

POLITECNICO DI MILANO
Corso di Laurea in Ingegneria Informatica
Dipartimento di Elettronica e Informazione



Meccanismi di incentivazione basati su
teoria dei giochi per lo spectrum sensing
cooperativo

AI & R Lab
Laboratorio di Intelligenza Artificiale
e Robotica del Politecnico di Milano

Relatore: Ing. Nicola Gatti
Correlatore: Ing. Matteo Cesana

Tesi di Laurea di:
Davide Codoro, matricola 725164

Anno Accademico 2009-2010

Ai miei genitori

Sommario

Il lavoro qui presentato si colloca in uno scenario che sta all'intersezione tra lo studio della teoria dei giochi e la progettazione di sistemi relativi alle reti di telecomunicazione. La teoria dei giochi è importante perchè fornisce le basi per costruire meccanismi a reputazione che siano in grado di incentivare i giocatori ad avere un comportamento onesto e sincero mentre le reti di telecomunicazione forniscono l'ambito applicativo, che è quello dello spectrum sensing distribuito. L'obiettivo è proprio progettare un sistema per lo spectrum sensing distribuito che cerchi di evitare che utenti maliziosi riescano a manipolare a loro piacimento l'utilizzo di una certa frequenza. In questo lavoro viene quindi applicato un adeguato meccanismo di reputazione al modello di una generica rete per spectrum sensing distribuito, vengono studiati gli equilibri di Nash del sistema così ottenuto e se ne propongono variazioni, estensioni e valutazioni riguardo alle prestazioni.

Ringraziamenti

Ringrazio Nicola e Matteo per il tempo che mi hanno dedicato.

Indice

Sommario	I
Ringraziamenti	III
1 Introduzione	1
2 Stato dell'arte	5
2.1 Basi di teoria dei giochi	5
2.1.1 Giochi in forma strategica	6
2.1.2 Giochi in forma estesa	7
2.1.3 Giochi ripetuti	9
2.2 Il modello di Jurca-Faltings	10
2.2.1 Meccanismi a reputazione	10
2.2.2 Utilità attesa dei giocatori	12
2.2.3 Regola di pagamento	12
2.2.4 Equilibri	13
2.2.5 Aggiunta dei trusted report	14
2.3 Lo spectrum sensing	15
2.3.1 Energy detection	15
2.3.2 Distanze di interferenza	16
2.3.3 Spectrum sensing distribuito	17
3 Incentivi alla cooperazione nello spectrum sensing	19
3.1 Obiettivo del lavoro	19
3.2 Presentazione del modello	20
3.2.1 Elementi	20
3.2.2 Funzioni degli elementi	20
3.2.3 Interazioni	20
3.2.4 Dinamiche delle interazioni	21
3.2.5 Obiettivi dei giocatori	21
3.3 Applicazione del modello di Jurca-Faltings	22

3.3.1	Utilità attesa dei nodi	22
3.3.2	Regola di pagamento	23
3.3.3	Equilibri	23
3.4	Aggiunta del rumore	23
3.4.1	Probabilità di falso allarme e probabilità di miss	23
3.4.2	Utilità attesa in presenza di rumore	24
3.5	Aggiunta dei trusted report	24
3.5.1	Minimizzazione delle invocazioni del database	25
3.5.2	Calcolo di k^*	25
3.6	Funzione di aggregazione	26
3.6.1	Probabilità di errore globale del sistema	26
3.6.2	Scelta dei valori m e n	26
3.7	Esempio di funzionamento	27
3.7.1	Assenza di rumore	27
3.7.2	Presenza di rumore	28
4	Analisi del problema	31
4.1	Sensing perfetto	31
4.2	Introduzione degli errori nel sensing	32
4.3	Singolo rater, assenza di trusted report	32
4.4	n rater, assenza di trusted report	37
4.5	Singolo rater, presenza di trusted report	42
4.6	n rater, presenza di trusted report	52
4.7	Sintesi dei risultati	58
5	Estensioni al modello	61
5.1	Considerazioni sulle interferenze	61
5.1.1	Omogeneità dello stato delle banda nella rete	61
5.1.2	L'ingresso del raggio di interferenza	62
5.1.3	La posizione dei ricevitori	64
5.2	Precisione dei nodi in sistemi reali	65
5.2.1	Scelta della probabilità di miss	65
5.2.2	Clusterizzazione	66
5.2.3	Funzione di pagamento dinamica	66
5.2.4	Esempio di applicazione	67
5.3	Aggregatore distribuito	68
5.4	Stima delle caratteristiche di una frequenza	70
5.4.1	Il duty cycle	70
5.4.2	Contributo del duty cycle al modello degli equilibri	71
5.4.3	Un esempio applicativo: il caso delle frequenze TV	72

6	Analisi in simulazione	75
6.1	Contesto generale	75
6.2	Studio degli effetti degli errori di sensing	76
6.2.1	Probabilità di miss globale	76
6.2.2	Probabilità di falso allarme globale	78
6.2.3	Crediti dei nodi	82
6.3	Studio degli effetti dei nodi maliziosi	85
6.3.1	Probabilità di miss globale	86
6.3.2	Probabilità di falso allarme globale	89
6.3.3	Crediti dei nodi	91
6.4	Studio degli effetti dei cambiamenti di stato della banda	98
6.4.1	Probabilità di miss globale	98
6.4.2	Probabilità di falso allarme globale	101
6.4.3	Crediti dei nodi	101
6.5	Studio degli effetti dei nodi egoisti	105
7	Direzioni future di ricerca e conclusioni	111
7.1	Conclusioni	111
7.2	Sviluppi futuri	112
	Bibliografia	113
	A Simulatore	115

Capitolo 1

Introduzione

Il lavoro qui presentato si colloca in uno scenario che sta all'intersezione tra lo studio della *teoria dei giochi* e la progettazione di sistemi relativi alle reti di telecomunicazione. La teoria dei giochi è importante perchè fornisce le basi per costruire *meccanismi a reputazione* che siano in grado di incentivare i giocatori ad avere un comportamento onesto e sincero mentre le reti di telecomunicazione forniscono l'ambito applicativo, che è quello dello *spectrum sensing distribuito*. L'obiettivo è proprio progettare un sistema per lo spectrum sensing distribuito che cerchi di evitare che utenti maliziosi riescano a manipolare a loro piacimento l'utilizzo di una certa frequenza.

Lo spectrum sensing è stato proposto recentemente come soluzione a quella che da molti è percepita come una scarsità di frequenze su cui trasmettere [7]. Tale fenomeno è in parte dovuto a un'effettiva scarsità fisica di spettro, in parte a un'inefficiente allocazione delle frequenze stesse tramite rigide licenze di trasmissione. Questa rigidità porta infatti ad avere porzioni dello spettro scarsamente utilizzate perchè sotto licenza di trasmettitori poco attivi. Lo spectrum sensing propone che utenti senza licenza possano effettuare opportune misurazioni per determinare se una certa frequenza sotto licenza sia o meno in uso e, nel caso non lo sia, che questi stessi utenti possano accedervi in modo *opportunistico* per poter effettuare le loro trasmissioni. Un comportamento di questo tipo presuppone però il rischio che l'utente in possesso di licenza possa subire delle interferenze da parte di chi la licenza non la ha, nel caso in cui le misurazioni di quest'ultimo in merito allo stato della frequenza su cui si trasmette siano errate. Infatti tali misurazioni si basano normalmente su meccanismi di *energy detection*, e sono quindi soggette a effetti di rumore [6]. Di conseguenza l'utente opportunistico deve dotarsi di strumentazioni molto precise prima di poter trasmettere su frequenze sotto licenza altrui. Lo spectrum sensing distribuito offre un'alternativa a tale pro-

spettiva: nel caso in cui diversi utenti condividano le rispettive misurazioni sarebbero necessari sensori meno precisi, in quanto si avrebbero interferenze solo nel caso in cui diversi utenti effettuassero valutazioni errate. Già in [7] è tuttavia segnalato un problema collegato a questo approccio, relativo al livello di onestà di chi opera le misurazioni. Utenti intenzionati a utilizzare in modo esclusivo una data frequenza potrebbero per esempio fornire false misurazioni al sistema, per fare credere che tale frequenza, di fatto libera, sia invece occupata. Ecco quindi che sono necessari meccanismi a reputazione in grado di incentivare la condivisione di misurazioni sincere e di emarginare i trasmettitori disonesti. Soluzioni di questo tipo sono già largamente adottate nei siti per aste online come il celeberrimo *eBay* e in molti siti per valutazione di prodotti. Il contesto dello spectrum sensing ha tuttavia caratteristiche peculiari, e quindi è necessario scegliere un meccanismo adeguato. Esso dovrà tra le altre cose essere in grado di sfruttare la possibilità di avere valutazioni sicuramente corrette, ma potenzialmente costose, riguardo allo stato di una frequenza, che verosimilmente saranno fornite da un apposito database [4].

Il primo passo del lavoro è stata l'analisi dei sistemi a reputazione attualmente disponibili, alla ricerca di uno particolarmente adatto al contesto in esame. La scelta è caduta sul modello di Jurca-Faltings [8]. In seguito è stato costruito un modello di funzionamento generale per una sistema di spectrum sensing distribuito, e a esso si è applicato Jurca-Faltings. Nel fare ciò il modello a reputazione originale è stato modificato ed esteso al fine di gestire gli effetti di errori nelle valutazioni operate dagli utenti. La fase successiva è stata l'analisi degli *equilibri di Nash* del sistema, per assicurare che un comportamento sincero fosse in effetti incentivato. In questa fase si è studiato come gli equilibri varino al variare di ogni parametro significativo del modello, in modo da capire che tipo di valori siano ottimali per essi. In seguito sono state studiate alcune possibili estensioni del modello per gestire situazioni ed esigenze diverse e per sfruttare il più possibile le informazioni disponibili. Infine si è proceduto a un'analisi in simulazione delle prestazioni del sistema.

