di quelle assunte nel punto 1. Bob allora stima le nuove proprietà del canale sul quale trasmetterà Alice, basandosi sulle misure effettuate nel punto 1.

3. *Trasmissione*

   Alice trasmette un messaggio a Bob, passando per la IRS. Bob calcola le proprietà del canale analizzando il messaggio ricevuto.

4. *Autenticazione*

   Bob, confronta le misure delle proprietà del canale effettuate nel punto 3 con quelle stimate nel punto 2 e decide se il messaggio è autentico.

Inoltre la configurazione scelta da Bob, dove essere cambiata periodicamente, idealmente ciò dovrebbe avvenire ad ogni messaggio trasmesso. Se da una parte sfruttiamo la controllabilità del canale per l'autenticazione, dobbiamo anche soddisfare vincoli non legati alla sicurezza, come il consumo di energia. Infatti, volendo esplorare una maggiore quantità di configurazioni, la misura delle proprietà di canale richiede un maggiore impiego di tempo ed energia. E per quanto più configurazioni possibili rendano più difficile un attacco da parte di Eve, dovremmo limitare le configurazioni attuabili per soddisfare una certa qualità di comunicazione, un vincolo non trascurabile. [2]

2.2 Errori di Autenticazione

Essendo il canale parzialmente controllabile, data la variabilità che lo contraddistingue, le stime effettuate non saranno identiche alle misure. Il messaggio è ritenuto autentico se la distanza

tra le stime e le misure è inferiore ad una certa soglia. Quindi non sempre autenticheremo correttamente il messaggio. Possono verificarsi due casi di errore:

- misdetection (MD): in cui autentichiamo un messaggio di Eve come proveniente da Alice;
- false alarm (FA): in cui scartiamo un messaggio di Alice, nonostante sia autentico.

3

IRS e modello di canale

Una intelligent reflective surface (IRS), superficie intelligente riflettente, è una superficie composta da tante celle di metamateriale che possono essere controllate singolarmente, nel nostro caso dal ricevitore, per ottenere una determinata configurazione della IRS. Ogni cella redireziona il segnale e introduce un cambiamento di fase, modificando così le proprietà del canale. Le IRS sono adatte all'autenticazione CR-PLS, avendo un'alta direttività e fornendo molti e diversi canali a diversi dispositivi. Inoltre il gran numero di elementi presenti sulla IRS permette anche un'alta variabilità dei canali ottenuti. [2]
Consideriamo una situazione in cui Alice, Bob e Eve hanno più antenne per trasmettere e per ricevere. Ci troviamo quindi in un canale Multiple Input Multiple Output (MIMO). Ogni antenna trasmetterà un segnale e possiamo descrivere il messaggio inviato come un vettore di lunghezza pari al numero di antenne del trasmettitore.
Identifichiamo con $\boldsymbol{x}$ il vettore trasmesso da Alice, con $\boldsymbol{y}$ il vettore ricevuto dalla IRS, con $\boldsymbol{z}$ il vettore trasmesso dalla IRS e con $\boldsymbol{q}$ il vettore ricevuto da Bob. Consideriamo il caso in cui Alice ha K antenne, Bob M, Eve V e la IRS ha N celle.
Modelliamo il canale tra Alice e l'IRS con una matrice $\boldsymbol{G}$ $N \times K$, quindi:

$$\boldsymbol{y} = \boldsymbol{G}\boldsymbol{x} \tag{3.1}$$

La IRS introdurrà poi un cambiamento di fase del segnale ricevuto $\boldsymbol{y}$, inviando il segnale $\boldsymbol{z}$. Possiamo modellare questo comportamento con una matrice diagonale $\boldsymbol{\Phi}$ $N \times N$, in cui ogni elemento della diagonale è un numero complesso di modulo 1 e fase ϕ_i. Abbiamo quindi:

$$\boldsymbol{z} = \boldsymbol{\Phi}\boldsymbol{y} \tag{3.2}$$

Infine il segnale arriverà a Bob dalla IRS e la matrice $\boldsymbol{H}$ $M \times N$ modella questo canale.

$$\boldsymbol{q} = \boldsymbol{H}\boldsymbol{z} \tag{3.3}$$

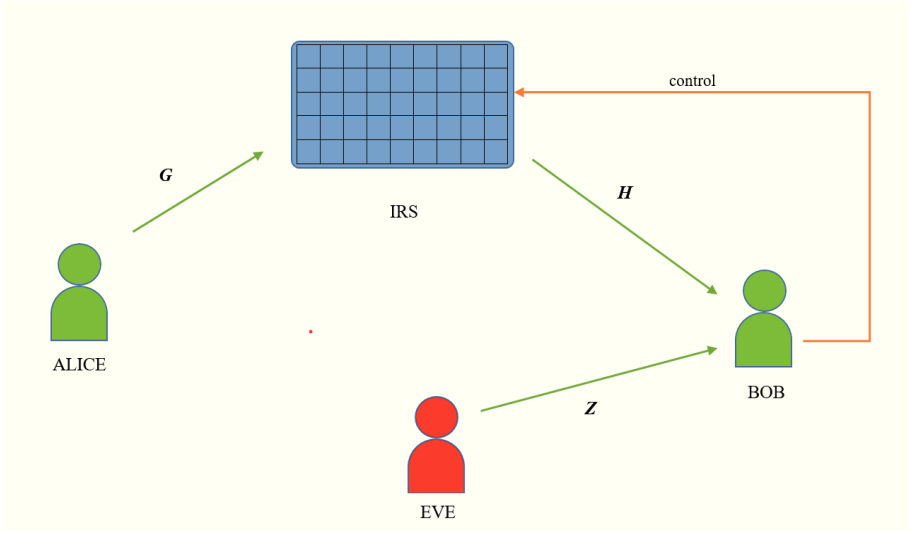

Figure 3.1: Schema del sistema di comunicazione con IRS

Il canale da Alice a Bob può essere scritto come:

$$\boldsymbol{Q}^{(A,I,B)} = \boldsymbol{H}\boldsymbol{\Phi}\boldsymbol{G} \tag{3.4}$$

Il segnale è corrotto da rumore AWGN, perciò quando sarà Alice a trasmettere, Bob stimerà il canale:

$$\hat{\boldsymbol{Q}} = \bar{\boldsymbol{Q}}^{(A,I,B)} + \boldsymbol{W} \tag{3.5}$$

dove $\boldsymbol{W}$ rappresenta l'errore della stima da parte di Bob, modellizzato come AWGN a media nulla ed elementi indipendenti, con potenza pari a σ_B^2.
Invece quando il segnale proviene da Eve:

$$\hat{\boldsymbol{Q}} = \boldsymbol{Z} + \boldsymbol{W} \tag{3.6}$$

indicando con $\boldsymbol{Z}$ il canale generato da Eve per fingersi Alice.

3.1 GLRT

Per determinare la soglia entro la quale considerare il messaggio ricevuto come autentico utilizziamo il Generalized Likelihood Ratio Test (GLRT). Bob autentica il messaggio secondo due ipotesi:
H_0: il messaggio è stato inviato da Alice;
H_1: il messaggio non è stato inviato da Alice.

