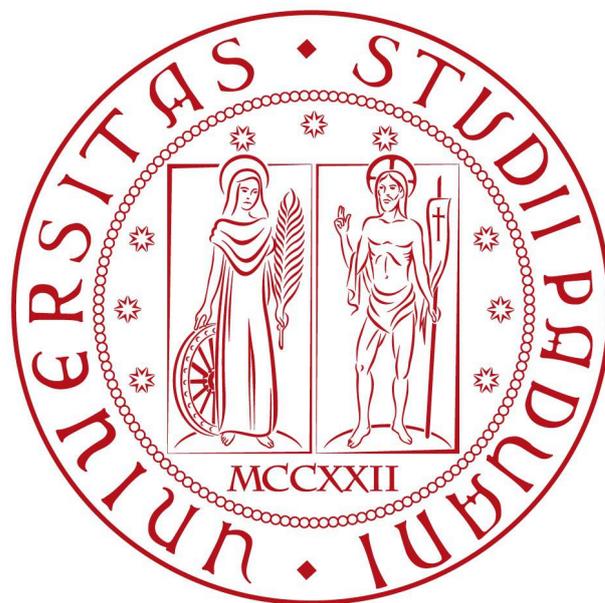


Università degli studi di Padova

Anno accademico 2012-2013

Dipartimento di Ingegneria dell'Informazione

Tesi di laurea triennale in Ingegneria dell'Informazione



# Un approccio induttivo a possibili innovazioni nel Jamming sfruttando la Teoria dell'Informazione

RELATORE: NICOLA LAURENTI

LAUREANDO: ALESSANDRO BELTRAMIN



*“It is not the things we do in life that we regret on our death bed. It is the things we do not.”*

Randy Pausch

*Ai miei genitori, Leandro e Roberta, e a mia sorella, Laura.*



# Indice

<b>I</b>	<b>Introduzione</b>	<b>3</b>
<b>II</b>	<b>Conoscenze preliminari</b>	<b>5</b>
<b>III</b>	<b>Osservazioni personali</b>	<b>7</b>
<b>1</b>	<b>Procedimento induttivo</b>	<b>7</b>
1.1	Sorgente di informazione . . . . .	7
1.2	Canale di trasmissione . . . . .	8
1.3	Ricevitore . . . . .	9
<b>IV</b>	<b>Sviluppo dei modelli</b>	<b>13</b>
<b>2</b>	<b>Giochi di potenza</b>	<b>13</b>
2.1	Lotta con l'ambiente . . . . .	13
2.2	Lotta con gli utenti . . . . .	14
2.3	Lotta con il Jammer . . . . .	15
2.4	Ottimizzazione energetica del Jammer . . . . .	17
<b>3</b>	<b>Giochi di informazione</b>	<b>19</b>
3.1	Canale numerico . . . . .	19
3.2	Canale Gaussiano . . . . .	21
3.2.1	A) Ipotesi di accesso al segnale codificato . . . . .	21
3.2.2	B) Ipotesi di accesso al segnale originale . . . . .	24
3.3	Conclusioni parziali . . . . .	25
<b>V</b>	<b>Modelli Avanzati</b>	<b>26</b>
<b>4</b>	<b>Controllo della Potenza</b>	<b>26</b>
<b>5</b>	<b>Correlazione probabilistica</b>	<b>26</b>
<b>VI</b>	<b>Conclusioni</b>	<b>29</b>
<b>6</b>	<b>Riferimenti bibliografici</b>	<b>32</b>



## Sommario

In ambito civile, il Jamming ha ricevuto attenzioni solo recentemente, a fronte dell'enorme diffusione dei telefoni cellulari e degli strumenti wireless. Spesso, l'elevato consumo di potenza nei disturbatori, causerebbe seri problemi di usura e costo, ma anche di compattezza e mobilità. Inoltre, un'inibizione indiscriminata porterebbe ad uno spreco enorme in termini energetici, con ripercussioni anche per la salute umana. Si pensi, ad es., ad un dispositivo per limitare l'utilizzo dei cellulari in un ospedale, o in altri luoghi pubblici. Per ridurre l'impatto ambientale, sarebbe interessante ingegnarsi per progettare apparecchiature più intelligenti, che siano efficaci ed efficienti dal punto di vista energetico.

Sulle stesse tracce della Teoria dell'Informazione del corso di Telecomunicazioni, vogliamo dunque intraprendere uno studio teorico, mirato a definire delle linee guida per la costruzione di un nostro "Optimum Jammer" (in simpatica contrapposizione allo studio dell'"Optimum Detector"). Utilizzeremo un approccio induttivo: "approccio", nel senso che ci poniamo da neofiti nel settore, utilizzando solo le conoscenze e gli strumenti a nostra disposizione; in maniera "induttiva", cioè basata sull'osservazione critica, di fenomeni, intuizioni ed idee, per lo sviluppo di modelli matematici e la ricerca di "possibili" soluzioni ingegneristiche.



---

## Parte I

# Introduzione

Utilizzati soprattutto in ambito militare, i Jammers nascono essenzialmente per contrastare i radar, ma anche per bloccare le comunicazioni del nemico. In ambito civile, il Jamming ha ricevuto attenzioni solo recentemente, a fronte dell'enorme diffusione dei telefoni cellulari e degli strumenti wireless. In parallelo si è sviluppato, inoltre, il settore dell'anti-jamming. Tra i motivi di tale ritardo, l'elevato consumo di potenza nei disturbatori, che causerebbe seri problemi di usura e costo, ma anche di compattezza e mobilità [1]. Inoltre, un'inibizione indiscriminata porterebbe ad uno spreco enorme in termini energetici, con ripercussioni anche nella salute umana [2]. Si pensi, ad es., ad un dispositivo per limitare l'utilizzo dei cellulari in un ospedale, o in altri luoghi pubblici. Per ridurre l'impatto ambientale, sarebbe interessante ingegnarsi per progettare apparecchiature più intelligenti, che siano efficaci ed efficienti dal punto di vista energetico.

Sulle stesse tracce della Teoria dell'Informazione del corso di Telecomunicazioni, vogliamo dunque intraprendere uno studio teorico, mirato a definire delle linee guida per la costruzione di un nostro "Optimum Jammer" (in simpatica contrapposizione allo studio dell'"Optimum Detector"). Utilizzeremo un approccio induttivo: "approccio", nel senso che ci poniamo da neofiti nel settore, utilizzando solo le conoscenze e gli strumenti a nostra disposizione; in maniera "induttiva", cioè basata sull'osservazione critica, di fenomeni, intuizioni ed idee, per lo sviluppo di modelli matematici e la ricerca di "possibili" soluzioni ingegneristiche.