Nel Capitolo 2 viene presentato lo stato dell'arte in materia di teoria dei giochi, meccanismi a reputazione e spectrum sensing. Nel Capitolo 3 si passa alla descrizione del modello di una rete di spectrum sensing distribuito a cui viene applicato il meccanismo a reputazione di Jurca-Faltings, esteso in modo da gestire le specificità del contesto in esame. Nel Capitolo 4 vengono studiati gli equilibri di Nash del sistema ottenuto. Nel Capitolo 5 vengono proposte delle possibili modifiche o estensioni del modello per renderlo compatibile con situazioni diverse. Più nello specifico vengono espone alcune

considerazioni sull'effetto delle interferenze e viene analizzato come possano essere gestite le specificità degli utenti. Inoltre viene proposta una variazione in cui l'*aggregatore*, ossia l'agente che si occupa di raccogliere le valutazioni dei singoli utenti e di creare una valutazione collettiva, è a sua volta un utente opportunistico, e si discute di come sfruttare nel modello informazioni *a priori* relative all'utilizzo che il possessore della licenza fa della frequenza in esame. I risultati dell'analisi in simulazione sono poi presentati nel Capitolo 6, dove vengono valutati gli effetti sul sistema degli errori nel sensing, della presenza di nodi maliziosi ed egoisti e della variazione periodica dello stato della banda. Infine il Capitolo 7 è dedicato a considerazioni sui risultati ottenuti e su possibili sviluppi futuri. In appendice è riportato il codice del simulatore usato per ottenere i risultati numerici.

Capitolo 2

Stato dell'arte

In questo capitolo viene presentato lo stato dell'arte in merito agli ambiti correlati allo scenario in esame. Dapprima si introducono alcuni concetti fondamentali di teoria dei giochi, poi viene presentato il modello di Jurca-Faltings nel contesto dei meccanismi a reputazione, infine vengono esposte le principali tematiche relative allo spectrum sensing.

2.1 Basi di teoria dei giochi

La teoria dei giochi è lo studio matematico delle interazioni tra agenti indipendenti interessati a massimizzare il proprio utile [16]. La branca dominante della teoria dei giochi è quella che si occupa dei giochi *non cooperativi*, che si contrappone a quella che studia i giochi *cooperativi*. Nella prima l'unità base attorno a cui si costruisce il modello è il singolo agente, nella seconda il gruppo.

Nei giochi non cooperativi ogni agente associa a ogni possibile stato del mondo un valore numerico: ciò avviene tramite la *funzione di utilità*. Tanto più uno stato è appetibile per un agente, tanto più questo gli assegnerà un alto valore di utilità (o *payoff*). Evidentemente un agente interessato a massimizzare il proprio utile cercherà di trovarsi negli stati che per esso hanno il più alto possibile valore di utilità, e quindi agirà di conseguenza. Se poi nel gioco dovessero esistere elementi di casualità, si parlerà di *funzione di utilità attesa* in riferimento al valore atteso della funzione di utilità rispetto alla distribuzione di probabilità sugli stati. I giochi con queste caratteristiche sono detti *Bayesiani*.

2.1.1 Giochi in forma strategica

La forma più comune con cui si possono descrivere le interazioni tra i diversi giocatori è la *forma strategica*, o *normale* [16]. Essa prevede che gli stati del mondo dipendano dalle azioni combinate dei giocatori stessi.

Definizione 2.1.1 (Gioco in forma strategica) *Un gioco in forma strategica a n giocatori è una tupla (N, A, u) dove:*

- N è un insieme finito di n giocatori;
- $A = A_1 \times \dots \times A_n$, dove A è un insieme finito di azioni disponibili per il giocatore i . Ogni vettore $a = (a_1, \dots, a_n) \in A$ è chiamato profilo di azioni;
- $u = (u_1, \dots, u_n)$ dove $u_i : A \mapsto \mathfrak{R}$ è la funzione di utilità a valori reali del giocatore i .

I giochi in forma strategica vengono normalmente rappresentati tramite una matrice che indica, per ogni profilo di azioni, i valori di utilità dei diversi giocatori.

Nei giochi in forma normale è possibile seguire due tipi di strategie. Se si seleziona una singola azione e la si esegue si parla di *strategia pura*. Se invece si seleziona un insieme di azioni e a ognuna di esse si associa la probabilità con cui la si eseguirà si ha una *strategia mista*. L'insieme delle azioni associate a una probabilità strettamente positiva è detto *supporto* della strategia mista.

Per individuare le strategie che un giocatore dovrebbe seguire per massimizzare la propria utilità si possono seguire diversi approcci, il più utilizzato dei quali è quello basato sugli equilibri di Nash. Esso prevede per prima cosa l'introduzione della cosiddetta *best-response*.

Definizione 2.1.2 (Best-response) *La best-response del giocatore i al profilo di strategia s_{-i} è una strategia mista $s_i^* \in S_i$ t.c $u_i(s_i^*, s_{-i}) \geq u_i(s_i, s_{-i}) \forall s_i \in S_i$.*

Evidentemente tutte le azioni pure contenute nel supporto di una best-response avranno la stessa utilità attesa. A questo punto si può introdurre il concetto di equilibrio di Nash.

Definizione 2.1.3 (Equilibrio di Nash) *Un profilo di strategia $s = (s_1, \dots, s_n)$ è un equilibrio di Nash se, per ogni agente i , s_i è una best-response a s_{-i} .*

Nessun agente ha convenienza a deviare da un equilibrio di Nash se gli altri agenti continuano a seguirlo, quindi si tratta di un equilibrio stabile. A

Tabella 2.1: Tabella delle utilità per il dilemma del prigioniero.

Azione	C	NC
C	2, 2	-1, 3
NC	3, -1	0, 0

seconda che la best-response di ogni giocatore sia o meno unica si hanno equilibri di Nash rispettivamente *forti* e *deboli*. Se esse sono strategie miste, allora gli equilibri saranno necessariamente deboli.

Un classico esempio di gioco in forma strategica è il *dilemma del prigioniero*. Esso prevede due giocatori, che possono decidere se collaborare o meno. Se entrambi collaborano si ha un'utilità per entrambi maggiore rispetto al caso in cui nessuno lo faccia, mentre se a collaborare è solo uno dei due esso si ritrova nello stato con utilità minima e il suo avversario in quello a utilità massima. La tabella delle utilità di una delle tante versioni di questo gioco [13] è riportata in Tabella 2.1.

E' immediato notare che il profilo di azioni (C, C) non rappresenta un equilibrio di Nash, in quanto ogni giocatore potrebbe incrementare la propria utilità deviando da esso, ammesso ovviamente che l'altro non lo faccia. Il profilo (NC, NC) è invece un equilibrio di Nash, in quanto deviando da esso un giocatore potrebbe solo diminuire la propria utilità, sempre ammesso che l'altro non lo faccia.

2.1.2 Giochi in forma estesa

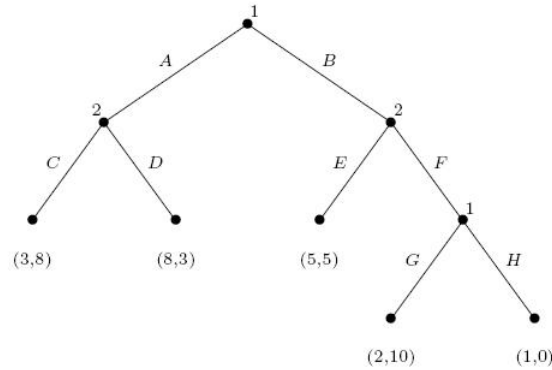
Nei giochi in forma normale i giocatori agiscono simultaneamente, non è possibile rendere l'aspetto temporale. Per fare ciò si deve passare ai *giochi in forma estesa* [16]. Nel caso di informazione perfetta (ossia quando i giocatori conoscono tutto riguardo al gioco e ai loro avversari) essi possono essere rappresentati tramite dei grafi ad albero, in cui i nodi rappresentano i punti di scelta dei giocatori, gli archi le possibili azioni e le foglie gli stati a cui si giunge, ognuno dei quali è associato al suo valore di utilità per i diversi giocatori.

Definizione 2.1.4 (Gioco a informazione perfetta in forma estesa)

Un gioco a informazione perfetta in forma estesa è una tupla $G = (N, A, H, Z, \chi, \rho, \sigma, u)$ dove:

- N è un insieme di n giocatori;
- A è un insieme di azioni;

Figura 2.1: Rappresentazione di un gioco in forma estesa.



- H è un insieme di nodi di scelta non terminali;
- Z è un insieme di nodi terminali, disgiunto da H ;
- $\chi : H \mapsto 2^A$ è la funzione azione, che assegna a ogni nodo di scelta un insieme di possibili azioni;
- $\rho = H \times A \mapsto H \cup Z$ è la funzione successore, che associa un nodo di scelta e un'azione a un nuovo nodo di scelta o a un nodo terminale t.c. $\forall h_1, h_2 \in H$ e $a_1, a_2 \in A$ se $\sigma(h_1, a_1) = \sigma(h_2, a_2)$ allora $h_1 = h_2$ e $a_1 = a_2$;
- $u = (u_1, \dots, u_n)$ dove $u_i : Z \mapsto \mathfrak{R}$ è una funzione utilità a valori reali per il giocatore i sui nodi terminali Z .

Il caso di informazione imperfetta richiede una trattazione in parte differente, che qui non verrà presentata. A tale proposito si introduce solo il concetto di *belief*, che indica l'insieme di convinzioni che un certo giocatore ha in merito agli aspetti del gioco di cui non è a conoscenza, per esempio i valori di utilità che un suo avversario associa ai diversi stati.

Ogni gioco a informazione perfetta in forma estesa ha almeno un equilibrio di Nash a strategia pura. E' anche opportuno introdurre il concetto di *storia* di un nodo, ossia la sequenza di scelte che portano dalla radice a esso. Un esempio di rappresentazione di un gioco in forma estesa è dato in Figura 2.1.

Osservando la figura è anche possibile capire perchè il concetto di equilibrio di Nash non è abbastanza restrittivo per risolvere giochi in forma estesa. Infatti $[(B, H)(C, E)]$ è un equilibrio di Nash, in quanto nessun giocatore può

incrementare la sua utilità deviando da esso, ammesso che l'altro continui a seguirlo. Tuttavia il giocatore 1 non avrebbe nessun motivo di scegliere H invece di G , si tratta solo di una minaccia non credibile per spingere il suo avversario a scegliere E . Per risolvere i giochi in forma estesa si introduce allora il concetto di *equilibrio di sottogioco perfetto*, dove per sottogioco si intende qualsiasi gioco in forma estesa il cui albero abbia radice in un nodo del grafo iniziale.

Definizione 2.1.5 (Equilibrio di sottogioco perfetto) *Un equilibrio di sottogioco perfetto di un gioco G è un qualsiasi profilo di strategia s t.c. per ogni sottogioco G' di G la restrizione di s a G' è un equilibrio di Nash di G' .*

Ogni equilibrio di sottogioco perfetto è un equilibrio di Nash, e ogni gioco in forma estesa ne ha almeno uno. Tornando alla Figura 2.1 si può notare come l'unico equilibrio di sottogioco perfetto sia $[(A, G), (C, F)]$.