Chiamiamo con $f_{\hat{Q}|H_0}(a)$ la densità di probabilità della stima del canale $\hat{\boldsymbol{Q}}$ sotto l'ipotesi H_0, e definiamo la funzione di verosimiglianza come:

$$\Psi = \log f_{\hat{\boldsymbol{Q}}|H_0}(\hat{\boldsymbol{Q}}) \tag{3.7}$$

Dalla (3.5) sotto l'ipotesi H_0, $\hat{\boldsymbol{Q}}$ è distribuita come una gaussiana di media $\bar{\boldsymbol{Q}}^{(A,I,B)}(\boldsymbol{\Phi}')$ e varianza in ogni dimensione pari a $\sigma^2 = 2\sigma_{\mathrm{B}}^2$ otteniamo

$$\Psi \propto \frac{2}{\sigma^2} \sum_{m=0}^{KM-1} |\mathrm{vec}(\hat{\boldsymbol{Q}})_m - \mathrm{vec}(\bar{\boldsymbol{Q}}^{(A,I,B)}(\boldsymbol{\Phi}'))_m|^2 \tag{3.8}$$

Se il valore restituito da Ψ è minore o uguale di una certa soglia τ, allora Bob decide che il messaggio proviene da Alice (H_0), altrimenti lo scarta (H_1).
La probabilità di FA si verifica quando, sotto l'ipotesi H_0, $\Psi > \tau$

$$P_{\mathrm{FA}} = P[\Psi > \tau | H_0] = 1 - F_{\chi^2,0}(\tau) \tag{3.9}$$

Dalla (3.6), sotto l'ipotesi H_1 otteniamo:

$$\Psi \propto \frac{2}{\sigma^2} \sum_{n=0}^{KM-1} |\mathrm{vec}(\boldsymbol{Z})_n + \mathrm{vec}(\boldsymbol{W}'')_n - \mathrm{vec}(\hat{\boldsymbol{Q}}^{(A,I,B)}(\boldsymbol{\Phi}'))_n|^2 \tag{3.10}$$

La probabilità di MD si verifica quando, sotto l'ipotesi H_1, $\Psi < \tau$

$$P_{\mathrm{MD}}(\zeta(\boldsymbol{\Phi}')) = P[\Psi < \tau | H_1] = F_{\chi^2,\zeta(\boldsymbol{\Phi}')}(\tau), \tag{3.11}$$

Dove $F_{\chi^2,\zeta(\boldsymbol{\Phi}')}(k)$ è la funzione di distribuzione di una variabile aleatoria chi quadrato e $\zeta(\boldsymbol{\Phi}')$ è il parametro di non centralità, pari a

$$\zeta(\boldsymbol{\Phi}') = \frac{2}{\sigma^2} \left|\left| \boldsymbol{Z} - \boldsymbol{Q}^{(A,I,B)}(\boldsymbol{\Phi}') \right|\right|^2 \tag{3.12}$$

Imponendo una P_{FA}, possiamo ricavare la soglia τ sulla quale Bob base le decisioni di autenticazione del messaggio:

$$\tau = F_{\chi^2,0}^{-1}(1 - P_{\mathrm{FA}}) \tag{3.13}$$

Infine così possiamo calcolare P_{MD}:

$$P_{\mathrm{MD}}(\zeta(\boldsymbol{\Phi}')) = F_{\chi^2,\zeta(\boldsymbol{\Phi}')}\big(F_{\chi^2,0}^{-1}(1 - P_{\mathrm{FA}})\big) \tag{3.14}$$

3.2 Antenna Singola

Possiamo semplificare il modello considerando una singola antenna al trasmettitore e al ricevitore. In questo modo le matrici $\boldsymbol{H}$ e $\boldsymbol{G}$ diventano rispettivamente dei vettori riga e colonna. Per massimizzare il rapporto segnale-rumore, la configuarazione ottima per la IRS introduce un cambiamento di fase:

$$\bar{\theta}_n = \alpha - \angle H_{1,n} - \angle G_{n,1}, \quad n = 1, \ldots, N, \tag{3.15}$$

con α indichiamo l'angolo comune a tutti gli elementi della IRS.
Bob potrà quindi modificare la configurazione della IRS attorno a quella ottima, ottenendo un nuovo cambiamento di fase:

$$\theta_n = \bar{\theta}_n + \epsilon_n \tag{3.16}$$

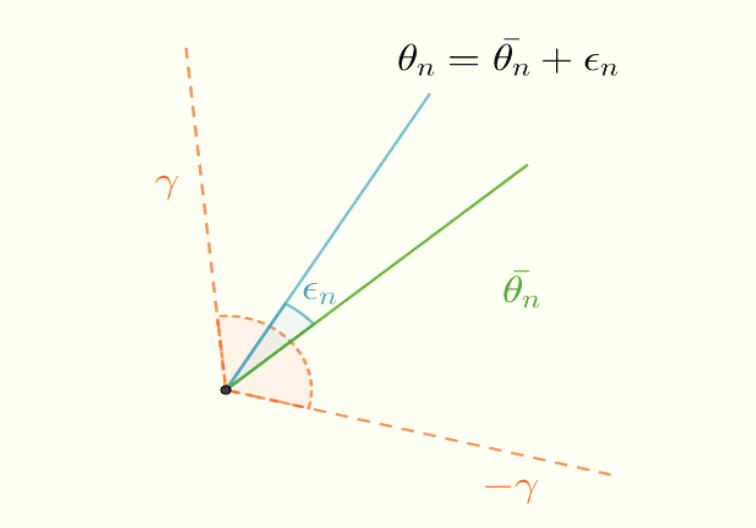

Figure 3.2: Schema della configurazione di un singolo elemento della IRS

Avendo una sola antenna, abbiamo che $\Psi = \frac{2}{\sigma^2}|\delta|^2$
Sotto l'ipotesi H_0

$$\delta = \boldsymbol{H}\boldsymbol{\Phi}'\boldsymbol{G} + W'' - \boldsymbol{H}\boldsymbol{\Phi}'\boldsymbol{G} - W', \tag{3.17}$$

invece sotto l'ipotesi H_1

$$\delta = Z + W'' - \boldsymbol{H}\boldsymbol{\Phi}'\boldsymbol{G} - W', \tag{3.18}$$

La capacità di canale tra Alice è Bob, con una configurazione casuale della IRS è data da:

$$C_{\text{sec}}(\bar{\boldsymbol{\Phi}}) = \log_2\left(1 + \frac{\left|\sum_{n=0}^{N-1} H_{1,n}G_{n,1}e^{j\theta_n}\right|^2}{\sigma_B^2}\right). \tag{3.19}$$

Studiamo ora il caso in cui gli N elementi della IRS tendano ad infinito, con $H_{1,n}$ e $G_{n,1}$ variabili aleatorie gaussiane complesse indipendenti e identicamente distribuite: $H_{1,n}, G_{n,1} \simeq \mathcal{CN}(0,1)$.
Scriviamo μ_{sec} in funzione della media di $e^{j\epsilon_n}$, definiamo:

$$\mathtt{m} = \mathbb{E}[e^{j\epsilon_n}] = \mathbb{E}[\cos\epsilon_n] + j\mathbb{E}[\sin\epsilon_n] \tag{3.20}$$

Assumiamo che la densità di probabilità di ϵ_n sia pari, dato che la funzione $\sin\epsilon_n$ è dispari e calcolando il valore atteso nell'intervallo $[-\gamma, \gamma]$, abbiamo che $\mathtt{m}$ è reale:

$$\mathtt{m} = \mathbb{E}[\cos \epsilon_n] \tag{3.21}$$

Definiamo anche:

$$\mathtt{s} = \mathtt{s}_R + j\mathtt{s}_I = \mathbb{E}[\cos^2 \epsilon_n] + j\mathbb{E}[\sin^2 \epsilon_n] \tag{3.22}$$