---

La tesi è così strutturata:

- la Parte II indica le conoscenze sufficienti alla comprensione;
- la Parte III contiene le motivazioni e le osservazioni personali, che hanno spinto allo studio del problema;
- la Parte IV si occupa dello sviluppo di modelli basilari, partendo da abbozzi e rielaborazioni, frutto dell'interazione con quelli provenienti dalla letteratura;
- la Parte V presenta dei modelli avanzati, con scenari ben più complessi;
- la Parte VI riassume le conclusioni.

---

## Parte II

# Conoscenze preliminari

Come strumenti a disposizione per il nostro lavoro, daremo per note tutte le nozioni apprese durante il corso di Laurea Triennale in Ingegneria dell'Informazione, in particolare (Telecomunicazioni, Algebra Lineare, Analisi dei Dati)

Utilizzeremo inoltre conoscenze ausiliarie sulla Teoria dei Giochi, che sintetizziamo qui sotto in breve.

## Teoria dei Giochi

Un gioco strategico è un modello matematico di interazione tra decisori (giocatori), in cui ciascuno pianifica le proprie azioni una volta per tutte, simultaneamente. Vengono studiate le situazioni di conflitto, per ricercare soluzioni competitive e cooperative.

I giocatori, che si assumono razionali, assegnano un proprio valore di utilità a ciascuno dei risultati possibili, frutto delle decisioni congiunte dei vari decisori (dette *profili*), e orienteranno le proprie scelte a massimizzare ciascuno la propria utilità.

Il modello matematico prevede la definizione di una *funzione utilità* o *payoff*  $v(x)$ .

E' inoltre possibile assegnare un'utilità anche ad un evento aleatorio (di cui sia nota la distribuzione probabilistica) e definire quindi una *utilità attesa*, data dal valore atteso dell'utilità dei vari risultati.

Daremo particolare importanza ai "Giochi a somma zero" con due giocatori, come modello di tutte quelle situazioni in cui la contrapposizione dei due giocatori è totale: la vincita di un giocatore coincide esattamente con la perdita dell'altro.

Utilizzeremo il termine di "Minimax", come metodo per minimizzare la massima perdita possibile - o, in alternativa, per massimizzare il minimo guadagno ("Maximin") - ed il concetto di equilibrio di Nash.

---

## Parte III

# Osservazioni personali

## 1 Procedimento induttivo

Vengono presentate qui alcune osservazioni personali di partenza, emerse utilizzando solo come riferimento il testo [3]. Questo percorso darà poi seguito al lavoro di rielaborazione e ricerca bibliografica.

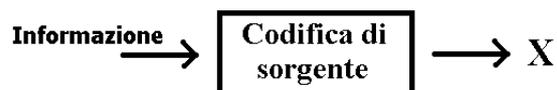
### 1.1 Sorgente di informazione

Si parta dal modello di trasmissione di un messaggio digitale [3, pag.162], secondo cui viene definita una variabile aleatoria discreta  $X$ , con un alfabeto finito su uno spazio di probabilità.

Si intende trasportare l'informazione attraverso il verificarsi di eventi nel tempo, nota la loro descrizione statistica.

Si definisce poi  $i_x$ , funzione informazione di  $X$ , e la rispettiva entropia  $H(X) = E[i_x(X)]$

Supposto di utilizzare  $X$  come sorgente, lo scopo del modello era trasmettere quanta più informazione possibile, massimizzando  $H(X)$  : di questo se ne occupa la codifica di sorgente.



Da come è stata formulata la Teoria dell'Informazione nel corso di Telecomunicazioni, si era ipotizzato che l'informazione non potesse mai calare (per la non-negatività della funzione informazione, imposta dall'Assioma A1 [3, pag.163]). Questo fatto ha sollevato alcuni dubbi e perplessità in merito, infatti in apparenza renderebbe la teoria poco adatta a modellare alcune situazioni in cui aggiungendo "qualcosa", si spera di limitare o addirittura negare l'informazione (attacco Denial of Service), e quindi far calare la funzione informazione.

Un eventuale Jammer sarebbe impossibilitato ad agire in questo contesto, perché risulterebbe non conveniente. Infatti con questa misura dell'informazione, aggiungendo un qualunque evento ( $B$ ) statisticamente indipendente ad uno già presente ( $A$ ), l'informazione congiunta  $i(A \cap B) = i(A) + i(B)$  risulterà sempre in una somma positiva delle rispettive informazioni trasportate (Assioma A4).

Si aprono allora due strade: modificare gli assiomi e ridefinire una funzione informazione più adatta a modellare un possibile intervento del Jammer - matematicamente difficoltosa - oppure cambiare fronte, sfruttando questa idea intuitiva di dover far calare l'informazione.

Si cambia fronte e si provano a studiare i passi successivi, necessari al trasporto dell'informazione.

## 1.2 Canale di trasmissione

In fase di trasmissione, l'informazione viaggia dalla sorgente  $X$  al destinatario  $Y$ , attraverso un canale (che avrà una certa modulazione, ma per ora si trascura): per semplicità si prenda il modello a Canale Numerico.

In questo ambito, il Jammer è sicuramente interessato a minimizzare l'informazione che giunge ad  $Y$ : una funzione adatta per gli scopi è data dall'informazione mutua tra  $X$  ed  $Y$  e definita come:

$$I(X, Y) = H(X) + H(Y) - H(X, Y) = H(X) - H(X|Y)$$

Intuitivamente, se l'entropia  $H(X)$  è considerata una misura dell'incertezza riguardo a una variabile aleatoria, allora  $H(X|Y)$  è una misura di ciò che  $Y$  non dice riguardo a  $X$ . Questo è "l'ammontare di incertezza che rimane riguardo a  $X$  dopo che  $Y$  è noto".

Dalla definizione risulta banalmente che  $I(X; X) = H(X)$ .

Poiché  $I(X; X) \geq I(X; Y)$ , si può affermare che una variabile aleatoria contiene almeno altrettanta informazione riguardo a se stessa di quanta ne può fornire una qualsiasi altra variabile.

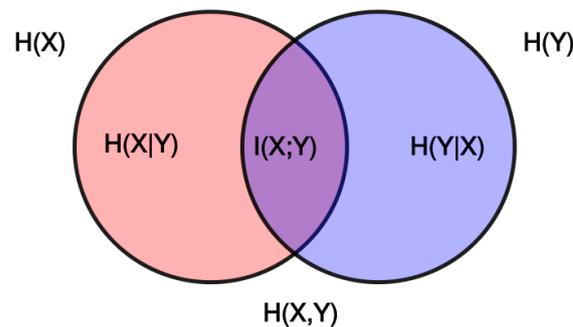
In sintesi, l'aver introdotto  $Y$  gioca a sfavore di  $X$ : **l'informazione è vulnerabile lungo il tragitto di trasmissione.**

Si osservi infatti la presenza del termine di sottrazione: il Jammer vorrà massimizzarlo, per minimizzare l'informazione mutua. Ma di quanto?