2.1.3 Giochi ripetuti

La costruzione di un *gioco ripetuto* parte dal concetto di *stage-game* [13], che altro non è che un gioco in forma strategica o in forma estesa. Esso viene giocato in ogni periodo $t \in \{0, 1, \dots\}$. Con $p^t \in P^t$ si indica poi una storia che va dal periodo 0 al periodo $t - 1$. Per ogni storia $p^t \in P$ si definisce *gioco di continuazione* il gioco ripetuto infinitamente che inizia al periodo t , seguendo la storia p^t . Infine ogni stage game può generare una certa utilità. Poiché un guadagno in un futuro lontano viene normalmente valutato meno di un guadagno in un futuro prossimo ogni giocatore sconta questa utilità con il *fattore di sconto* $\delta \in [0, 1)$, cosicché l'*utilità scontata media* del giocatore i nell'infinita sequenza (u_i^0, u_i^1, \dots) è data da:

$$(1 - \delta) \sum_{t=0}^{\infty} \delta^t u_i^t$$

dove u_i^t indica l'utilità ottenuta nel periodo t .

Di fatto un gioco ripetuto può essere rappresentato in forma estesa come una sequenza di T stage-game, ognuno dei quali può essere un gioco in forma strategica o in forma estesa a sua volta. Quindi per analizzare gli equilibri si può riprendere il concetto di equilibrio di sottogioco perfetto, considerando come sottogiochi non solo gli effettivi sottogiochi dello stage-game, ma anche quelli che nascono concatenando i diversi stage-game giocati nei periodi successivi.

Definizione 2.1.6 (Equilibrio di sottogioco perfetto del gioco ripetuto)

Un profilo di strategia s è un equilibrio di sottogioco perfetto del gioco ripetuto se, per ogni storia $p^t \in P$, s è un equilibrio di Nash del gioco ripetuto che parte da p^t .

Tornando all'esempio del dilemma del prigioniero si può notare come se esso venga considerato lo stage-game di un gioco ripetuto si possano avere strategie nuove. Infatti, se il gioco viene ripetuto T volte, ogni giocatore i cercherà di massimizzare la somma scontata dei payoff, ossia;

$$(1 - \delta) \sum_{t=0}^T \delta^t u_i(a_i^t, a_{-i}^t)$$

Una strategia potrebbe essere quella in cui un giocatore coopera solo nella prima giocata e in ogni giocata che segua una in cui l'altro giocatore ha cooperato. Se entrambi i giocatori si comportano in questo modo si giunge al periodo n senza che nessuno abbia smesso di cooperare. A questo punto un giocatore può scegliere se continuare a cooperare, e avere quindi un payoff normalizzato scontato pari a 2, o smettere di cooperare, accettando un payoff pari a $3(1 - \delta)$. Se $2 \geq 3(1 - \delta)$, e quindi $\delta \geq \frac{1}{3}$, allora conviene continuare a cooperare.

2.2 Il modello di Jurca-Faltings

Verrà ora presentato il modello di Jurca-Faltings nel contesto dei meccanismi a reputazione.

2.2.1 Meccanismi a reputazione

Come si è visto nella versione ripetuta dell'esempio del dilemma del prigioniero, nei giochi ripetuti si individuano comportamenti che non possono apparire in interazioni isolate. Questo porta a introdurre il concetto di *reputazione*, che istituisce un legame tra azioni passate e azioni future attese [13].

Il concetto di reputazione è ampiamente sfruttato, spesso in modo solo intuitivo, nei sistemi per aste online come *eBay* e nei meccanismi di *peer-to-peer* (p2p), per evitare comportamenti disonesti nel primo caso, egoisti nel secondo. Sono stati anche proposti diversi modelli matematici per studiare gli effetti che la reputazione produce sulle azioni dei giocatori.

Un primo approccio cerca, a partire da uno stage-game dato, di creare un sistema di reputazione che spinga il più possibile i giocatori a giocare secondo

le regole. In [15] si cerca di fare questo nel caso delle aste online, partendo dal presupposto che ogni venditore ha una probabilità p di essere onesto, e quindi $1 - p$ di non esserlo. Il belief che gli acquirenti hanno relativamente a p varia nel tempo come il rapporto tra il costo delle transizioni positive e quello delle transizioni totali. Un aspetto interessante di questo modello è come riesca a combinare, nel definire le strategie degli acquirenti, la reputazione del venditore e la propria esperienza personale. In [2] viene invece proposto un meccanismo per incentivare la collaborazione tra nodi in reti p2p. Esso prevede che a ogni nodo venga associato un valore di utilità, funzione delle risorse e dei servizi a cui ha accesso e del costo per fornirli, e una reputazione: combinando questi valori è possibile aumentare la cooperazione e punire chi aiuta nodi egoisti. Un nodo può anche spendere la propria reputazione per ottenere risorse.

Un altro approccio cerca di costruire giochi in cui vengano imposti, tramite opportuni *incentivi*, gli equilibri di Nash desiderati. In [1] viene presentato un metodo generale per fare ciò, e il punto critico viene individuato nella fase di definizione di come i feedback vadano aggregati. Inoltre vengono sollevate delle perplessità in merito alle differenze tra modello e mondo reale, alla validità del concetto di fattore di sconto e al livello di razionalità degli essere umani. Figli di questo secondo approccio sono i modelli di Miller-Resnick-Zeckhauser [14] e quello di Jurca-Faltings [8].

Quello di Miller-Resnick-Zeckhauser è un meccanismo a reputazione che, tramite l'introduzione di appositi incentivi, garantisce che in un sistema di valutazione di un prodotto tramite dei feedback fornire un parere sincero sia l'equilibrio di Nash con l'utilità massima. Ciò avviene grazie all'utilizzo di *proper scoring rules*, ossia di funzioni che calcolano il pagamento per un giocatore in funzione della distribuzione di probabilità fornita da questo e dall'evento che poi effettivamente si è verificato [22][5]. La proprietà chiave è che il giocatore massimizza il suo pagamento quando la sua previsione coincide con il suo belief.

In contesti in cui il prodotto viene valutato in modo binario (buono o cattivo, attivo o inattivo, libero o occupato etc) e la valutazione dipende anche dal tempo è possibile utilizzare il più semplice modello di Jurca-Faltings. In estrema sintesi esso prevede che i giocatori osservino un segnale binario e forniscano la loro valutazione di esso, sempre binaria. Il pagamento avviene se la valutazione inviata da un giocatore corrisponde a quella inviata dal suo *rater*, ossia il giocatore che invia la valutazione successiva.

2.2.2 Utilità attesa dei giocatori

Jurca-Faltings prevede che l'utilità attesa di un giocatore che osserva il segnale s_i dipenda dallo stesso s_i , dalla strategia σ seguita dal giocatore e dalla strategia σ' seguita dal suo rater [8], secondo la formula:

$$E[\sigma, \sigma', s_i] = \sum_{j=1}^2 \alpha_j^i \cdot \left(\sum_{k=1}^2 Pr[s_k | s_i] \cdot \left(\sum_{l=1}^2 \beta_l^k \cdot R(s_j, s_l) \right) \right)$$

dove:

- s_1, s_2 è l'insieme dei possibili segnali;
- α_j^i indica la probabilità che il giocatore riporti il segnale j se ha osservato il segnale i (è quindi il parametro che definisce la strategia σ);
- $Pr[s_k | s_i]$ è la probabilità che il rater osservi il segnale s_k se il giocatore ha osservato il segnale s_i (è quindi il parametro che quantifica la correlazione tra segnali ricevuti in istanti di tempo successivi);
- β_l^k è la probabilità che il rater riporti il segnale l se ha osservato il segnale k (è quindi il parametro che definisce la strategia σ');
- $R(s_j, s_l)$ è la regola di pagamento.

2.2.3 Regola di pagamento

Una valutazione viene pagata una quota p_A se la valutazione fornita dal rater ha il suo medesimo valore, altrimenti viene pagata 0. E' stata scelta una soluzione di questo tipo poiché non è scontato che le informazioni su valutazioni passate possano essere tenute segrete al giocatore con cui si sta interagendo, quindi il pagamento deve dipendere da valutazioni future. Infatti, se il pagamento dipendesse non dalla valutazione successiva ma, per esempio, dalla valutazione precedente, un giocatore disonesto potrebbe in qualche modo risalire a questo valore e inviare una valutazione analoga al solo scopo di essere pagato [9].

La regola di pagamento è quindi:

$$R(s_j, s_l) = \begin{cases} p_A & \text{se } s_j = s_l \\ 0 & \text{altrimenti} \end{cases}$$

2.2.4 Equilibri

Una strategia di report σ è un equilibrio di Nash del meccanismo a reputazione se e solo se, per ogni segnale osservato, nessun giocatore razionale devia da σ se il rater segue σ .

In un contesto binario compatibile con gli incentivi riportare una valutazione sincera è un equilibrio di Nash, ma è possibile dimostrare che fornire sempre valutazioni positive o sempre valutazioni negative sono anch'essi equilibri. Inoltre, almeno uno di questi due equilibri garantisce un payoff maggiore di quello che si avrebbe con valutazioni sincere [8].

Dimostrazione 2.2.1 *Indicata con σ^* la strategia associata alle valutazioni sincere, si ha:*

$$E[\sigma^*, \sigma^*, s_1] \geq E[s_2, \sigma^*, s_1]$$

$$E[\sigma^*, \sigma^*, s_2] \geq E[s_2, \sigma^*, s_2]$$

Poiché $Pr[s_1|s_1] \geq Pr[s_1|s_2]$ si ha che:

$$R(s_1, s_1) \geq R(s_2, s_1)$$

$$R(s_2, s_2) \geq R(s_1, s_2)$$

Quindi:

$$E[s_1, s_1, \cdot] \geq E[s_2, s_1, \cdot]$$

$$E[s_2, s_2, \cdot] \geq E[s_1, s_2, \cdot]$$

Questo significa che riportare sempre lo stesso valore costituisce un equilibrio di Nash. Sia poi:

$$\rho = \max(R(s_1, s_1), R(s_2, s_2))$$

Allora:

$$\begin{aligned} E[\sigma^*, \sigma^*, s_1] &= Pr[s_1|s_1]R(s_1, s_1) + Pr[s_2|s_1]R(s_1, s_2) \leq \\ &Pr[s_1|s_1]R(s_1, s_1) + Pr[s_2|s_1]R(s_2, s_2) \leq \rho \end{aligned}$$

perciò almeno uno dei due equilibri a valutazioni costanti fornisce un payoff maggiore di quello che si ha nell'equilibrio delle valutazioni sincere.