E infine:

$$\mathtt{r} = \mathbb{E}[\cos \epsilon_n \sin \epsilon_n] \tag{3.23}$$

Per gli stessi motivi del valore atteso di $\sin \epsilon_n$, nel nostro caso:

$$\mathtt{r} = 0 \tag{3.24}$$

La media dei termini nella sommatoria in (3.19) è:

$$\begin{aligned} \mu_{\text{sec}} &= \mathbb{E}[H_{1,n} G_{n,1} e^{j\theta_n}] = \mathbb{E}[|H_{1,n} G_{n,1}| e^{j\epsilon_n}] = \\ &= \mathbb{E}[|H_{1,n}|]\mathbb{E}[|G_{n,1}|]\mathbb{E}[e^{j\epsilon_n}] = \\ &= \frac{\sqrt{\pi}}{2}\frac{\sqrt{\pi}}{2}\mathtt{m} = \frac{\pi}{4}\mathtt{m} \end{aligned} \tag{3.25}$$

Poichè $H_{1,n}$,$G_{n,1}$ e $e^{j\epsilon_n}$ sono indipendenti, il valore atteso del prodotto è il prodotto dei valori attesi. Il modulo di $H_{1,n}$ (e di $G_{n,1}$), ha una distribuzione di Rayleigh, il cui valore atteso è pari a $\mathbb{E}[H_{1,n}] = \mathbb{E}[G_{1,n}] = \sigma\sqrt{\frac{\pi}{2}} = \frac{\sqrt{\pi}}{2}$, dato che la parte reale e la parte immaginaria sono variabili aleatorie gaussiane a media nulla e varianza $\sigma^2 = \frac{1}{2}$.

La varianza dei termini nella sommatoria in (3.19) è:

$$\begin{aligned} \sigma^2_{\text{sec}} &= \mathbb{E}\left[\left|H_{1,n} G_{n,1} e^{j\theta_n} - \mu_{\text{sec}}\right|^2\right] = \\ &= 1 - \mu^2_{\text{sec}} = 1 - \frac{\pi^2}{16}\mathtt{m}^2 \end{aligned} \tag{3.26}$$

Applicando il teorema centrale del limite, approssimiamo i termini nella sommatoria come gaussiane, con media $N\mu_{\text{sec}}$ e varianza $N\sigma^2_{\text{sec}}$. Ricordando che, per una variabile aleatoria complessa a simmetria circolare y con media complessa m e varianza reale σ^2, la media di $|y|^2$ (avendo $\omega = \omega_R + j\omega_I$ variabile aleatoria gaussiana complessa a simmetria circolare a media nulla e a varianza unitaria) è:

$$\mathbb{E}[|m + \sigma w|^2] = \frac{\sigma^2}{2}\mathbb{E}\left[\left(m_R\frac{\sqrt{2}}{\sigma} + \sqrt{2}w_R\right)^2 + \left(m_I\frac{\sqrt{2}}{\sigma} + \sqrt{2}w_I\right)^2\right] = \frac{\sigma^2}{2}(2 + \lambda) \tag{3.27}$$

con $\lambda = \frac{2|\mu|^2}{\sigma^2}$.

Possiamo quindi approssimare il SNR come:

$$\Omega \approx \frac{N\sigma_{\text{sec}}^2}{2\sigma_{\text{B}}^2}\left(2+\frac{2N^2\mu_{\text{sec}}^2}{N\sigma_{\text{sec}}^2}\right)=\frac{N}{\sigma_{\text{B}}^2}(N\mu_{\text{sec}}^2+\sigma_{\text{sec}}^2)=\frac{N}{\sigma_{\text{B}}^2}\left((N-1)\frac{\pi^2}{16}\mathtt{m}^2+1\right) \tag{3.28}$$

3.3 Attacco con conoscenza completa dei canali

Ipotizziamo che Eve conosca tutti i canali di trasmissione tra i dispositivi e che solo la configurazione della IRS le rimanga ignota. Per massimizzare la probabiltà che l'attacco abbia successo, Eve imporrà:

$$\boldsymbol{Z}=\mathbb{E}[\boldsymbol{Q}^{(A,I,B)}], \tag{3.29}$$

il valore atteso considerato è quello della configurazione casuale della IRS. Considerando la strategia Challenge-Response, otteniamo

$$\boldsymbol{Z}=\boldsymbol{H}\mathbb{E}[\boldsymbol{\Phi}]\boldsymbol{G}=\boldsymbol{H}\bar{\boldsymbol{\Phi}}\mathbb{E}[\text{diag}\{e^{j\epsilon_n}\}]\boldsymbol{G} \tag{3.30}$$

Mettendoci nel caso in cui abbiamo un'antenna singola si ha

$$Z=\mathtt{m}\boldsymbol{H}\bar{\boldsymbol{\Phi}}\boldsymbol{G}, \tag{3.31}$$

e la (3.18) diventa

$$\begin{aligned}\delta =&\mathtt{m}\boldsymbol{H}\bar{\boldsymbol{\Phi}}\boldsymbol{G}+W''-\boldsymbol{H}\boldsymbol{\Phi}'\boldsymbol{G}-W'\\ =&\sum_n H_{1,n}e^{j\bar{\theta}_n}\left[\mathtt{m}-e^{j\epsilon_n}\right]G_{1,n}+W''-W'.\end{aligned} \tag{3.32}$$

Nel caso Rayleigh-fading, i termini nella sommatoria sono indipendenti e identicamente distribuiti con media

$$\mathbb{E}\left[H_{1,n}e^{j\bar{\theta}_n}\left[\mathtt{m}-e^{j\epsilon_n}\right]G_{1,n}\right]=0, \tag{3.33}$$

con varianza della parte reale e della parte immaginaria:

$$\begin{aligned}\sigma_{\text{R}}^2=&\mathbb{E}\left[\text{Re}\left\{H_{1,n}e^{j\bar{\theta}_n}\left[\mathtt{m}-e^{j\epsilon_n}\right]G_{1,n}\right\}^2\right]=\\ =&\mathbb{E}\left[(\mathtt{m}-\cos\epsilon_n)^2\right]=\\ =&\mathtt{m}^2-2\mathtt{m}\mathbb{E}[\cos\epsilon_n]+\mathbb{E}[\cos^2\epsilon_n]=\\ =&\mathtt{m}^2-2\mathtt{m}^2+\mathtt{s}_R=\\ =&\mathtt{s}_R-\mathtt{m}^2\end{aligned} \tag{3.34}$$

$$\begin{aligned}\sigma_{\mathrm{I}}^2 &= \mathbb{E}\left[\mathrm{Im}\left\{H_{1,n}e^{j\bar{\theta}_n}\left[\mathtt{m}-e^{j\epsilon_n}\right]G_{1,n}\right\}^2\right] = \\ &= \mathbb{E}[\sin^2\epsilon_n] = \mathtt{s}_I\end{aligned} \tag{3.35}$$

e correlazione incrociata

$$\begin{aligned}&\mathbb{E}\left[\mathrm{Re}\left\{H_{1,n}e^{j\bar{\theta}_n}\left[\mathtt{m}-e^{j\epsilon_n}\right]G_{1,n}\right\}\mathrm{Im}\left\{H_{1,n}e^{j\bar{\theta}_n}\left[\mathtt{m}-e^{j\epsilon_n}\right]G_{1,n}\right\}\right] = \\ &= \mathbb{E}\left[(\mathtt{m}-\cos\epsilon_n)(-\sin\epsilon_n)\right] = \\ &= -\mathtt{m}\mathbb{E}[\sin\epsilon_n] + \mathbb{E}\left[\cos\epsilon_n\sin\epsilon_n\right] = \\ &= \mathbb{E}\left[\cos\epsilon_n\sin\epsilon_n\right] = \mathtt{r} = 0\end{aligned} \tag{3.36}$$

Per la legge dei grandi numeri, per $N \to \infty$, abbiamo che δ è una gaussiana complessa con media $\mu_\delta = 0$, con parte reale e parte immaginaria indipendenti e varianza $\sigma_{\delta,\mathrm{R}}^2 = N\sigma_{\mathrm{R}}^2 + \frac{\sigma^2}{2}$ and $\sigma_{\delta,\mathrm{I}}^2 = N\sigma_{\mathrm{I}}^2 + \frac{\sigma^2}{2}$.