Esiste un bound teorico (vedi 6.68 pag.405 libro TLC):

$$0 \leq I(X, Y) \leq \min\{H(X), H(Y)\}$$

Secondo questo modello, il limite inferiore è raggiungibile se e solo se  $X$  ed  $Y$  sono statisticamente indipendenti tra loro.

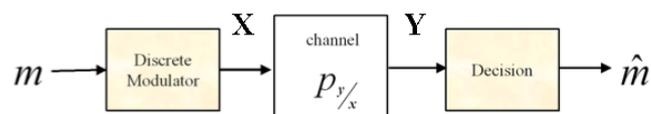


### 1.3 Ricevitore

Ci si pone ora sul “fronte” della Modulazione Digitale, osservando il ricevitore.

Nei sistemi di trasmissione dati, i segnali trasmessi attraverso canali fisici sono necessariamente analogici e a tempo continuo.

Grazie ai processi di modulazione e demodulazione è possibile ragionare su un modello di canale più semplice: quello Vettoriale Discreto. Qui i segnali analogici vengono mappati nelle loro rappresentazioni vettoriali.



**Optimum Data Detection** In questo contesto, il ricevitore lotta per la Optimum Data Detection, secondo cui deve massimizzare  $P_C$ , ossia la prob-

abilità di corretta rivelazione del messaggio trasmesso dalla sorgente.

$$P_c = 1 - P_e = 1 - P\{\hat{m} \neq m\} = P\{\hat{m} = m\}$$

Può agire adottando delle strategie di decisione, scegliendo tra vari criteri. Con il criterio ML, per il Teorema Minimax [4, pag.18], il ricevitore riesce a minimizzare la massima probabilità di errore media possibile, rispetto a tutte le distribuzioni del valore trasmesso, quando la distribuzione statistica dell'ingresso è sconosciuta e le probabilità di errore risultanti sono indipendenti dal valore trasmesso.

Ciò rappresenta un ostacolo non indifferente per un eventuale Jammer, interessato invece a massimizzare la Probabilità di errore.

In questo caso, l'unica alternativa più efficace sarebbe agire a posteriori rispetto al ricevitore (Jammer attivo, Trasmettitore inattivo), riuscendo a scoprire “qualcosa di più”, sia a livello statistico sia di funzionamento del ricevitore (es. Modulazione, Costellazione..), ipotizzando anche che il jammer abbia a disposizione un dispositivo di intercettazione.

**Idee su componenti irrilevanti** Si presentano infine, in maniera informale, alcune idee come spunto per sviluppi futuri.

Spesso il segnale ricevuto contiene informazioni che sono irrilevanti per determinare quale messaggio era stato trasmesso. Il ricevitore, sulla base del Teorema di Irrilevanza [4, pag.20], scarta le componenti che ritiene inutili, pur mantenendo invariata la Probabilità di errore.

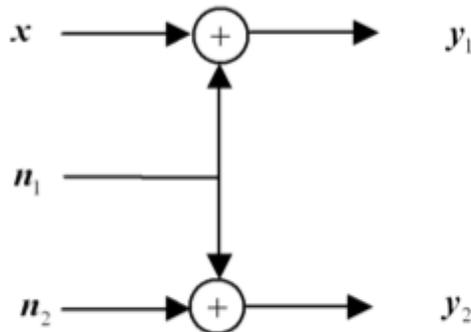
Ciò suggerisce che, ai fini del gioco competitivo, *il Jammer non debba sprecare energia in queste componenti irrilevanti.*

Il vettore che rappresenta il segnale di disturbo  $J \in L_2[0, T]$  dovrebbe quindi essere quanto più “parallelo” possibile allo spazio generato dalle componenti rilevanti, ossia le  $n$  basi ortonormali  $\{\phi_1, \dots, \phi_n\}$ .

Infatti, se le componenti ortogonali nello Spazio dei Segnali sono statisticamente indipendenti, il ricevitore le scarta sicuramente.

Se, invece, le componenti ortogonali nello Spazio dei Segnali sono stasticamente dipendenti, o correlate, con quelle parallele, si permetterebbe

addirittura al ricevitore di costruire una stima del segnale di disturbo e di riuscire, quindi, a cancellarlo parzialmente (per la Noise Cancellation).



Tutto ciò suggerisce l'idea che più si conosce riguardo la sorgente, il ricevitore ed il canale, più efficacemente si riesce a disturbare.

**Alcune precisazioni** Finora abbiamo sempre utilizzato impropriamente i termini “correlazione”, indipendenza e la nozione di ortogonalità.

E' fondamentale a questo punto non confondere l'indipendenza *lineare* e l'indipendenza *probabilistica*.

Bisogna precisare sempre su quali spazi lineari stiamo lavorando: Spazio dei Segnali o Spazio di Probabilità.

Lo Spazio di Probabilità è definito come l'insieme delle variabili aleatorie che ammettono secondo momento, ovvero:

$$S = \{X : \Omega \rightarrow \mathfrak{R} | E(X^2) < \infty\}$$

Lo Spazio dei Segnali invece è definito come: l'insieme dei segnali  $x(t)$ ,  $t \in \mathfrak{R}$  a tempo continuo con energia finita.

Quest'ultimo è stato utilizzato per ragionare geometricamente sull'parallelismo e ortogonalità a livello di costellazione; mentre vedremo, nelle prossime Sezioni, se si riveli effettivamente utile sfruttare gli stessi concetti dal punto di vista probabilistico.