Questo significa che il modello non è robusto rispetto alle *coalizioni*: infatti, se un gruppo abbastanza numeroso di giocatori si accordasse per fornire sempre la stessa valutazione, ognuno di loro avrebbe un payoff maggiore di quello che otterrebbe riportando valutazioni sincere.

2.2.5 Aggiunta dei trusted report

Per far sì che l'equilibrio a payoff massimo sia quello delle valutazioni sincere, e scoraggiare quindi le coalizioni, si possono introdurre i cosiddetti *trusted report* [8]. Se il rater è un'entità di tipo *trusted*, e quindi la sua valutazione è sempre vera, evidentemente fornire valutazioni sincere è l'unico equilibrio di Nash del sistema. Tuttavia le valutazioni fornite da entità *trusted* sono di norma costose, perciò vanno minimizzate. E' quindi necessario calcolare un valore k^* che indichi la probabilità che ha ogni valutazione di un giocatore di essere confrontata con una valutazione *trusted*. k^* deve essere il valore minimo sufficiente a garantire che la strategia σ^* di riportare valutazioni sincere sia l'equilibrio di Nash a payoff massimo:

$$k^* = \min(k) \text{ t.c. } f(k^*) = 0, f(k) = \max_{\sigma, s_i} E_k[\sigma^*, \sigma^*, s_i] \text{ t.c. } \sigma \text{ è un equilibrio di Nash}$$

Il calcolo di k^* può essere effettuato tramite la seguente formula:

$$k^* = \max \left(\frac{1 - Pr'[-|-]}{Pr'[-|-]}, \frac{1 - Pr'[+|+]}{Pr'[+|+]} \right)$$

dove + e - indicano i due possibili valori dei segnali e delle valutazioni e le due probabilità indicano le correlazioni di questi valori in istanti successivi.

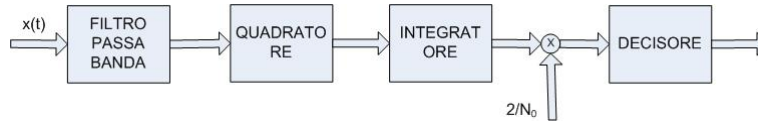
Va notato che il valore k^* serve per portare il sistema da una qualsiasi situazione iniziale all'equilibrio di Nash della valutazione sincera. Una volta che vi si è giunti si può smettere di usare le valutazioni *trusted*. Infatti, quando ci si trova in un certo equilibrio, per passare a un certo altro equilibrio è necessario che una parte considerevole dei giocatori inizi a giocare secondo il nuovo equilibrio. Solo in questo caso seguire la strategia legata al nuovo equilibrio diventa razionale. In Jurca-Faltings quindi, perché smetta di essere razionale essere sinceri, sarà necessario che almeno una percentuale pari a $1 - k^*$ dei nodi si accordino per seguire la strategia legata a un altro equilibrio [8].

Un altro modo per incentivare l'equilibrio associato alle valutazioni sincere prevede di non considerare più un singolo rater, ma un numero n di essi. Il pagamento potrebbe allora avvenire nel caso in cui tutti i rater tranne uno siano d'accordo con la valutazione inviata dal giocatore, abbattendo così l'utilità garantita dagli equilibri associati a valutazioni sempre positive o sempre negative [10].

Infine, nel caso ci si trovi in un certo equilibrio di Nash σ , è possibile calcolare la k_σ necessaria per passare da σ all'equilibrio delle valutazioni sincere [8]. Essa è pari a:

$$k_\sigma = \max_{s_i} \frac{E[\sigma, \sigma, s_i] - E[\sigma^*, \sigma^*, s_i]}{E[\sigma, \sigma, s_i] - E[\sigma, \sigma^*, s_i]}$$

Figura 2.2: Rappresentazione di un meccanismo di energy detection.



2.3 Lo spectrum sensing

Negli ultimi decenni si sono iniziati a percepire alcuni limiti nella disponibilità di frequenze su cui trasmettere, in particolare per quanto riguarda gli operatori senza licenza. D'altra parte l'utilizzo relativamente basso delle frequenze sotto licenza, a cominciare da quelle destinate alle trasmissioni televisive, suggerisce che questi limiti siano dovuti più a un'inefficiente allocazione delle frequenze stesse che a un'effettiva mancanza fisica di spettro [7].

Questa situazione ha portato alla necessità di meccanismi di spectrum sensing, ossia tecniche che consentano a un trasmettitore di determinare se su una certa banda di frequenza vi sia o meno una trasmissione in corso. Se non c'è trasmissione significa che la banda è disponibile, e il trasmettitore stesso potrebbe usarla. Ciò può consentire un accesso opportunistico da parte di dispositivi senza licenza (o secondari) a frequenze sotto licenza (di dispositivi primari), ma che al momento non sono in uso. Questo comporta ovviamente il rischio, nel caso si valuti in modo errato lo stato della banda, di creare interferenze con le trasmissioni del possessore della licenza, quindi il sensing deve essere ragionevolmente preciso. Inoltre non è possibile trasmettere su una certa banda e nello stesso tempo effettuare rilevazioni su di essa, perciò bisogna prevedere che le trasmissioni secondarie debbano essere periodicamente sospese per rilevare se un trasmettitore primario abbia eventualmente iniziato a usare la banda.

2.3.1 Energy detection

Il trasmettitore secondario, per valutare lo stato della banda, può misurare l'energia ricevuta in un certo intervallo di tempo, e dichiarare la banda libera se essa è inferiore a una certa soglia. Questo metodo prende il nome di energy detection [6]. Tuttavia non è possibile discriminare l'energia generata da una trasmissione dall'energia generata da fonti di rumore, quindi la valutazione è soggetta a errori.

Più in dettaglio, un meccanismo di energy detection come quello illustrato in Figura 2.2 prevede i seguenti componenti:

- un filtro passa-banda, per eliminare il rumore presente su frequenze diverse da quella in esame;
- un dispositivo che eleva al quadrato il segnale ricevuto, per misurare l'energia;
- un integratore, che valuta l'energia raccolta nell'intervallo di tempo;
- un moltiplicatore, che normalizza il valore ottenuto dividendolo per $N_0/2$;
- un decisore, che confronta il risultato con un valore soglia γ . Se esso è maggiore di γ allora la banda viene considerata occupata, altrimenti libera.

Questo problema viene spesso formulato come un test di ipotesi, nella forma:

$$x(t) = \begin{cases} n(t) & H_0 \text{ (banda libera)} \\ hs(t) + n(t) & H_1 \text{ (banda occupata)} \end{cases}$$

dove:

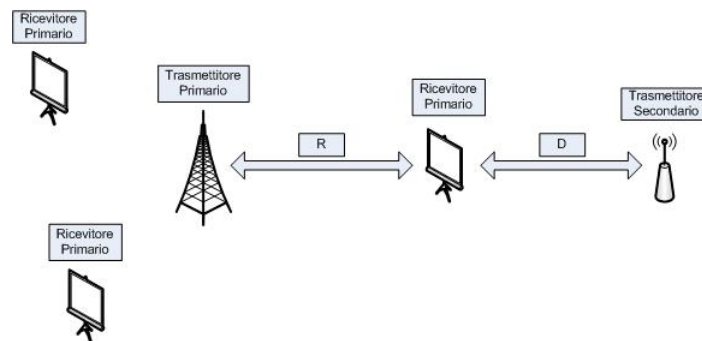
- $n(t)$ rappresenta il rumore;
- $s(t)$ rappresenta il segnale trasmesso dal dispositivo primario;
- h rappresenta il guadagno in ampiezza del canale.

2.3.2 Distanze di interferenza

Teoricamente, per non disturbare l'operatore primario, un dispositivo secondario dovrebbe essere in grado di rilevare trasmettitori primari attivi in un raggio $R + D$ da lui, dove R è la distanza tra un trasmettitore primario e il suo ricevitore più lontano, e D è il *raggio di interferenza* del dispositivo secondario, ossia la massima distanza da un ricevitore primario per cui l'interferenza che esso genera è ancora considerata dannosa [7]. In Figura 2.3 è data una rappresentazione grafica di questi concetti.

Evidentemente un sistema di questo tipo è molto conservativo. Ciò è motivato dal fatto che la cosa più importante non è sfruttare al massimo la banda, ma evitare di interferire con le trasmissioni dell'operatore primario.

Figura 2.3: Rappresentazione di una rete per spectrum sensing.



2.3.3 Spectrum sensing distribuito

Se le informazioni sullo stato di una banda vengono condivise tra diversi utenti secondari interessati a trasmettere, allora la valutazione che ne risulta è più affidabile e sono necessari sensori meno precisi. In questo caso si parla di spectrum sensing distribuito. Ciò consente inoltre di evitare che diversi dispositivi secondari cerchino di trasmettere alla stessa frequenza, ostacolandosi a vicenda, e di diminuire il tempo da dedicare al sensing.

Il modello base di una rete per spectrum sensing distribuito prevede un aggregatore che raccolga le valutazioni dei singoli utenti e le combini per avere una più affidabile valutazione collettiva. In questo modo un singolo utente malizioso potrebbe però cercare di impedire all'intera rete di utilizzare una certa frequenza semplicemente inviando valutazioni false relative al suo stato, quindi è necessario studiare meccanismi per incentivare gli utenti a comportarsi in modo onesto [7].

In letteratura il problema è già stato affrontato in diversi modi. In alcuni casi si è cercato di pesare le singole valutazioni in base a quanto fossero vicine o lontane alla media delle valutazioni stesse, in modo da ridurre l'influenza dei valori isolati [21]. Una soluzione simile è ignorare una certa percentuale delle valutazioni, partendo da quelle più estreme [11]. In altri casi la pesatura è stata operata in base a dei valori di reputazione associati agli utenti, in modo da dare più valore alle valutazioni di utenti che in passato sono stati affidabili [3], o addirittura da escludere dall'aggregazione i dati inviati da nodi con troppo bassa reputazione [20].

Capitolo 3

Incentivi alla cooperazione nello spectrum sensing

In questo capitolo viene presentato il modello di rete per spectrum sensing considerato nel lavoro, e vi si applica il meccanismo a reputazione di Jurca-Faltings. Sono poi mostrate le modifiche allo stesso necessarie per poter gestire le specificità del contesto e gli effetti del rumore sulle misurazioni degli utenti. Infine un esempio riassume il comportamento del sistema.