La probabilità di misdetection media si può approssimare con:

$$\bar{P}_{\mathrm{MD}} = \mathbb{P}\left[\delta_R^2 + \delta_I^2 \leq \frac{\sigma^2\tau}{2}\right] \approx \mathbb{P}\left[\sigma_{\delta,\mathrm{R}}^2 g_1^2 + \sigma_{\delta,\mathrm{I}}^2 g_2^2 \leq \frac{\sigma^2\tau}{2}\right] \tag{3.37}$$

Dove g_1 e g_2 sono due variabili aleatorie gaussiane: $g_1, g_2 \simeq \mathcal{N}(0,1)$. Per poter calcolare la (3.37), dobbiamo usare la funzione di distribuzione della combinazione lineare di due variabili chi quadrato centrali indipendenti, ognuna con un grado di libertà. Non è ancora nota una forma chiusa per tale distribuzione ma in [3], ne è stata calcolata un'espansione in serie.

4

Risultati numerici

4.1 Clipped Gaussian

In particolare, scegliamo di far variare ϵ_n tra $-\gamma$ e γ, con una distribuzione gaussiana. Dobbiamo allora introdurre un termine di normalizzazione per la densità di probabilità che è pari a:

$$\int_{\gamma}^{\gamma} \frac{1}{\sqrt{2\pi}} e^{\frac{-x^2}{2}}\, dx \; = \operatorname{erf}\left(\frac{\gamma}{\sqrt{2}}\right) \tag{4.1}$$

La densità di probabilità di ϵ_n è quindi:

$$p_{\epsilon_n}(x) = \frac{1}{\sqrt{2\pi}} \frac{e^{\frac{-x^2}{2}}}{\operatorname{erf}\left(\frac{\gamma}{\sqrt{2}}\right)} \tag{4.2}$$

Per trovare il valore atteso di $e^{j\epsilon_n}$ abbiamo eseguito i seguenti passaggi:

$$\mathbb{E}\left[e^{jx}\right] = \int_{-\gamma}^{\gamma} \frac{1}{\sqrt{2\pi}} \frac{e^{\frac{-x^2}{2}}}{\operatorname{erf}\left(\frac{\gamma}{\sqrt{2}}\right)} e^{jx}\, dx \;=$$

$$= \frac{1}{\sqrt{2\pi}} \frac{1}{\operatorname{erf}\left(\frac{\gamma}{\sqrt{2}}\right)} \int_{-\gamma}^{\gamma} e^{\frac{-x^2}{2}} e^{jx}\, dx \;=$$

$$= \frac{1}{\sqrt{2\pi}} \frac{1}{\operatorname{erf}\left(\frac{\gamma}{\sqrt{2}}\right)} \int_{-\gamma}^{\gamma} e^{\frac{-x^2}{2} - jx}\, dx \;=$$

completiamo il quadrato

$$= \frac{1}{\sqrt{2\pi}} \frac{1}{\operatorname{erf}\left(\frac{\gamma}{\sqrt{2}}\right)} \int_{-\gamma}^{\gamma} e^{-\left(\frac{x}{\sqrt{2}} - \frac{j}{\sqrt{2}}\right)^2 - \frac{1}{2}}\, dx \;=$$

sostituiamo $\left(\dfrac{\mathrm{x}}{\sqrt{2}} - \dfrac{\mathrm{j}}{\sqrt{2}}\right) = \mathrm{t}$

$$= \frac{1}{\sqrt{2\pi}} \frac{1}{\operatorname{erf}\left(\frac{\gamma}{\sqrt{2}}\right)} \frac{1}{\sqrt{e}} \int_{\frac{-\gamma-j}{\sqrt{2}}}^{\frac{\gamma-j}{\sqrt{2}}} e^{-t^2} \sqrt{2}\, dt \;=$$

$$= \frac{1}{\sqrt{\pi}} \frac{1}{\operatorname{erf}\left(\frac{\gamma}{\sqrt{2}}\right)} \frac{1}{\sqrt{e}} \frac{\sqrt{\pi}}{2} \left[\operatorname{erf}\left(\frac{\gamma - \mathrm{j}}{\sqrt{2}}\right) - \operatorname{erf}\left(\frac{-\gamma - \mathrm{j}}{\sqrt{2}}\right)\right] =$$

dato che $\operatorname{erf}(-\mathrm{z}) = -\operatorname{erf}(\mathrm{z})$

$$= \frac{1}{\operatorname{erf}\left(\frac{\gamma}{\sqrt{2}}\right)} \frac{1}{\sqrt{e}} \frac{1}{2} \left[\operatorname{erf}\left(\frac{\gamma - \mathrm{j}}{\sqrt{2}}\right) + \operatorname{erf}\left(\frac{\gamma + \mathrm{j}}{\sqrt{2}}\right)\right] =$$

inoltre $\operatorname{erf}(\mathrm{z}^*) = \operatorname{erf}(\mathrm{z})^*$

e $\dfrac{z + z^*}{2} = \operatorname{Re}\{\mathrm{z}\}$

$$= \frac{\operatorname{Re}\left\{\operatorname{erf}\left(\frac{\gamma+\mathrm{j}}{\sqrt{2}}\right)\right\}}{\sqrt{e}\operatorname{erf}\left(\frac{\gamma}{\sqrt{2}}\right)} \tag{4.3}$$

Avendo scelto questa distribuzione per ϵ_n, abbiamo quindi i seguenti risultati:

$$\mu_{sec} = \frac{\pi}{4} \frac{\operatorname{Re}\left\{\operatorname{erf}\left(\frac{\gamma+\mathrm{j}}{\sqrt{2}}\right)\right\}}{\sqrt{e}\operatorname{erf}\left(\frac{\gamma}{\sqrt{2}}\right)} \tag{4.4}$$

$$\sigma^2_{sec} = 1 - \left(\frac{\pi}{4} \frac{\operatorname{Re}\left\{\operatorname{erf}\left(\frac{\gamma+\mathrm{j}}{\sqrt{2}}\right)\right\}}{\sqrt{e}\operatorname{erf}\left(\frac{\gamma}{\sqrt{2}}\right)}\right)^2 \tag{4.5}$$

$$\Omega \approx \frac{N}{\sigma^2_{\mathrm{B}}} \left((N-1)\frac{\pi^2}{16} \left(\frac{\operatorname{Re}\left\{\operatorname{erf}\left(\frac{\gamma+\mathrm{j}}{\sqrt{2}}\right)\right\}}{\sqrt{e}\operatorname{erf}\left(\frac{\gamma}{\sqrt{2}}\right)}\right)^2 + 1\right) \tag{4.6}$$