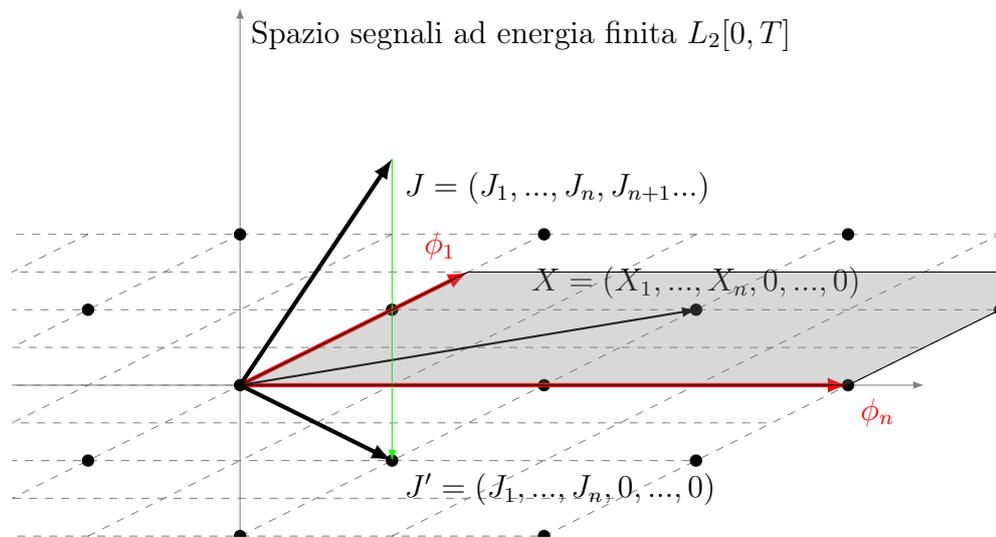


Figure 1: Dove potrebbe giacere un buon segnale di Jamming

## Parte IV

# Sviluppo dei modelli

## 2 Giochi di potenza

Viene presentato qui un percorso semplificato di rielaborazione personale, nota l'esistenza di modelli con scenari ben più variegati e complessi.

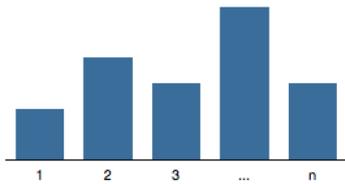
### 2.1 Lotta con l'ambiente

Un punto fondamentale di partenza è lo studio di come il trasmettitore lotti con l'ambiente per accesso al mezzo (medium access).

Presentiamo un modello interessante, in cui il trasmettitore cerca di spedire dell'informazione attraverso  $n$  risorse che il canale mette a disposizione, come potrebbero ad esempio essere degli slots temporali. Viene fissato un limite di potenza  $\bar{T}$ .

La suddivisione è definita dalla n-pla:

$$T = (T_1, T_2, \dots, T_n) \text{ con } T_i \geq 0 \text{ e tale che } \sum_{i=1}^n \pi_i T_i \leq \bar{T}$$



Ad ogni risorsa è stato inoltre associato un peso  $\pi_i > 0$ . Esso può essere interpretato come la capacità disponibile nei diversi intervalli di tempo e dipende da condizioni ambientali variabili, il cui stato varia in un insieme finito di stati  $i \in [1, n]$ , secondo un certo processo aleatorio ergodico e con distribuzione stazionaria  $\{\pi_i\}$ .

Si definisce l'SNR come:

$$SNR \triangleq \frac{T}{N}$$

La strategia del trasmettitore utilizza un approccio chiamato water-filling: si compensano cioè le perdite causate dalle disomogeneità nelle risorse del canale.

Una funzione obiettivo, in versione semplificata, è data quindi dal valore medio dell' $\boxed{\text{SNR}}$ :

$$v(T) = \sum_{i=1}^n \pi_i \frac{T_i}{N_i^0}$$

## 2.2 Lotta con gli utenti

Il trasmettitore si trova necessariamente a dover interagire anche con altre sorgenti di informazione, oltre che con l'ambiente.

Il documento [5] dunque caratterizza la competizione tra gli utenti per l'accesso al mezzo: vengono posti a confronto uno scenario cooperativo ed uno non-cooperativo tra le sorgenti per suddividersi le risorse di canale. Il modello di canale comprende inoltre un guadagno di fading, come indice di qualità del mezzo.

Viene spontaneo scegliere l'SINR come funzione obiettivo. Inoltre, a supporto della bontà della scelta, si nota l'esistenza di una relazione pressoché lineare tra SINR ed throughput, in regime di basso SINR. [5, pag.2]

Si definisce l'SINR del Trasmettitore 1 come:

$$\text{SINR} = \frac{\alpha_1 T_{(1)}}{N_0 + \alpha_2 T_{(2)}}$$

dove  $\alpha_j > 0$  sono i guadagni di canale del trasmettitore  $j$ ,  $N_0$  è il livello di rumore ambientale.

**Osservazione:** nella formula precedente, il termine al denominatore quantifica la potenza del rumore e comprende sia quello ambientale, sia quello dovuto alle altre sorgenti, considerandoli omogenei; tuttavia, intuitivamente, il segnale dovuto alle altre sorgenti potrebbe in qualche modo risultare più interferente, in quanto più "elaborato" rispetto al semplice rumore ambientale e più simile a quello della prima sorgente. In termini probabilistici, si

potrebbe definire più “correlato”. Vedremo in seguito (Sezione III) se si può fare qualcosa a riguardo.

Ritornando al modello proposto, nell’approccio non-collaborativo ogni utente tenta di massimizzare il suo  $\boxed{\text{SINR}}$  medio:

$$v_j(T_1, T_2) = \sum_{i=1}^n \pi_i \frac{\alpha_j^i T_j^i}{N_0^i + \alpha_j^i T_j^i}$$

Dove  $\alpha_j^i > 0$  sono i guadagni di fading dell’utente  $j$  quando l’ambiente si trova nello stato  $i$ , e  $\hat{j} = 3 - j$ .

Si suppone inoltre che tutti i guadagni di fading  $\alpha_j^i$ , i livelli di rumore  $N_0^i$  e le potenze totali  $\bar{T}_j$  siano note ad entrambi gli utenti.

Con opportune modifiche, questo scenario è particolarmente interessante per studiare un attacco Denial-Of-Service da parte di un Jammer.

## 2.3 Lotta con il Jammer

Si consideri il modello precedente e ci si ponga, ad esempio, nel contesto di una modulazione di tipo OFDM (Orthogonal Frequency-Division Multiplexing): le  $n$  risorse corrispondono ora alle diverse bande di frequenza che il canale mette a disposizione. La scelta di come assegnare diversi livelli di potenza tra i vari sotto-canali è ora un ottimo grado di libertà per l’azione di jamming. In questo caso si prenda un peso di  $\pi_i = \frac{1}{n}$  per ogni  $i$ .

Dal punto di vista della Teoria dei Giochi, si faccia riferimento al gioco del Colonnello Blotto, in cui i giocatori devono distribuire contemporaneamente delle risorse limitate su diversi “campi di battaglia”.

Il documento [6] tratta uno scenario simile: si suppone che jammer e trasmettore abbiano una quantità limitata di energia a disposizione, da suddividere a proprio piacimento tra vari sottocanali. Inoltre, Trasmettitore e Jammer non sono a conoscenza di come l’altro deciderà di distribuire le proprie risorse.

Nello scenario originale, però, il jammer è visto come avversario e si cerca la strategia ottima per il trasmettitore: tuttavia, per trovare il punto di equilibrio, vengono ugualmente studiate anche le strategie per il jammer.