3.1 Obiettivo del lavoro

L'obiettivo del lavoro presentato è ottenere un sistema da poter utilizzare nel contesto dello spectrum sensing distribuito. E' stato quindi necessario partire da un modello di rete per spectrum sensing generalmente accettato in letteratura: in questo caso l'approccio seguito è simile a quello presentato in [7] [6]. Tale modello è stato esteso tramite il meccanismo a reputazione di Jurca-Faltings in modo da ottenere un sistema con alcune particolarità che lo differenziano dagli altri modelli visti in letteratura, e accennati nel Capitolo 2. I principali vantaggi sono tre:

- tramite variazioni di alcuni parametri è possibile portare il sistema negli equilibri di Nash desiderati;
- il sistema è robusto rispetto alle coalizioni;
- il sistema è in grado di sfruttare in modo efficiente informazioni certe, anche se costose, sullo stato di una determinata frequenza. Ciò è utile perchè al momento è ragionevole credere che verranno sviluppati sistemi in grado di fornirle [4].

3.2 Presentazione del modello

Il modello di rete per spectrum sensing considerato in questo lavoro è presentato in termini di elementi che lo compongono, di interazioni tra di essi e di obiettivi dei giocatori.

3.2.1 Elementi

Il modello è costituito dai seguenti componenti:

- n dispositivi di trasmissione senza licenza, per semplicità chiamati *nodi*;
- un aggregatore trusted (A);
- un database trusted (D).

3.2.2 Funzioni degli elementi

Queste le funzioni degli elementi:

- ogni nodo i può valutare autonomamente lo stato della banda o chiedere informazioni all'aggregatore o al database. A esso è associato un valore c_i che indica il numero di crediti a sua disposizione;
- l'aggregatore si occupa di aggregare le valutazioni dei nodi sullo stato della banda. A esso è associato un valore c_A che indica il numero di crediti a sua disposizione. Inoltre è a conoscenza del valore c_i di ogni nodo i ;
- il database fornisce un'informazione certa sullo stato della banda. Pagando una quota periodica una rete di nodi si garantisce un certo numero di crediti da spendere invocando i servizi del database.

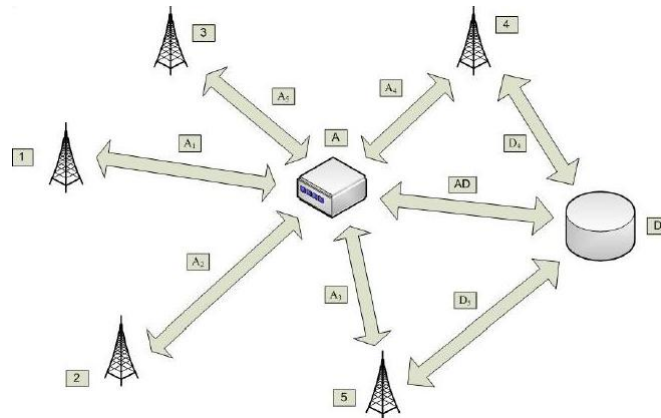
3.2.3 Interazioni

Nel modello sono considerate le seguenti interazioni tra i componenti:

- il nodo i può interagire con l'aggregatore (A_i) ed eventualmente, per alcune i , con il database (D_i);
- l'aggregatore può interagire con il nodo i (A_i) e con il database (AD);
- il database può interagire con alcuni nodi i (D_i) e con l'aggregatore (AD).

In Figura 3.1 è rappresentato il modello descritto.

Figura 3.1: Interazioni nella rete per spectrum sensing presa in considerazione.



3.2.4 Dinamiche delle interazioni

Queste le dinamiche delle interazioni:

- interazione nodo-aggregatore: un nodo i può chiedere all'aggregatore quale sia la più recente valutazione disponibile sullo stato di una certa banda. Per averla, deve pagare una quota q_A . Nella stessa interazione può anche fornire la propria valutazione, che verrà pagata con una quota p_A determinata da una opportuna regola, che dipende dalla sua correttezza;
- interazione nodo-database: un nodo i può chiedere al database se una certa banda sia o meno disponibile. Per farlo deve pagare una quota q_D ;
- interazione aggregatore-database: l'aggregatore può chiedere al database se una certa banda sia o meno disponibile. Per farlo deve pagare una quota q_D .

3.2.5 Obiettivi dei giocatori

Ogni nodo punta a massimizzare la propria capacità di trasmissione evitando di creare interferenze con le trasmissioni dei licenziatari. Per fare ciò cerca di avere informazioni il più possibile precise sullo stato della frequenza e di evitare che siano altri nodi senza licenza a usarla. Per avere le informazioni il nodo deve spendere crediti, e il suo unico modo per guadagnarli è fornire valutazioni sincere sullo stato della banda. D'altra parte fornire valutazioni

false potrebbe contribuire a scoraggiare altri nodi dal trasmettere, quindi bisogna prevedere che nodi egoisti possano mentire.

3.3 Applicazione del modello di Jurca-Faltings

Come si è visto nel capitolo precedente, quello di Jurca-Faltings è un meccanismo a reputazione compatibile con gli incentivi adatto a contesti in cui il segnale osservato è di tipo binario e dipende anche dal tempo, ossia può essere modellato come una *catena di Markov* [8]. Per lo spectrum sensing ciò è verificato, dato che una valutazione di un certo tipo porta spesso ad altre valutazioni del medesimo tipo.

Jurca-Faltings può anche essere adattato in modo da renderlo in grado di gestire l'impatto che la presenza di rumore può avere sulle rilevazioni. Inizialmente questa componente verrà però trascurata, e si supporrà che ogni nodo effettui rilevazioni sullo stato della banda sempre corrette.

3.3.1 Utilità attesa dei nodi

Come si è già visto, l'utilità attesa per i nodi facenti parte della rete è:

$$E[\sigma, \sigma', s_i] = \sum_{j=1}^2 \alpha_j^i \cdot \left(\sum_{k=1}^2 Pr[s_k | s_i] \cdot \left(\sum_{l=1}^2 \beta_l^k \cdot R(s_j, s_l) \right) \right)$$

dove:

- s_1, s_2 è l'insieme dei possibili segnali ('banda libera' o 'banda occupata');
- α_j^i indica la probabilità che il nodo riporti il segnale j se ha osservato il segnale i (è quindi il parametro che definisce la strategia σ);
- $Pr[s_k | s_i]$ è la probabilità che il rater osservi il segnale s_k se il nodo ha osservato il segnale s_i (è quindi il parametro che quantifica la correlazione tra gli stati della banda in istanti di tempo successivi);
- β_l^k è la probabilità che il rater riporti il segnale l se ha osservato il segnale k (è quindi il parametro che definisce la strategia σ');
- $R(s_j, s_l)$ è la regola di pagamento.

3.3.2 Regola di pagamento

In Jurca-Faltings una valutazione viene pagata una quota p_A se la valutazione fornita dal rater ha il suo medesimo valore, altrimenti viene pagata 0. La regola di pagamento è quindi:

$$R(s_j, s_l) = \begin{cases} p_A & \text{se } s_j = s_l \\ 0 & \text{altrimenti} \end{cases}$$

3.3.3 Equilibri

Come si è già detto in Jurca-Faltings riportare in modo sincero la propria valutazione è un equilibrio di Nash, ma non è quello a payoff massimo. Fornire sempre valutazioni positive o sempre valutazioni negative sono infatti anch'essi equilibri di Nash, e almeno uno di questi due equilibri garantisce un payoff maggiore di quello che si ha con le valutazioni sincere [8]. Ciò significa che il modello non è robusto rispetto alle coalizioni.

3.4 Aggiunta del rumore

Ora verrà presa in considerazione la possibilità che la presenza di rumore possa perturbare le rilevazioni effettuate dai nodi. Ogni nodo avrà quindi una certa probabilità di errore nel rilevare l'effettivo stato della banda. Questo fenomeno può essere espresso a partire dal valore $Pr[s_k|s_i]$ incontrato nella formula dell'utilità attesa dei nodi in assenza di rumore.

Prima di procedere è opportuno operare un cambio di nomenclatura. Dato che si ha a che fare con solo due tipi di segnali ('banda libera' e 'banda occupata'), si può porre che:

$$s_i \in \{+, -\}$$

dove + indica 'banda libera' e - indica 'banda occupata'.

3.4.1 Probabilità di falso allarme e probabilità di miss

Come si è detto, la rilevazione può essere errata. Ciò viene catturato da due diverse probabilità di errore:

- P_f (*probabilità di falso allarme*) è la probabilità di considerare occupata una banda libera;
- P_m (*probabilità di miss*) è la probabilità di considerare libera una banda occupata.

24 Capitolo 3. Incentivi alla cooperazione nello spectrum sensing

Tra questi due valori si ha un trade-off. Dato che è la probabilità di miss a portare all'errore più grave, normalmente si fissa a priori un valore accettabile per Pm e, a partire da esso, si cerca di minimizzare Pf . Per il momento si supporrà che ogni nodo del sistema abbia gli stessi valori di Pf e Pm .

3.4.2 Utilità attesa in presenza di rumore

A causa della possibilità di errore sarà necessario passare dalla correlazione tra gli effettivi stati della banda in istanti successivi, indicata in precedenza con $Pr[s_k|s_i]$, a quella tra gli stati rilevati dai nodi, che si indicherà invece con $Pr'[s_k|s_i]$. Ovviamente, a causa della maggiore casualità portata dal rumore, la correlazione vista dai nodi sarà minore della correlazione effettiva. Le relazioni tra i valori di partenza e quelli appena introdotti si possono esprimere nella forma seguente.

$$Pr[s_k|s_i] = \begin{cases} Pr[+|+](1 - Pf)^2 + Pr[-|-]Pm^2 + (Pr[-|+] + Pr[+|-])(1 - Pf)Pm & \text{se } s_i = +, s_k = + \\ Pr[+|+](1 - Pf)Pf + Pr[-|-]Pm(1 - Pm) + Pr[-|+](1 - Pf)(1 - Pm) + \\ Pr[+|-]PmPf & \text{se } s_i = +, s_k = - \\ Pr[+|+]Pf(1 - Pf) + Pr[-|-](1 - Pm)Pm + Pr[-|+]PfPm + \\ Pr[+|-](1 - Pm)(1 - Pf) & \text{se } s_i = -, s_k = + \\ Pr[+|+]Pf^2 + Pr[-|-](1 - Pm)^2 + (Pr[-|+] + Pr[+|-])Pf(1 - Pm) & \text{se } s_i = -, s_k = - \end{cases}$$

La formula per l'utilità attesa diventa quindi:

$$E[\sigma, \sigma', s_i] = \sum_{j=+,-} \alpha_j^i \cdot \left(\sum_{k=+,-} Pr'[s_k|s_i] \cdot \left(\sum_{l=+,-} \beta_l^k \cdot R(s_j, s_l) \right) \right)$$

Dato che Pf e Pm sono uguali per ogni nodo, e che non devono esistere nella rete nodi con probabilità di errore maggiore di questi valori (come si vedrà in seguito, non sarebbero infatti incentivati a essere sinceri), esse rappresentano il livello minimo di accuratezza richiesto ai nodi per entrare a fare parte del sistema. Questo aspetto verrà discusso in modo più approfondito nel Capitolo 5.