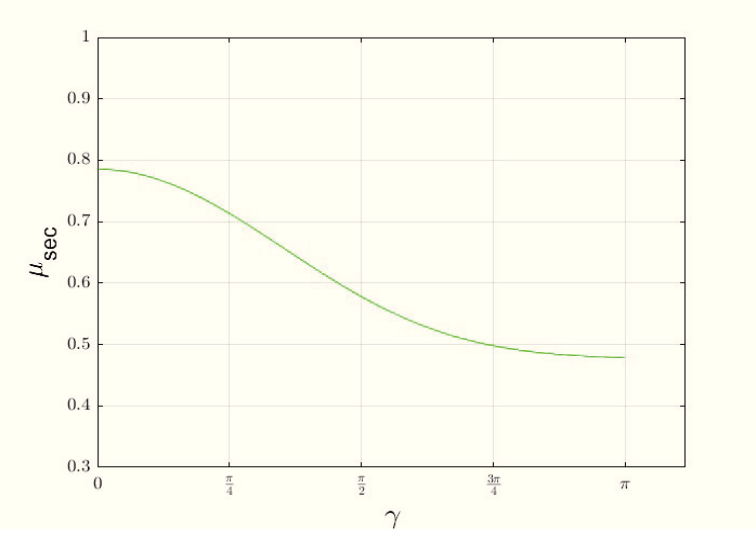

Figure 4.1: Andamento di μ_{sec}

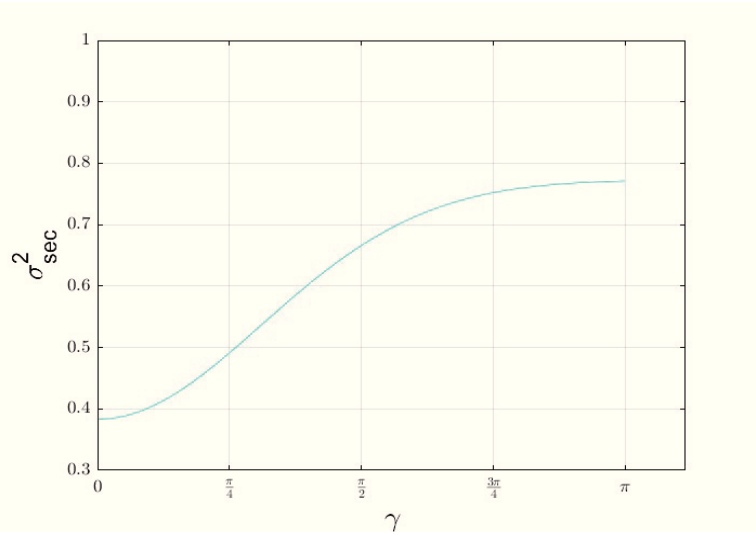

Figure 4.2: Andamento di σ^2_{sec}

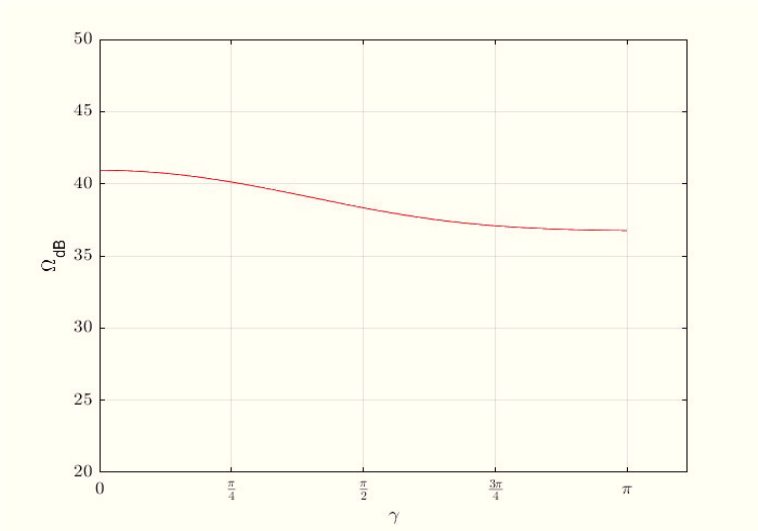

Figure 4.3: Andamento di Ω, scegliendo $N = 100$ e $\sigma_B^2 = 0.5$

Abbiamo simulato il comportamento di $H_{1,n}G_{n,1}e^{j\theta_n}$ con MatLab, generando 1000 realizzazioni e prendendone la media per 10 valori diversi di γ. Come possiamo vedere i pallini gialli si trovano sulla funzione di μ_{sec} che abbiamo riportato in verde, tracciata attraverso l'espansione in serie della funzione $\mathrm{erf(z)} = \frac{2}{\sqrt{\pi}} \sum_{\mathrm{n=0}}^{\infty} \frac{(-1)^{\mathrm{n}} \mathrm{z}^{2\mathrm{n}+1}}{\mathrm{n!(2n+1)}}$

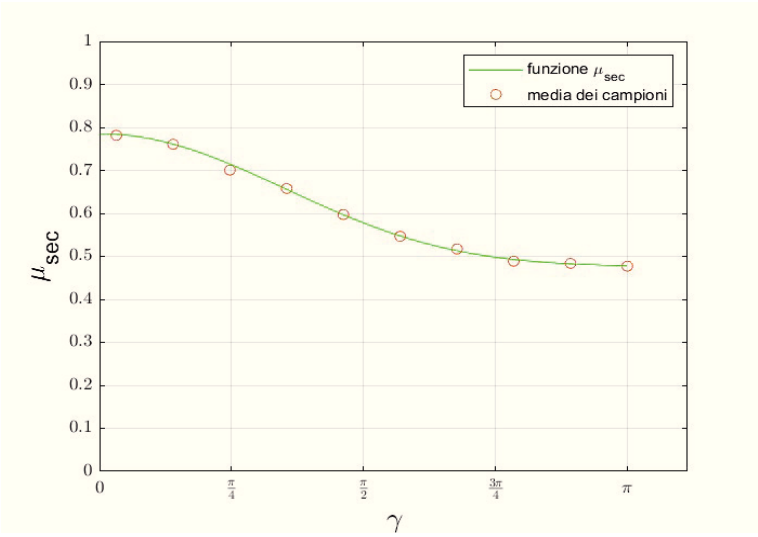

Figure 4.4: In giallo la media delle simulazioni di $H_{1,n}G_{n,1}e^{j\theta_n}$ per 10 valori diversi di γ.
In verde la funzione della media di $H_{1,n}G_{n,1}e^{j\theta_n}$

4.1.1 Attacco con completa conoscenza dei canali

Nel caso di antenna singola, per un attacco con completa conoscenza dei canali, δ avrà varianza reale e immaginaria pari a:

$$\sigma_{\mathrm{R}}^2 = \frac{1}{2}\left(1 - \frac{2\left(\mathrm{Re}\left\{\mathrm{erf}\left(\frac{\gamma+\mathrm{j}}{\sqrt{2}}\right)\right\}\right)^2}{e \cdot \mathrm{erf}\left(\frac{\gamma}{\sqrt{2}}\right)^2} + \frac{\mathrm{Re}\left\{\mathrm{erf}\left(\frac{\gamma+2\mathrm{j}}{\sqrt{2}}\right)\right\}}{e^2 \cdot \mathrm{erf}\left(\frac{\gamma}{\sqrt{2}}\right)}\right) \tag{4.7}$$

$$\sigma_{\mathrm{I}}^2 = \frac{1}{2}\left(1 - \frac{\mathrm{Re}\left\{\mathrm{erf}\left(\frac{\gamma+2\mathrm{j}}{\sqrt{2}}\right)\right\}}{e^2 \cdot \mathrm{erf}\left(\frac{\gamma}{\sqrt{2}}\right)}\right) \tag{4.8}$$