La strategia del trasmettitore è definita dalla n-pla  $T = (T_1, \dots, T_n)$  con  $T_i \geq 0$ ,  $i \in [1, n]$ . Inoltre, fissata la potenza totale  $\bar{T} > 0$  a disposizione del trasmettitore, dev'essere rispettata la condizione:  $\sum_{i=1}^n T_i = \bar{T}$ , dove  $n$  è il numero di sottocanali e  $T_i$  è il livello di potenza assegnato ad ogni sottocanale  $i$ .

Allo stesso modo si definisce la strategia per il Jammer  $J = (J_1, \dots, J_n)$ .

Si suppone che i coefficienti di guadagno di fading  $\alpha_i$  e  $\beta_i$ , i livelli di rumore  $N^0$  e le potenze totali  $\bar{T}$  e  $\bar{J}$  siano tutti parametri noti ad entrambi i giocatori.

Dapprima si considerano i problemi di ottimizzazione: solo il jammer è attivo, mentre il trasmettitore fissa in anticipo la propria strategia, rendendola nota all'altro giocatore.

Poi si considera il caso in cui entrambi siano giocatori attivi.

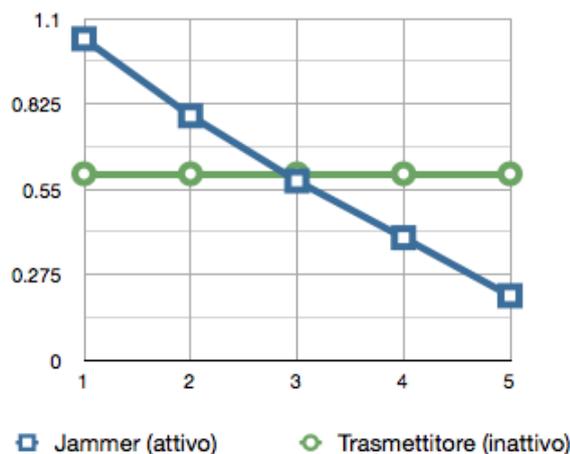
Il payoff per il trasmettitore è l'SINR medio, ossia:

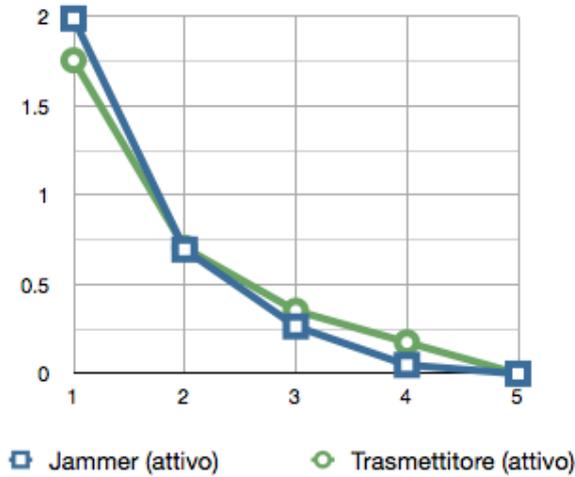
$$v_T(T, J) = \sum_{i=1}^n \frac{\alpha_i T_i}{N_0 + \beta_i J_i}$$

mentre, essendo un gioco a somma zero, il payoff per il jammer è:

$$v_J(T, J) = -v_T(T, J)$$

Con i dati ricavati dal documento [6], si è tracciato un grafico:





Per ipotesi, i canali sono stati ordinati per qualità decrescente (1 ottimo, 5 pessimo).

Viene mostrato come la strategia ottimale per il Jammer sia disturbare i sotto-canali con il più alto SINR atteso (sottocanali 1 e 2), privilegiandoli rispetto ai sotto-canali a più bassa qualità.

Tuttavia un Trasmettitore attivo, in risposta, potrebbe tentare di inviare una parte di informazione tramite i sottocanali a bassa qualità (sottocanali 3 e 4). Ciò rappresenta un punto di equilibrio per entrambi.

## 2.4 Ottimizzazione energetica del Jammer

A completamento di questo breve percorso illustrativo, si prova ad ottimizzare il jammer a livello energetico.

E' necessario scegliere una opportuna funzione obiettivo, che prenda in considerazione anche il costo energetico necessario per la trasmissione.

Il documento [7] suggerisce di utilizzare, in alternativa allo SINR, la Capacità di Shannon:

$$C = \log(1 + SINR)$$

E per entrambi i giocatori (T = Trasmettitore, J = Jammer), inserire un termine di Costo di trasmissione, con  $c_T > 0$  e  $c_J > 0$ .

Il rispettivo payoff risulta quindi:

$$v_T(J, N) = \sum_{i=1}^n \pi_i \ln \left( 1 + \frac{g_i T_i}{h_i J_i + N_i^0} \right) - c_T \sum_{i=1}^n \pi_i T_i$$

$$v_J(J, N) = - \sum_{i=1}^n \pi_i \ln \left( 1 + \frac{g_i T_i}{h_i J_i + N_i^0} \right) - c_N \sum_{i=1}^n \pi_i J_i$$

dove  $N^0$  è il livello di rumore incontrollato dell'ambiente allo stato  $i$ ,  $g_i > 0$  e  $h_i > 0$  sono i guadagni di fading per il canale quando l'ambiente si trova allo stato  $i$ . Si assume inoltre, come già visto in precedenza, che vi siano  $n$  risorse indipendenti, utilizzabili contemporaneamente da entrambi i giocatori, e per ogni risorsa vi sia un "peso" di  $\pi_i$ .

Osservando i payoff, si nota che il primo termine rappresenta il valore atteso della capacità di Shannon, mentre il secondo termine è il Costo medio della trasmissione.

Poiché quest'ultimo termine viene sempre sottratto, il gioco teorico, di fatto, non è più modellabile come problema a somma-zero.

I risultati sono comunque abbastanza confrontabili con quelli precedenti.

Infine, facciamo notare che le ipotesi in cui ci si è posti siano abbastanza restrittive e poco realistiche: sia nell'assumere una proporzionalità di scambio tra bit e potenza (il coefficiente del costo è infatti un rapporto tra unità di misura differenti), sia nel peso delle risorse.