3.5 Aggiunta dei trusted report

Perchè l'equilibrio di Nash associato alle valutazioni sincere emerga come equilibrio a payoff massimo, e quindi per scoraggiare le coalizioni, è necessario inserire dei trusted report. Nel contesto dello spectrum sensing essi

potrebbero essere forniti da un database che la *FCC* (*Federal Communications Commission*) sta pensando di realizzare per raccogliere informazioni riguardo all'utilizzo delle frequenze sotto licenza [4]. Tuttavia l'allestimento e il mantenimento di un simile servizio avrà dei costi non irrisori, quindi è ragionevole credere che la sua consultazione non sarà gratuita. Ecco perchè è necessario minimizzare gli accessi al database.

3.5.1 Minimizzazione delle invocazioni del database

Per minimizzare le invocazioni del database è possibile calcolare un valore k^* che indichi la probabilità che ha ogni valutazione di un nodo di essere confrontata con una valutazione del database. k^* deve essere il valore minimo sufficiente a garantire che la strategia σ^* di riportare valutazioni sincere sia l'equilibrio di Nash a payoff massimo:

$$k^* = \min(k) \text{ t.c. } f(k^*) = 0, f(k) = \max_{\sigma, s_i} E_k[\sigma^*, \sigma^*, s_i] \text{ t.c. } \sigma \text{ è un equilibrio di Nash}$$

Come già si è detto questo valore k^* serve per portare il sistema da una qualsiasi situazione iniziale all'equilibrio di Nash della valutazione sincera. Una volta che vi si è giunti si può smettere di usare le valutazioni trusted, e quindi non serve più nemmeno invocare il database. L'unica fase in cui si devono comprare delle valutazioni affidabili è quindi quella di transizione verso l'equilibrio della sincerità, che si ha all'avvio del sistema e ogni qual volta l'equilibrio sincero venga abbandonato. Perchè succeda ciò è necessario che almeno una percentuale pari a $1 - k^*$ dei nodi si accordino per seguire la strategia legata a un altro equilibrio [8].

3.5.2 Calcolo di k^*

Il calcolo di k^* può essere effettuato tramite la seguente formula:

$$k^* = \max \left(\frac{1 - Pr'[-|-]}{Pr'[-|-]}, \frac{1 - Pr'[+|+]}{Pr'[+|+]} \right)$$

Come si è visto in precedenza, + indica che la banda in esame è libera, - che è occupata. Inoltre viene qui riportata anche la formula per determinare una k_σ che consenta di passare da un certo equilibrio σ all'equilibrio di Nash delle valutazioni sincere [8].

$$k_\sigma = \max_{s_i} \frac{E[\sigma, \sigma, s_i] - E[\sigma^*, \sigma^*, s_i]}{E[\sigma, \sigma, s_i] - E[\sigma, \sigma^*, s_i]}$$

3.6 Funzione di aggregazione

L'aggregatore deve decidere, in base ai valori delle ultime n rilevazioni che ha ricevuto in merito allo stato di una certa banda, se tale banda vada considerata libera o meno. Si può usare una regola del tipo m -su- n , ossia considerare la banda libera (o occupata) se almeno m delle n rilevazioni suggeriscono ciò.

La funzione di aggregazione può anche coincidere con la funzione di pagamento: in questo modo, se una valutazione viene pagata, allora il valore di quella valutazione viene preso come stato attuale della banda, altrimenti viene preso il valore opposto. Per aumentare l'affidabilità del sistema sarà bene considerare quindi non un singolo rater ma n , dei quali, perchè avvenga il pagamento, almeno m devono essere concordi con la valutazione stessa. In questo lavoro si è scelto tale approccio.

3.6.1 Probabilità di errore globale del sistema

Le relazioni tra le probabilità di errore dei singoli nodi e le probabilità di errore globali del sistema dovute al rumore si possono esprimere in questo modo:

$$Qf_L = \sum_{i=0}^{m-1} \binom{n}{i} (1 - Pf)^i Pf^{n-i}$$

$$Qm_L = \sum_{i=m}^n \binom{n}{i} Pm^i (1 - Pm)^{n-i}$$

$$Qf_O = \sum_{i=m}^n \binom{n}{i} Pf^i (1 - Pf)^{n-i}$$

$$Qm_O = \sum_{i=0}^{m-1} \binom{n}{i} (1 - Pm)^i Pm^{n-i}$$

dove Qf_L e Qf_O rappresentano le probabilità di falso allarme globale del sistema nel caso arrivino rilevazioni rispettivamente di tipo 'banda libera' e 'banda occupata' mentre Qm_L e Qm_O rappresentano le probabilità di miss globale del sistema nel caso arrivino rilevazioni sempre di tipo 'banda libera' e 'banda occupata'.

3.6.2 Scelta dei valori m e n

Per determinare n bisogna considerare diversi aspetti, molti dei quali dipenderanno dalle specifiche della rete come il numero dei nodi, la frequenza con

cui vengono fornite valutazioni, la reattività che deve avere il sistema in caso di variazione dello stato della banda etc.

A seconda del valore di n scelto si possono modificare equilibri e prestazioni del sistema variando il valore di m . Queste tematiche verranno analizzate in modo più approfondito nel Capitolo 4 e nel Capitolo 6.

3.7 Esempio di funzionamento

Si supponga di avere una rete composta da 10 nodi, un aggregatore A e un database D . All'istante iniziale ogni nodo i dispone di $c_i = 5$ crediti, mentre l'aggregatore dispone di $c_A = 10$ crediti. Siano:

- $q_A = 1$ la quota che un nodo deve pagare all'aggregatore per accedere al servizio;
- $q_D = 2$ la quota che un nodo deve pagare al database per accedere al servizio;
- $p_A = 1.5$ la quota che un nodo riceve in cambio di una valutazione coincidente con quella del rater.

Inoltre sia $\alpha_+^+ = 1$ la probabilità con cui un nodo riporta una valutazione del tipo 'banda libera' se la sua misurazione lo induce a credere che la banda sia libera, e lo stesso valga per α_-^- (si tratta quindi di nodi tutti onesti). Siano poi questi i valori della correlazione tra gli stati della banda in istanti di tempo successivi:

$$Pr[+|+] = 0.95$$

$$Pr[+|-] = 0.1$$

$$Pr[-|+] = 0.05$$

$$Pr[-|-] = 0.9$$

Infine, si consideri una funzione di aggregazione del tipo 2-su-5.

3.7.1 Assenza di rumore

Per iniziare si consideri la situazione in assenza di rumore. Date queste premesse, il pagamento atteso per un nodo che vede la banda libera e comunica la sua valutazione è:

$$E[\sigma, \sigma, +] = \sum_{j=+,-} \alpha_j^i \cdot \left(\sum_{h=+,-} Pr[s_h|+] \cdot \left(\sum_{l=+,-} \beta_l^h \cdot R(s_j, s_l) \right) \right) = 1 \cdot 0.95 \cdot 1 \cdot 1.5 = 1.425$$

28 Capitolo 3. Incentivi alla cooperazione nello spectrum sensing

Se invece vede la banda occupata il pagamento atteso è:

$$E[\sigma, \sigma, -] = \sum_{j=+,-} \alpha_j^i \cdot \left(\sum_{h=+,-} Pr[s_h|-] \cdot \left(\sum_{l=+,-} \beta_l^h \cdot R(s_j, s_l) \right) \right) = 1 \cdot 0.9 \cdot 1 \cdot 1.5 = 1.35$$

Ciò costituisce un equilibrio di Nash, ma è facile notare che se ogni nodo comunicasse sempre una valutazione positiva (o negativa) il pagamento atteso sarebbe $1.5 > 1.425$, $1.5 > 1.35$. Perciò è necessario prevedere che con probabilità k^* la valutazione del rater debba essere di tipo trusted. k^* è data da:

$$k^* = \max \left(\frac{1 - Pr'[-|-]}{Pr'[-|-]}, \frac{1 - Pr'[+|+]}{Pr'[+|+]} \right) = \max \left(\frac{1 - 0.9}{0.9}, \frac{1 - 0.95}{0.95} \right) = 0.111$$

3.7.2 Presenza di rumore

La presenza di rumore porta a dover considerare con quale probabilità i nodi possano sbagliare le loro rilevazioni. Sia $Pf = 0.05$ e $Pm = 0.03$. Per prima cosa è necessario calcolare i valori di $Pr'[s_h|s_i]$.

$$Pr'[+|+] = Pr[+|+](1 - Pf)^2 + Pr[-|-]Pm^2 + (Pr[-|+]+Pr[+|-])(1 - Pf)Pm = 0.862$$

$$Pr'[+|-] = Pr[+|+](1 - Pf)Pf + Pr[-|-]Pm(1 - Pm) + Pr[-|+](1 - Pf)(1 - Pm) + Pr[+|-]PmPf = 0.118$$

$$Pr'[-|+] = Pr[+|+](1 - Pf)Pf + Pr[-|-](1 - Pm)Pm + Pr[-|+](1 - Pf)Pm + Pr[+|-](1 - Pm)(1 - Pf) = 0.164$$

$$Pr'[-|-] = Pr[+|+](1 - Pf)^2 + Pr[-|-](1 - Pm)^2 + (Pr[-|+]+Pr[+|-])Pf(1 - Pm) = 0.856$$

Il livello di correlazione a valle dell'effetto del rumore risulta quindi pari a:

$$\begin{aligned} Pr'[+|+] &= 0.862 \\ Pr'[+|-] &= 0.118 \\ Pr'[-|+] &= 0.164 \\ Pr'[-|-] &= 0.856 \end{aligned}$$