E correlazione incrociata:

$$\mathbb{E}\left[\left(\frac{\mathrm{Re}\left\{\mathrm{erf}\left(\frac{\gamma+\mathrm{j}}{\sqrt{2}}\right)\right\}}{\sqrt{e}\,\mathrm{erf}\left(\frac{\gamma}{\sqrt{2}}\right)} - \cos\epsilon\right)(-\sin\epsilon)\right] = 0. \tag{4.9}$$

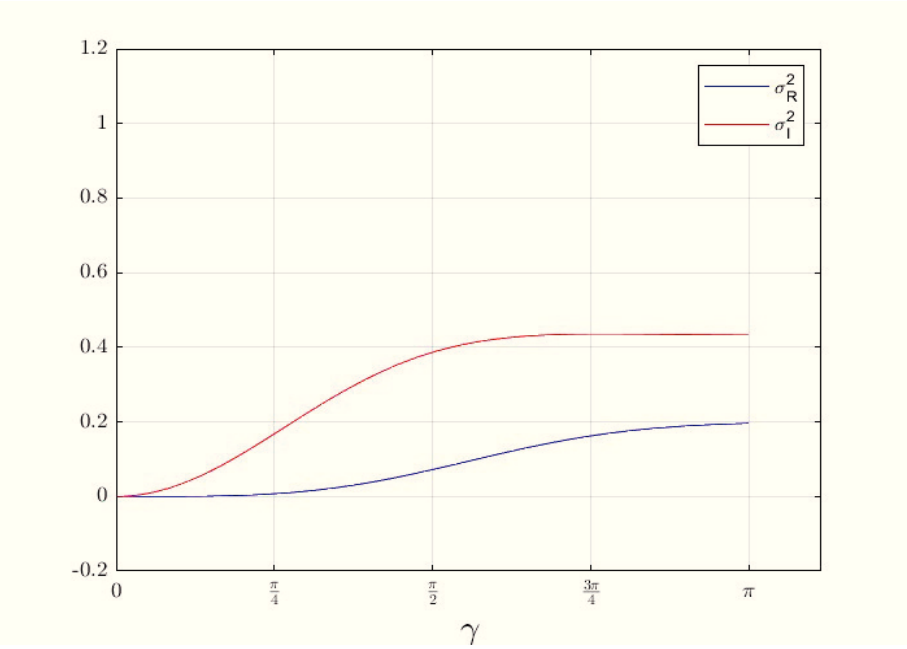

Figure 4.5: Andamento della varianza reale σ_R^2 (blu), della varianza immaginaria σ_I^2 (rosso), in funzione di γ

E andamento di $\bar{P}_{MD}$ al variare di γ scegliendo $N = 100$ e $\sigma^2 = 1$

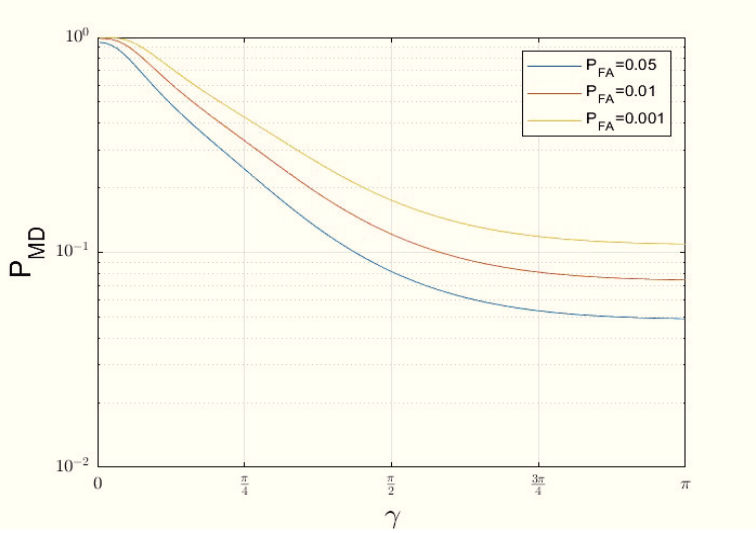

Figure 4.6: Andamento di P_{MD} al variare di γ con una densità clipped gaussian, $N = 100$ e $\sigma^2 = 1$

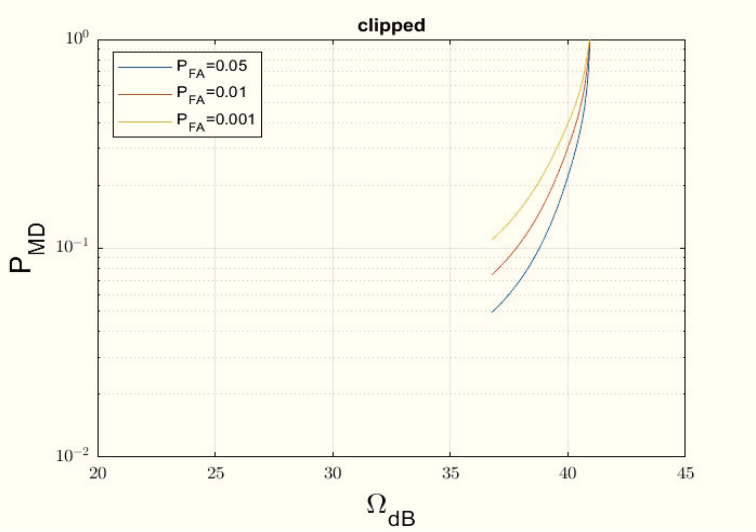

Figure 4.7: Andamento della P_{MD} rispetto ad Ω per una densità clipped gaussian, con $N = 100$, $\sigma^2 = 1$

4.2 Distribuzione uniforme

Se scegliamo di far variare ϵ_n tra $-\gamma$ e γ con una distribuzione uniforme, abbiamo i seguenti risultati:

$$\mathtt{m} = \frac{\sin\gamma}{\gamma} \tag{4.10}$$

$$\mu_{sec} = \frac{\pi}{4}\frac{\sin\gamma}{\gamma} \tag{4.11}$$

$$\sigma^2_{sec} = 1 - \left(\frac{\pi}{4}\frac{\sin\gamma}{\gamma}\right)^2 = 1 - \frac{\pi^2}{16}\frac{\sin^2\gamma}{\gamma^2} \tag{4.12}$$