## 3 Giochi di informazione

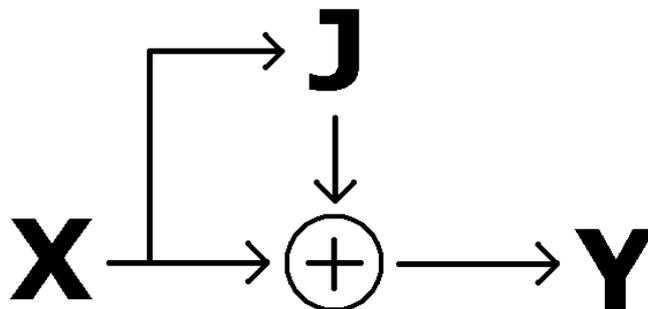
### 3.1 Canale numerico

Nella Sezione precedente (II) abbiamo intuito che il rumore, a denominatore dell'SINR, potesse contenere *un termine più “elaborato” rispetto al semplice rumore ambientale  $N_0$* . Si supponga allora che questo rumore interferente sia controllato da un Jammer, intelligente dal punto di vista della Teoria dell'Informazione.

Nella Sezione I, inoltre, ci siamo chiesti: *conoscendo di più, riguardo la sorgente, quanto meglio si riesce a disturbare? In che modo?*

**Ipotizziamo allora che il Jammer abbia pieno accesso al segnale della sorgente.**

*Proviamo a costruire da noi il modello più semplice che ci venga in mente, lavorando con il Canale Numerico introdotto nella Sezione I, che sia additivo.*



Dove  $X$  è la Sorgente,  $Y$  il Ricevitore,  $J$  il Jammer.

Sia:

$$J = f(X),$$

con  $f$  funzione deterministica,

mentre:

$$Y = X + J$$

Vorremo in qualche modo minimizzare la  $I(X, Y)$  e portarla a zero (limite teorico inferiore, dato dal bound della Sezione I).

Scegliendo **banalmente**

$$J = f(X) = -X,$$

potremo ottenere

$$Y = X + J = X + (-X) = 0$$

Poiché l'entropia di una variabile aleatoria costante è nulla,

$$H(Y) = 0$$

Per il bound

$$0 \leq I(X, Y) \leq \min \{H(X), H(Y)\}$$

otteniamo quindi:

$$I(X, Y) = 0$$

che era il nostro obiettivo.

**Estensione del modello** *Estendiamo ora il nostro modello basilare a qualcosa di più complicato, magari inserendoci dei vincoli sulla potenza e supponendo anche che il Jammer possa inserire una propria componente aleatoria  $\eta$ ,*

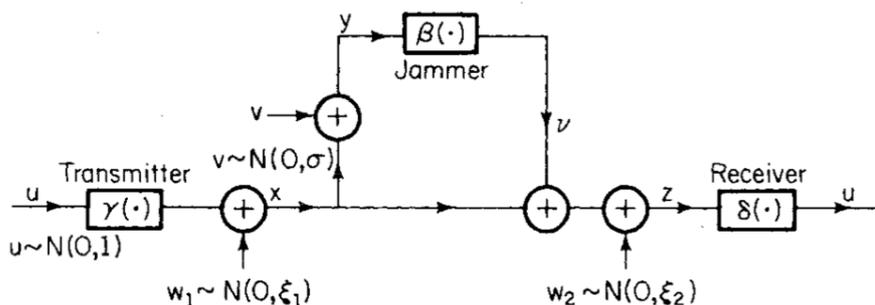
del tipo:

$$J = f(X) + \eta$$

### 3.2 Canale Gaussiano

Esiste uno scenario interessante che fa al caso nostro [8], sebbene consenta, inoltre, alla Sorgente di codificare il segnale tramite una mappa  $\gamma(\cdot)$ .

Ragioniamo su un modello di Canale Gaussiano, lineare, a canale unico, additivo e senza memoria, proposto in versione estesa:



#### 3.2.1 A) Ipotesi di accesso al segnale codificato

Il Jammer ha accesso al segnale codificato  $\gamma(u)$  trasmesso dalla Sorgente, in una versione corrotta da rumore, e può intervenire in retroazione nel canale,  $\nu = \beta(y)$ , così da modificare il segnale  $z$  in ingresso del Ricevitore.

*Scopo del Jammer è di distorcere quanto più possibile il segnale originale  $u$  (dopo aver definito opportunamente una misura della distorsione), rispettando dei limiti nella potenza.*

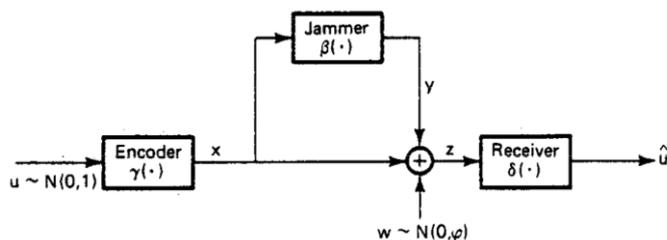
In questo scenario, la strategia di jamming più efficace è scegliere una **variabile aleatoria Gaussiana**, o una sequenza di variabili aleatorie Gaussiane i.i.d., che sia **correlata con il segnale in uscita dal Trasmettitore, in ingresso al Jammer**.

Inoltre, sotto particolari condizioni, la scelta del segnale di retroazione (come nel Canale Numerico visto prima!):

$$\beta^*(y) = -y$$

permetterebbe al Jammer di ottenere il massimo livello di distorsione possibile, cancellando di fatto la componente del segnale  $\gamma(x)$  dal segnale ricevuto  $z$ .

**Semplificazione del modello** Vediamo di esplicitare delle strategie utili, considerando uno scenario semplificato [9, Problema 3]:



Il Trasmettitore deve soddisfare al seguente limite di potenza:

$$\mathbb{E} \{[\gamma(u)]^2\} \leq c^2$$

Il Jammer deve soddisfare al seguente limite di potenza:

$$\mathbb{E} \{[\beta(u)]^2\} \leq k^2$$

Il rumore  $w \sim N(0, \varphi)$  è Gaussiano con media nulla e varianza  $\varphi > 0$

Al ricevitore arriva il segnale:

$$z = x + y + w = \gamma(u) + \beta(x) + w$$

Una misura della distorsione del segnale è data dall' Errore quadratico medio tra il segnale originale ed il segnale ricevuto.

Viene quindi scelto come payoff per il Jammer:

$$J(\gamma, \delta, \beta) = \mathbb{E} \{[u - \delta(z)]^2\}$$

Le strategie ottimali dipendono della scelta dei parametri  $k$ ,  $c$  e  $\varphi$ .

**Risultati:**

**Per  $k \geq c$ ,** ossia se il parametro di potenza del Jammer è più grande di quello del Trasmettitore:

scegliendo un segnale di retroazione

$$\beta^*(x) = -x$$

il Jammer riesce ad ottenere la massima distorsione possibile, ossia:

$$J^*(\gamma^*, \delta^*, \beta^*) = 1$$

qualunque sia il segnale  $\gamma^*(u)$  del trasmettitore.