Come si può notare, esso è calato, e allo stesso modo cala l'utilità attesa per ogni nodo:

$$E[\sigma, \sigma, +] = \sum_{j=+,-} \alpha_j^i \cdot \left(\sum_{h=+,-} Pr[s_h|+] \cdot \left(\sum_{l=+,-} \beta_l^h \cdot R(s_j, s_l) \right) \right) = 1 \cdot 0.862 \cdot 1 \cdot 1.5 = 1.293$$

$$E[\sigma, \sigma, -] = \sum_{j=+,-} \alpha_j^i \cdot \left(\sum_{h=+,-} Pr[s_h|-] \cdot \left(\sum_{l=+,-} \beta_l^h \cdot R(s_j, s_l) \right) \right) = 1 \cdot 0.856 \cdot 1 \cdot 1.5 = 1.284$$

Di conseguenza sarà necessario un maggior numero di valutazioni trusted per assicurare che l'equilibrio di Nash associato alle valutazioni sincere sia l'equilibrio a payoff massimo, infatti:

$$k^* = \max \left(\frac{1-Pr_{tot}[-|-]}{Pr_{tot}[-|-]}, \frac{1-Pr_{tot}[+|+]}{Pr_{tot}[+|+]} \right) = \max \left(\frac{1-0.856}{0.856}, \frac{1-0.862}{0.862} \right) = 0.168$$

Per finire si calcola la probabilità di errore globale del sistema dovuta al rumore:

$$Qf_L = \sum_{i=0}^{m-1} \binom{n}{i} (1 - Pf)^i Pf^{n-i} = 0.0085$$

$$Qm_L = \sum_{i=m}^n \binom{n}{i} Pm^i (1 - Pm)^{n-i} = 3 \cdot 10^{-5}$$

$$Qf_O = \sum_{i=m}^n \binom{n}{i} Pf^i (1 - Pf)^{n-i} = 3.9528 \cdot 10^{-6}$$

$$Qm_O = \sum_{i=0}^{m-1} \binom{n}{i} (1 - Pm)^i Pm^{n-i} = 0.0226$$

Capitolo 4

Analisi del problema

In questo capitolo vengono studiati gli equilibri di Nash del sistema presentato nella sezione precedente. Dapprima si descrive la situazione in un contesto di *sensing perfetto*, quindi vengono ripresi i possibili errori di sensing dovuti al rumore e si passa all'analisi vera e propria degli equilibri. Vengono presentate, nell'ordine, le situazioni che si hanno in caso di singolo rater, n rater, singolo rater con trusted report e n rater con trusted report. Infine vengono tratte alcune conclusioni.

4.1 Sensing perfetto

Si parla di sensing perfetto nel caso in cui gli agenti che operano il sensing siano infallibili. Ciò significa che se essi percepiscono una data banda come libera, allora essa sicuramente lo è, e allo stesso modo la banda è sicuramente occupata se viene percepita come occupata. Questa situazione non è evidentemente realistica, in quanto interferenze e imprecisioni non sono completamente eliminabili. Del resto, un sensing perfetto renderebbe inutile un meccanismo distribuito di condivisione delle rilevazioni, che ha appunto lo scopo di rendere meno dannosi gli errori nel sensing.

Detto questo, le condizioni che devono essere verificate per imporre un equilibrio di Nash della sincerità in un contesto di sensing perfetto sono le seguenti:

$$E(L|L) > E(O|L)$$

$$E(O|O) > E(L|O)$$

Esse significano che se si percepisce che la banda è libera si deve avere un payoff atteso maggiore nel caso in cui si dichiara che la banda è appunto libera rispetto al caso in cui si dichiara che è occupata, mentre se la si percepisce

come occupata il payoff atteso maggiore deve corrispondere al caso in cui la si dichiara occupata. In questa e in tutte le altre sezioni del capitolo si suppone un comportamento sincero da parte dei rater.

4.2 Introduzione degli errori nel sensing

Il punto di partenza per analizzare casi in cui il sensing non è perfetto è introdurre due probabilità a priori che rappresentano caratteristiche intrinseche della banda su cui si sta operando il sensing: la probabilità che in un dato istante la banda sia libera, indicata con PL , e quella che sia occupata, indicata con PO .

A partire da esse si introducono due coppie di probabilità condizionate, che rappresentano l'accuratezza del sensing. La prima coppia è costituita dalla probabilità che la banda sia effettivamente libera se la si vede libera:

$$P(L|L) = \frac{(1 - Pf)PL}{(1 - Pf)PL + PmPO}$$

e da quella che la banda sia occupata se la si vede libera:

$$P(O|L) = \frac{PmPO}{(1 - Pf)PL + PmPO}$$

La seconda coppia è simmetrica alla prima, perciò è costituita dalla probabilità che la banda sia effettivamente occupata se la si vede occupata:

$$P(O|O) = \frac{(1 - Pm)PO}{(1 - Pm)PO + PfPL}$$

e da quella che la banda sia libera se la si vede occupata:

$$P(L|O) = \frac{PfPL}{(1 - Pm)PO + PfPL}$$

Nelle precedenti espressioni, Pm rappresenta la probabilità di miss, ossia la probabilità di rilevare come libera una banda occupata, mentre Pf è la probabilità di falso allarme, ossia quella di rilevare come occupata una banda libera.

4.3 Singolo rater, assenza di trusted report

In questo primo caso verrà considerato un singolo rater, e non saranno presi in considerazione i trusted report. Il primo passo è la costruzione di una tabella, riportata in Tabella 4.1, che riassume le probabilità che hanno le

Tabella 4.1: Tabella dei payoff attesi nel caso a singolo rater in assenza di trusted report.

Val. del Nodo	Stato della Banda	Val. del Rater	Probabilità	Payoff
L	L	L	$1 - Pf$	1
L	L	O	Pf	0
L	O	L	Pm	1
L	O	O	$1 - Pm$	0
O	L	L	$1 - Pf$	0
O	L	O	Pf	1
O	O	L	Pm	0
O	O	O	$1 - Pm$	1

diverse configurazioni possibili di presentarsi, assieme al payoff associato a ognuna di esse.

Ora è possibile calcolare il payoff atteso associato a un comportamento sincero da parte di un dato nodo, che nel caso di rilevazione di banda libera risulta pari a:

$$E(L|L) = P(L|L)(1 - Pf) + P(O|L)Pm$$

mentre nel caso di banda occupata si ha:

$$E(O|O) = P(O|O)(1 - Pm) + P(L|O)Pf$$

Per quanto riguarda invece il comportamento non sincero, nel caso di rilevazione di banda libera si ha:

$$E(O|L) = P(L|L)Pf + P(O|L)(1 - Pm)$$

mentre nel caso di banda occupata si ha:

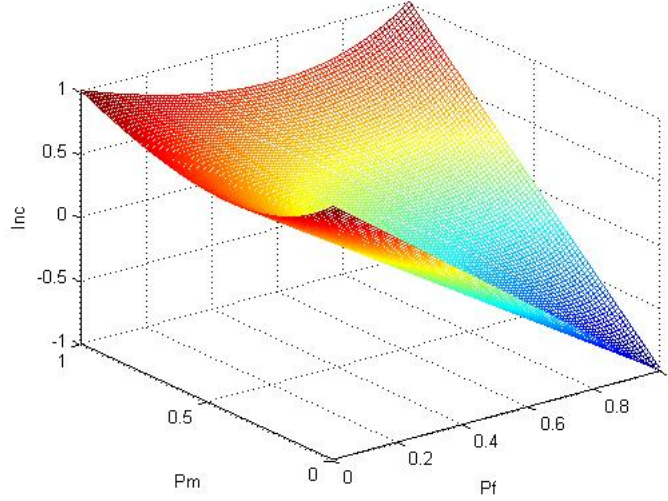
$$E(L|O) = P(O|O)Pm + P(L|O)(1 - Pf)$$

Per forzare un comportamento sincero esso deve essere conveniente in entrambe le situazioni, perciò devono essere verificate le due disequazioni:

$$P(L|L)(1 - Pf) + P(O|L)Pm > P(L|L)Pf + P(O|L)(1 - Pm)$$

$$P(O|O)(1 - Pm) + P(L|O)Pf > P(O|O)Pm + P(L|O)(1 - Pf)$$

Figura 4.1: Incentivo al comportamento sincero per banda libera con $PL = PO = 0.5$.



Introducendo dove possibile le probabilità condizionate presentate in precedenza si ottiene:

$$\frac{(1-Pf)PL}{(1-Pf)PL+PmPO}(1-Pf) + \frac{PmPO}{(1-Pf)PL+PmPO}Pm >$$

$$\frac{(1-Pf)PL}{(1-Pf)PL+PmPO}Pf + \frac{PmPO}{(1-Pf)PL+PmPO}(1-Pm)$$

$$\frac{(1-Pm)PO}{(1-Pm)PO+PfPL}(1-Pm) + \frac{PfPL}{(1-Pm)PO+PfPL}Pf >$$

$$\frac{(1-Pm)PO}{(1-Pm)PO+PfPL}Pm + \frac{PfPL}{(1-Pm)PO+PfPL}(1-Pf)$$

Risolvendo si giunge a:

$$\frac{PL(2Pf^2 - 3Pf + 1) + PO(2Pm^2 - Pm)}{(1-Pf)PL + PmPO} > 0$$

$$\frac{PL(2Pf^2 - Pf) + PO(2Pm^2 - 3Pm + 1)}{(1-Pm)PO + PfPL} > 0$$

Supponendo $PL = PO = 0.5$, facendo variare Pf e Pm da 0 a 1 si ottengono i grafici in Figura 4.1 e 4.2. A destra viene rappresentata Pf , a sinistra Pm e in verticale la differenza tra il payoff atteso del comportamento sincero e quello del comportamento non sincero, ossia l'incentivo alla sincerità. Come si può notare si tratta in entrambi i casi di un paraboloide il cui minimo, per qualsiasi PL e PO , ha coordinate rispettivamente $(1, 0, -1)$ e $(0, 1, -1)$. I punti di massimo sono invece 3 e corrispondono alle situazioni

Figura 4.2: Incentivo al comportamento sincero per banda occupata con $PL = PO = 0.5$.