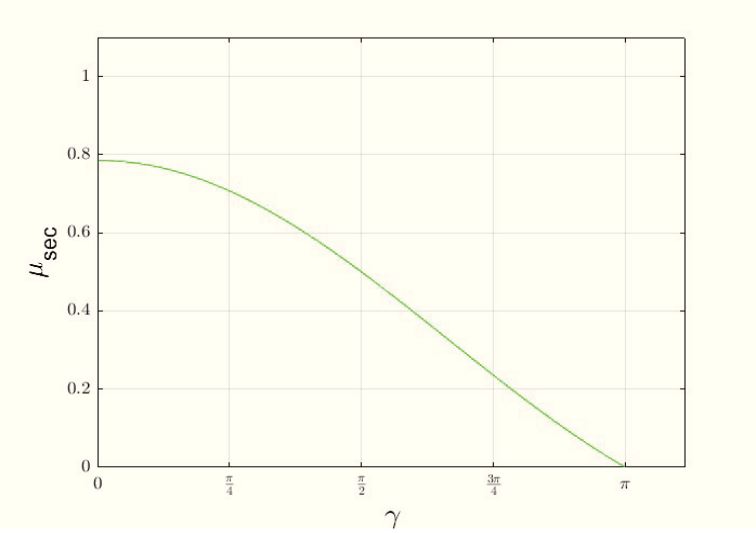

Figure 4.8: Andamento di μ_{sec}, con una distribuzione uniforme di γ

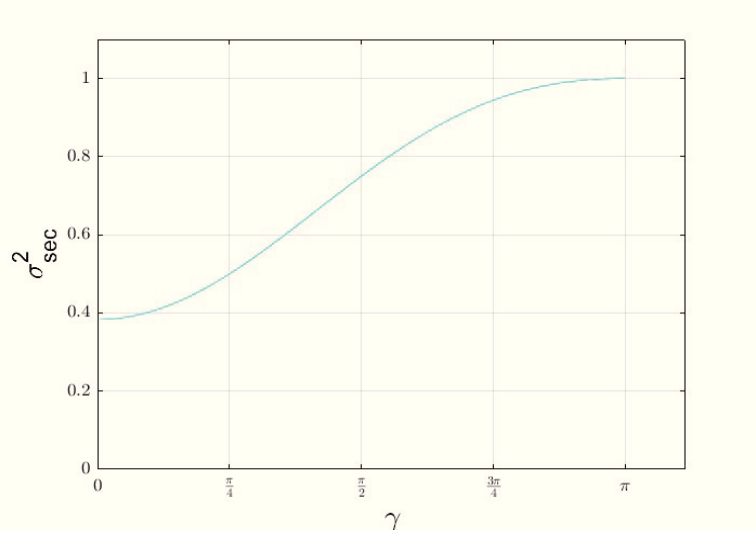

Figure 4.9: Andamento di σ^2_{sec}, con una distribuzione uniforme di γ

$$\Omega \approx \frac{N}{\sigma_{\mathrm{B}}^2}\left((N-1)\frac{\pi^2}{16}\frac{\sin^2\gamma}{\gamma^2}+1\right) \tag{4.13}$$

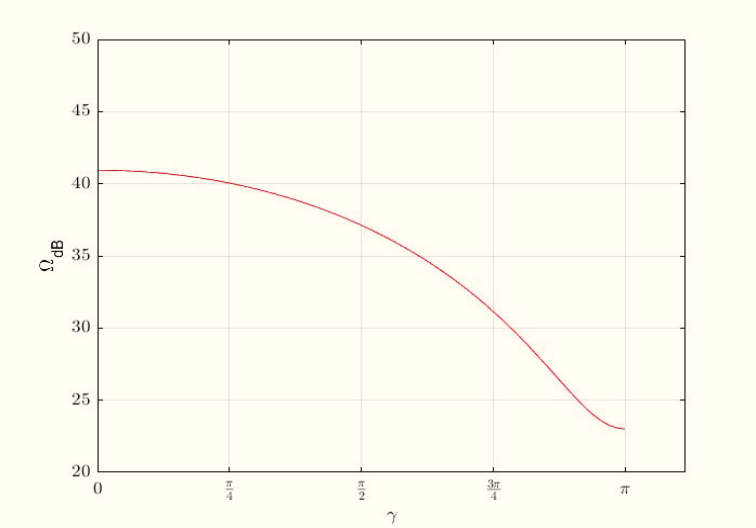

Figure 4.10: Andamento di Ω, scegliendo $N = 100$ e $\sigma_B^2 = 0.5$, con una distribuzione uniforme di γ

4.2.1 Attacco con completa conoscenza dei canali

Nel caso di antenna singola, per un attacco con completa conoscenza dei canali, δ avrà varianza reale e immaginaria pari a:

$$\sigma_{\mathrm{R}}^2 = \frac{1}{2}\left[\frac{\sin(\gamma)}{\gamma}\cos\gamma + 1 - 2\frac{\sin^2\gamma}{\gamma^2}\right] \tag{4.14}$$

$$\sigma_{\mathrm{I}}^2 = \frac{1}{2}\left[1 - \frac{\sin(\gamma)}{\gamma}\cos\gamma\right] \tag{4.15}$$

Con correlazione incrociata:

$$\mathbb{E}\left[\left(\frac{\sin\gamma}{\gamma} - \cos\epsilon_n\right)(-\sin\epsilon_n)\right] = 0 \tag{4.16}$$

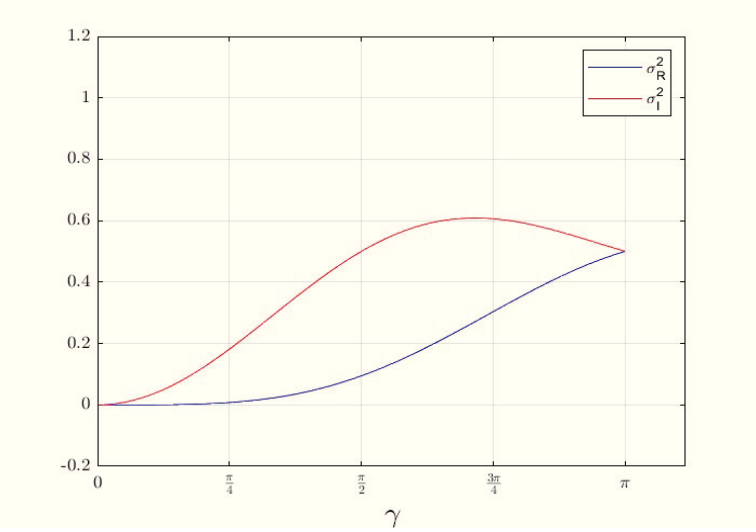

Figure 4.11: Andamento della varianza reale σ_R^2 (blu), della varianza immaginaria σ_I^2 (rosso), in funzione di γ, distribuita uniformemente

E andamento di $\bar{P}_{MD}$ al variare di γ scegliendo $N = 100$ e $\sigma^2 = 1$

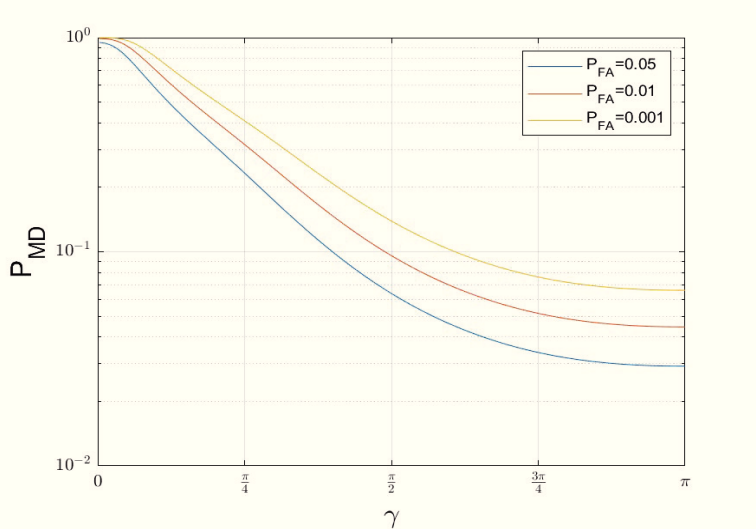

Figure 4.12: Andamento di P_{MD} al variare di γ con densità uniforme, $N = 100$ e $\sigma^2 = 1$