**Per  $k < c$  e  $k^2 - ck + \varphi > 0$ :** per assicurarsi una distorsione di almeno:

$$J^*(\gamma^*, \delta^*, \beta^*) = \frac{\varphi}{(c - k)^2 + \varphi}$$

il Jammer deve scegliere come segnale:

$$\beta^*(x) = -\left(\frac{k}{c}\right)x$$

**Per  $k < c$  e  $k^2 - ck + \varphi \leq 0$ :** per assicurarsi una distorsione di almeno:

$$J^*(\gamma^*, \delta^*, \beta^*) = \frac{k^2 + \varphi}{c^2}$$

il Jammer deve scegliere come segnale:

$$\beta^*(x) = -\left(\frac{k^2 + \varphi}{c^2}\right)x + \eta$$

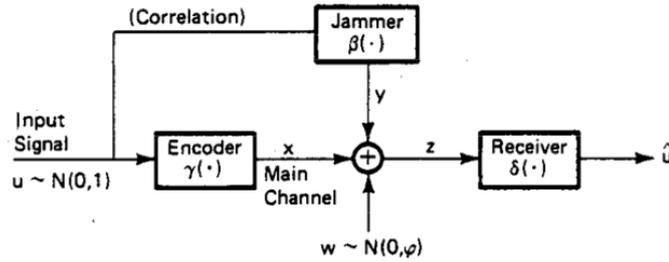
dove  $\eta$  è una variabile aleatoria Gaussiana a media nulla, con varianza  $k^2 - \frac{(k^2 + \varphi)^2}{c^2}$  ed indipendente da  $x$  e  $w$ .

*Notiamo come sia importante che il segnale di jamming **sia correlato con il segnale in uscita dal Trasmettitore.***

### 3.2.2 B) Ipotesi di accesso al segnale originale

Avevamo considerato il caso in cui il segnale di disturbo  $y$  introdotto dal jammer potesse avere accesso al segnale  $x$  in uscita dal trasmettitore.

Si suppone ora che possa, invece, avere accesso al segnale originale  $u$  in ingresso al Trasmettitore, prima che venga codificato tramite una qualche mappatura stocastica o deterministica ( $\gamma(u)$ ), sconosciuta al Jammer. Per semplicità, *consideriamo la codifica deterministica*.



**Risultati:** Non esiste un punto di equilibrio [9, Problem 2], ma vengono proposte solo le soluzioni Minimax e Maximin: la prima minimizza la massima perdita possibile, la seconda massimizza il minimo guadagno.

Si stanno cercando le strategie migliori per il Jammer: *dunque consideriamo la soluzione Maximin*.

Per assicurarsi un payoff di almeno:

$$J^*(\gamma^*, \delta^*, \beta^*) = \frac{k^2 + \varphi}{k^2 + \varphi + c^2}$$

la scelta del segnale di jamming ricade su:

$$\beta^*(u) = \eta \sim N(0, k^2)$$

dove  $\eta$  è una variabile Gaussiana con  $\mathbb{E}[u\eta] = 0$  e  $\mathbb{E}[\eta^2] = k^2$ , **indipendente da  $u$  e  $w$** .

*Sottolineiamo il fatto che la  $\beta$  ottimale debba necessariamente essere scorrelata con il messaggio originale di input:  $\mathbb{E}[u\eta] = 0$ .*

Infine, un'estensione dei risultati al Canale Vettoriale Gaussiano risulterebbe interessante, per esempi numerici si faccia riferimento a [10].

### 3.3 Conclusioni parziali

Notiamo una contrapposizione dei risultati tra le formulazioni (A) e (B): in quest'ultimo caso il segnale di jamming deve essere scorrelato con il segnale che dev'essere trasmesso, mentre nel primo dev'essere correlato con l'uscita dell'encoder. *Sarebbe interessante confrontarli con le intuizioni iniziali riguardo la correlazione della Sezione I, in cui erano state utilizzate tutt'altre tipologie di modelli.*

**Alcune impressioni aggiuntive** Nella ricerca di buon segnale per l'Optimum Jammer, si è visto che esso è Gaussiano, in qualche modo

“correlato con il segnale di uscita dal trasmettitore”

*(come se dovesse ricavare una stima probabilistica del trasmettitore e agire di conseguenza, distorcendo il contenuto informativo)*

e

“scorrelato con il messaggio originale da trasmettere”

*(quasi ad impedire di lasciarsi trapelare il contenuto informativo del messaggio originale a cui ha avuto accesso, ma anche per evitare di favorire la sorgente in talune circostanze. Vediamole.)*

Abbiamo detto che il Jammer non conosce la mappa di codifica. Potrebbe capitare che, per alcune mappe  $\gamma(\cdot)$ , un segnale di jamming correlato vada ad amplificare il segnale della sorgente, invece che attenuarlo. Una soluzione più prudente per il Jammer, la Maximin, è utilizzare la propria potenza quantomeno per innalzare il rumore. In questo scenario (B), quindi, crea più danni un segnale scorrelato.

## Parte V

# Modelli Avanzati

Nei capitoli precedenti abbiamo utilizzato le nostre idee un percorso di sviluppo di scenari basilari a scenari via via più complessi.

Pur avendo ragionato su modelli relativamente semplici, abbiamo trovato i parametri e le funzioni obiettivo più rilevanti, sempre rimanendo nell'ambito degli strumenti a nostra disposizione.

A questo punto il nostro lavoro di ricerca può ritenersi concluso, perché conduce all'utilizzo di strumenti e modelli ben più avanzati, specifici della disciplina delle Telecomunicazioni.

Ci limitiamo allora ad un lavoro di pura catalogazione bibliografica di alcuni scenari interessanti e dei risultati, come utile riferimento per ricerche future più avanzate.

## 4 Controllo della Potenza

Nei giochi di potenza, dove si utilizza l' $\boxed{\text{SINR}}$  come payoff, il Jammer spesso riesce a confondersi con il rumore ambientale, così da non essere rilevato.

Nel documento [11] vengono presentati esempi numerici di come evolva la distribuzione delle risorse nei canali, in base ad una conoscenza parziale sulla presenza del Jammer, da parte dell'Trasmettitore.

## 5 Correlazione probabilistica

Abbiamo intuito e osservato come il concetto di “correlazione probabilistica” sia particolarmente interessante se abbinato alla Teoria dell'Informazione.

Il documento [12] tratta esattamente questo contesto, riferendosi ad esso con il termine “*correlated jamming*”, ed estende alcuni risultati scoperti in precedenza.

Per alcune tipologie di canali, questo metodo può condurre ad attacchi particolarmente efficaci nel dominio delle *comunicazioni senza fili*, ma anche in quelle a *fibra ottica*. In queste ultime, infatti, i metodi tradizionali per la rivelazione del jamming, basati sulle variazioni della potenza ricevuta, sembrano non funzionare.