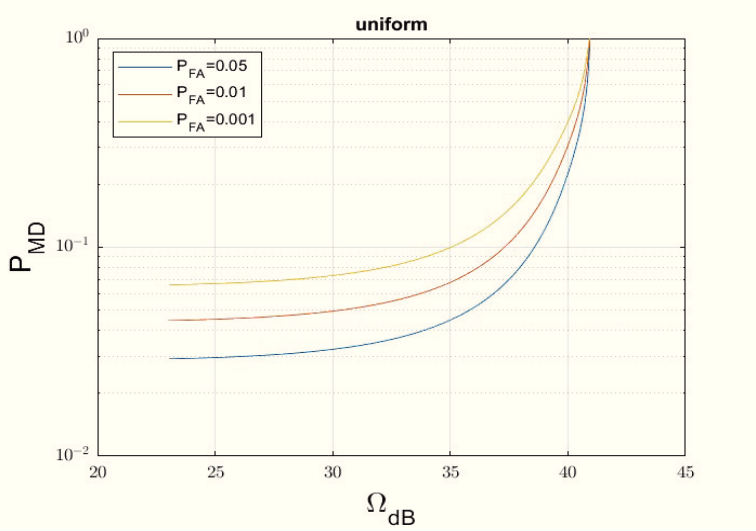

Figure 4.13: Andamento della P_{MD} in funzione di Ω per una densità uniforme, con $N = 100$, $\sigma^2 = 1$

5

Conclusioni

Abbiamo analizzato i casi in cui la densità di probabilità di ϵ_n poteva essere uniforme oppure clipped gaussian. Come ci aspettavamo, dai grafici riportati, possiamo osservare che, all'aumentare di γ, la probabilità di misdetection P_{MD} diminuisce, poichè utilizziamo un'intervallo più grande tra cui scegliere ϵ_n che determinerà la configurazione della IRS. Avendo un maggior numero di configurazioni, per Eve sarà più difficile forgiare un canale che le permetta di superare il controllo operato da Bob. Ampliando l'intervallo però, ci distanziamo sempre di più dalla configurazione ottimale, che otterremmo con $\gamma = 0$, diminuendo così il Ω.
Dal confronto delle due densità, osserviamo che, a parità di P_{MD}, risulta leggermente più vantaggioso utilizzare una densità clipped gaussian, rispetto ad una uniforme. Ma evidenziamo che aumentando γ, otteniamo una maggiore riduzione di P_{MD} con una densità uniforme, con il compromesso che questa maggiore sicurezza limiterà Ω.
La scelta di ricorrere ad una densità rispetto ad un'altra dipende comunque dal contesto di utilizzo di questo meccanismo di autenticazione. Se dovesse essere integrato con altri meccanismi ad alto livello allora potremmo preferire una densità che, a parità di P_{MD}, massimizzi la qualità della trasmissione; se invece la CR-PLS fosse la principale barriera contro attacchi malevoli, sarebbe preferibile una densità che punti a minimizzare la probabilità di successo dell'attacco.

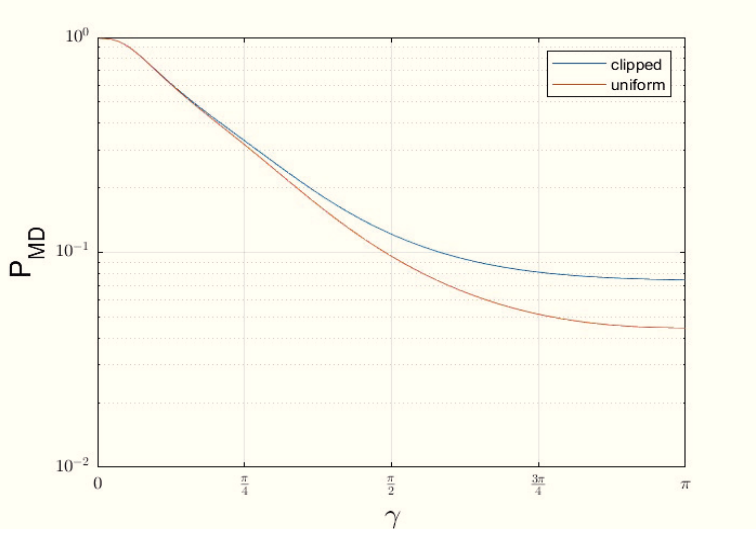

Figure 5.1: Confronto dell'andamento di P_{MD} al variare di γ tra densità uniforme e clipped gaussian, $P_{FA} = 0.01$, $N = 100$ e $\sigma = 1$

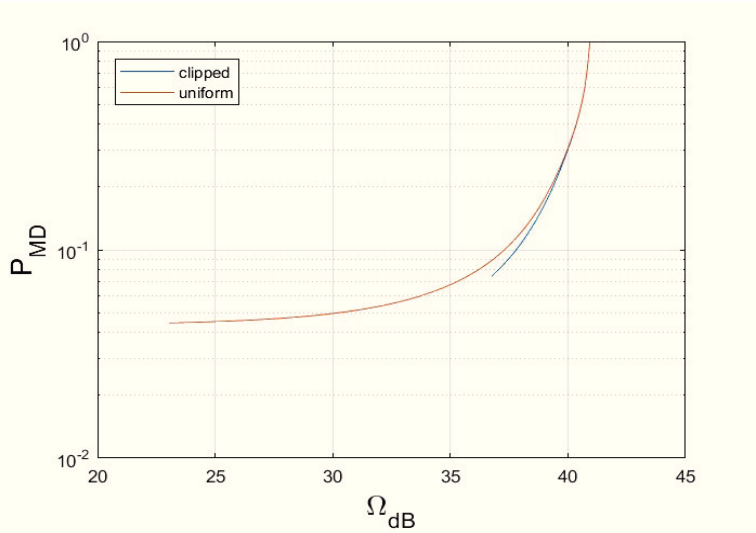

Figure 5.2: Confronto dell'andamento della P_{MD} in funzione di Ω tra una densità uniforme e clipped gaussian, con $N = 100$, $\sigma_B^2 = 1$ e $P_{FA} = 0.01$

6

Bibliografia

[1] L. Bai, L. Zhu, J. Liu, J. Choi and W. Zhang, "Physical layer authentication in wireless communication networks: A survey," in Journal of Communications and Information Networks, vol. 5, no. 3, pp. 237-264, Sept. 2020, doi: 10.23919/JCIN.2020.9200889.

[2] S. Tomasin, H. Zhang, A. Chorti and H. V. Poor, "Challenge-Response Physical Layer Authentication over Partially Controllable Channels," in IEEE Communications Magazine, vol. 60, no. 12, pp. 138-144, December 2022, doi: 10.1109/MCOM.001.2200339.

[3] Castaño-Martínez, A., López-Blázquez, F. Distribution of a sum of weighted noncentral chi-square variables. TEST 14, 397–415 (2005). https://doi.org/10.1007/BF02595410

7

Ringraziamenti

Grazie al professor Tomasin,
per avermi seguito durante la stesura di questa tesi.

Grazie ai miei compagni di università,
anche se ci siamo conosciuti solo in questo ultimo anno,
porterò con me ogni momento passato con voi,
sia quelli di ansia prima di un esame, sia quelli di gioia tutti insieme alla Murialdo.

Grazie ai miei amici,
alle persone con cui mi trovo più spesso,
a chi ho appena conosciuto ma ha già lasciato il segno,
a chi è distante ma un messaggio lo scrive sempre,
e a chi è rimasto presente nonostante le incombenze della vita,
con cui si fa presto a fare nottata, seduti a parlare attorno ad un tavolo per ore.

Grazie alla mia famiglia,
ai miei zii, che mi sostengono in ogni circostanza,
a mia sorella, che si affanna per me in cucina e che trova sempre un modo per punzecchiarmi,
a mio padre, che è stato l'esempio su cui ho fondato i miei valori e i miei princìpi,
a mia madre,
che ha affrontato tutto ciò che la vita ha scaraventato sul suo cammino,
che ha saputo farsi carico di ogni responsabilità con una forza e una determinazione senza pari,
che non ci ha fatto mai mancare nulla e il cui amore mi ha reso la persona che sono oggi.