Si presentano, inoltre, degli scenari in cui il jammer ha una conoscenza parziale del segnale della sorgente [14, 15] e su canali avanzati, che distorcono sia in fase che nel tempo.

Vediamo alcuni risultati per un modello di canale a noi noto (il Canale AWGN), ma anche per altri.

**Canale AWGN** In un Canale AWGN in cui viene utilizzata come payoff l' Informazione mutua tra il segnale trasmesso e ricevuto,

il *nostro Optimum Jammer* deve semplicemente generare un segnale di disturbo che è la somma di due componenti:

-**una parte correlata** con il segnale trasmesso: in cui amplifica negativamente (con coeff.  $\geq -1$ ) il segnale del Trasmettitore

-**una parte indipendente**: in cui genera rumore AWGN, scorrelato con il segnale del Trasmettitore e con il rumore già esistente.

**Canale con Phase Jitter** Se il canale introduce un phase shift  $\phi$ , tempo-invariante, completamente sconosciuto al Jammer,

per l'*Optimum Jammer* è preferibile un tipo di jamming scorrelato.

**Canale con Time Jitter** E' possibile che vi sia un ritardo temporale tra i segnali, dovuto a problemi di sincronizzazione.

Si tratta di un Canale ISI tempo-invariante con AWGN

### Canale con fading Rayleigh

Sorprendentemente, in un Canale con fading Rayleigh, la conoscenza del segnale di ingresso è inutile ai fini del jamming [13].

In questo contesto, un Jammer che ha accesso al segnale del Trasmettitore **non riesce** a disturbare più di un Jammer che non ne ha accesso. Un segnale correlato rischierebbe, infatti, di favorire il Trasmettitore in certe situazioni. Poiché il fading di Rayleigh è simmetrico rispetto al segno, risulta più sicuro un segnale scorrelato, non solo come soluzione Maximin, ma anche come soluzione media.

---

## Parte VI

# Conclusioni

Per concludere, riassumiamo i parametri più rilevanti, le funzioni di payoff ed i modelli con cui abbiamo lavorato, ma anche quelli incontrati nel nostro percorso (in verde):

PARAMETRI DI INTERESSE:
Costellazione
Potenza
Qualità dei canali
Costo
Entropia

FUNZIONI DI PAYOFF:
Probabilità di Errore
SNR
SINR
Errore Quadratico Medio
Informazione Mutua
Capacità

MODELLI DI CANALE:
Numerico
Vettoriale Discreto
Gaussiano
Gaussiano Vettoriale
ISI
Fading Rayleigh

---

Abbiamo ricavato delle linee guida fondamentali per il progetto del nostro *Optimum Jammer*, efficiente dal punto di vista energetico. Abbiamo visto come debba:

- concentrare la propria potenza sulle bande di frequenza a maggior qualità,
- produrre un segnale di feedback che sia la somma di due componenti aleatorie: una parte correlata con il segnale della sorgente ed una parte scorrelata con il segnale della sorgente ed il rumore già presente.

$$J = f(X) + \eta$$

- Inoltre si è lasciata una questione aperta: nella Sezione I, si è intuito che debba anche imitare la modulazione digitale del Trasmettitore. A fronte del recente sviluppo di algoritmi [16] per il riconoscimento automatico della modulazione (AMR), questa risulta essere una possibile direzione per ricerche future.



## 6 Riferimenti bibliografici

- [1] Azzam, S., Hijazi, A. and Mahmoudy, A., “ Smart jammer for mobile phone systems ”, American University of Beirut, FEA Student Conference, 2004.
- [2] Mobile & Personal Communications Committee of the Radio Advisory Board of Canada, “Use of Jammer and Disabler Devices for Blocking PCS, Cellular & Related Services”, RABC Publication, 2001
- [3] Laurenti, N. (2011) “Sources of Digital Information” and “Channel Coding and Capacity”, in Principles of Communications Networks and Systems (eds N. Benvenuto and M. Zorzi), John Wiley & Sons, Ltd, Chichester, UK.
- [4] John M. Cioffi, “Signal Processing and Detection”, scaricabile in formato pdf al seguente link: <http://www.stanford.edu/group/cioffi/book/chap1.pdf>
- [5] E. Altman, K. Avrachenkov, “Transmission Power control game with SINR as objective function”, in Proc. of NET-COOP 2008. Lecture notes in computer science, vol 5425, pp 112-120, 2009
- [6] E. Altman, K. Avrachenkov, “Jamming in wireless networks under uncertainty,” 7th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless , 2009.
- [7] E. Altman, K. Avrachenkov, “A Jamming Game in Wireless Networks with Transmission Cost”, Proceedings of the 1st EuroFGI international conference on Network control and optimization, p.1-12, Avignon, France, 2007
- [8] T. Basar, “The Gaussian test channel with an Intelligent Jammer”, IEEE Trans. Inform. Theory. Vol. IT-29. No.1. pp.152-157. Jan. 1983.
- [9] Basar, T., ”A complete characterization of minimax, and maximin encoder-decoder policies for communication channels with incomplete statistical description,” IEEE Transactions on Information Theory , vol. 31, pp. 482-489, Jan., 1985.
- [10] Basar, T.; Ying-Wah Wu, "Solutions to a class of minimax decision problems arising in communication systems," Decision and Control, 1984. The 23rd IEEE Conference on , vol.23, no., pp.1182,1187, Dec. 1984

- [11] E. Altman, K. Avrachenkov and A. Garnaev, "Jamming game with incomplete information about the jammer," in Proc. of ICST/ACM International Workshop on Game Theory in Communication Networks, 2009.
- [12] M. Médard, "Capacity of Correlated Jamming Channels", Allerton Conference on Communications, Computing and Control, University of Illinois, 1997.
- [13] Kashyap, A.; Basar, T.; Srikant, R., "Correlated jamming on MIMO Gaussian fading channels," Communications, 2004 IEEE International Conference on , vol.1, no., pp.458,462 Vol.1, 20-24 June 2004
- [14] S. Shafiee and S. Ulukus "Correlated jamming in multiple access channels", Proc. Conf. Information Sciences and Systems, 2005
- [15] Wang, T.; Giannakis, G.B., "Mutual Information Jammer-Relay Games," Information Forensics and Security, IEEE Transactions on , vol.3, no.2, pp.290,303, June 2008
- [16] Dobre, O.A.; Abdi, A.; Bar-Ness, Y.; Su, W., "Survey of automatic modulation classification techniques: classical approaches and new trends," Communications, IET , vol.1, no.2, pp.137,156, April 2007