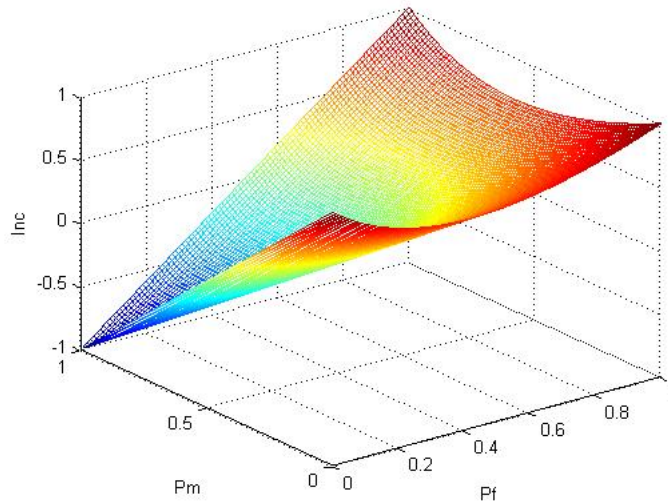


Figura 4.3: Incentivo al comportamento sincero per banda libera con $PL = 0.9$ e $PO = 0.1$.

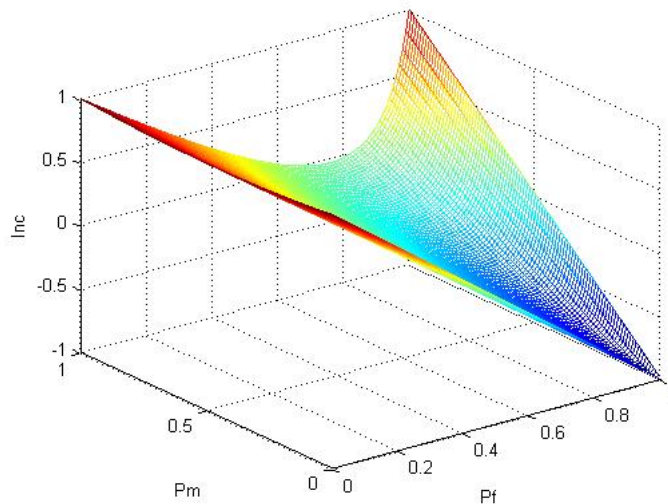


Figura 4.4: Incentivo al comportamento sincero per banda occupata con $PL = 0.9$ e $PO = 0.1$.

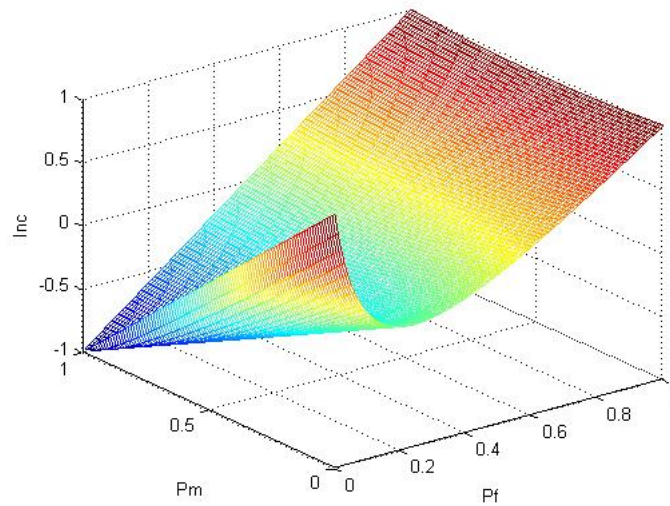


Figura 4.5: Incentivo al comportamento sincero per banda libera con $PL = 0.1$ e $PO = 0.9$.

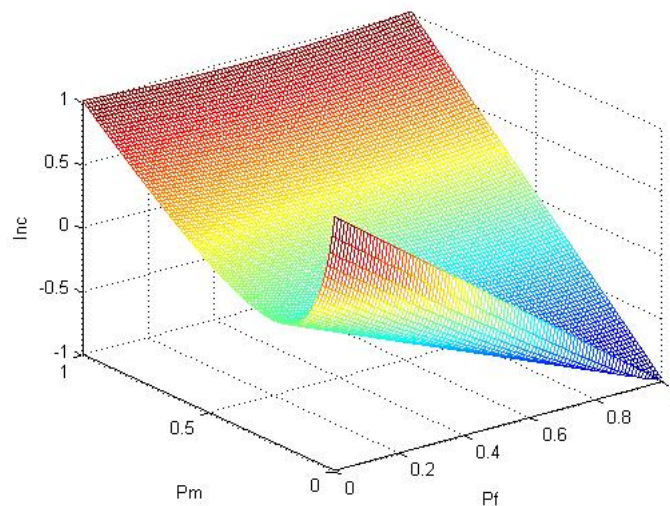
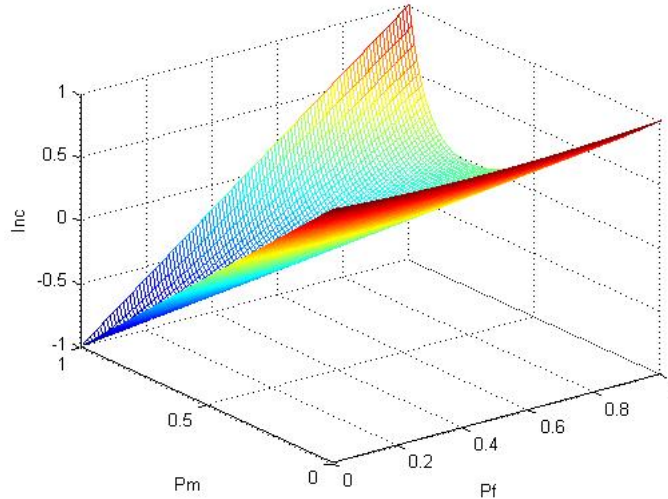


Figura 4.6: Incentivo al comportamento sincero per banda occupata con $PL = 0.1$ e $PO = 0.9$.



in cui si è certi che il rater confermerà la valutazione del nodo. Ciò avviene se non c'è possibilità di sbagliare o se c'è la certezza di sbagliare (e quindi la valutazione errata del rater confermerà quella errata del nodo).

Al variare di PL e PO i grafici cambiano sensibilmente. Per $PL = 0.9$ e $PO = 0.1$ si ottengono i grafici in Figura 4.3 e 4.4, mentre per $PL = 0.1$ e $PO = 0.9$ i grafici sono quelli in Figura 4.5 e 4.6. Come si può notare, al crescere di PL cresce nei grafici il peso di Pf e cala quello di Pm , mentre al crescere di PO succede il contrario. Perché sia incentivato un comportamento sincero è quindi necessario avere, per valori di PL alti, valori di Pf lontani da 0 (per Pm alti) e 1 (per Pm bassi), mentre per valori di PL bassi servono valori di Pm lontani da 0 (per Pf alti) e 1 (per Pf bassi).

4.4 n rater, assenza di trusted report

Una strategia per diminuire l'incidenza di Pf e Pm sugli equilibri del sistema potrebbe essere quella di aumentare il numero dei rater. Nella sua forma più generale possibile questa soluzione potrebbe prevedere di pagare un report solo se almeno m degli n rater considerati sono concordi con esso.

Come nel caso precedente si considera la tabella dei payoff attesi, riportata in Tabella 4.2.

Tabella 4.2: Tabella dei payoff attesi nel caso a n rater in assenza di trusted report.

Val. Nodo	St. Banda	Val. Rater	Probabilità	Payoff
L	L	$L \geq m$	$\sum_{i=m}^n \binom{n}{i} (1-Pf)^i Pf^{n-i}$	1
L	L	$L < m$	$\sum_{i=0}^{m-1} \binom{n}{i} (1-Pf)^i Pf^{n-i}$	0
L	O	$L \geq m$	$\sum_{i=m}^n \binom{n}{i} Pm^i (1-Pm)^{n-i}$	1
L	O	$L < m$	$\sum_{i=0}^{m-1} \binom{n}{i} Pm^i (1-Pm)^{n-i}$	0
O	L	$O < m$	$\sum_{i=0}^{m-1} \binom{n}{i} Pf^i (1-Pf)^{n-i}$	0
O	L	$O \geq m$	$\sum_{i=m}^n \binom{n}{i} Pf^i (1-Pf)^{n-i}$	1
O	O	$O < m$	$\sum_{i=0}^{m-1} \binom{n}{i} (1-Pm)^i Pm^{n-i}$	0
O	O	$O \geq m$	$\sum_{i=m}^n \binom{n}{i} (1-Pm)^i Pm^{n-i}$	1

I payoff attesi relativi al comportamento sincero sono:

$$E(L|L) = P(L|L) \sum_{i=m}^n \binom{n}{i} (1-Pf)^i Pf^{n-i} + P(O|L) \sum_{i=m}^n \binom{n}{i} Pm^i (1-Pm)^{n-i}$$

$$E(O|O) = P(O|O) \sum_{i=m}^n \binom{n}{i} (1-Pm)^i Pm^{n-i} + P(L|O) \sum_{i=m}^n \binom{n}{i} Pf^i (1-Pf)^{n-i}$$

Quelli relativi al comportamento non sincero sono invece:

$$E(O|L) = P(L|L) \sum_{i=m}^n \binom{n}{i} Pf^i (1-Pf)^{n-i} + P(O|L) \sum_{i=m}^n \binom{n}{i} (1-Pm)^i Pm^{n-i}$$

$$E(L|O) = P(O|O) \sum_{i=m}^n \binom{n}{i} Pm^i (1-Pm)^{n-i} + P(L|O) \sum_{i=m}^n \binom{n}{i} (1-Pf)^i Pf^{n-i}$$

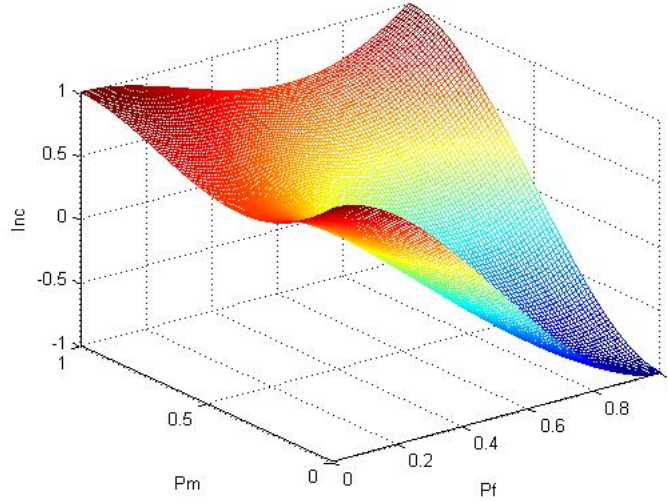
Come nel caso precedente sia che venga rilevata una banda libera sia che venga rilevata una banda occupata deve essere incentivato un comportamento sincero, perciò bisogna impostare le due disequazioni:

$$P(L|L) \sum_{i=m}^n \binom{n}{i} (1-Pf)^i Pf^{n-i} + P(O|L) \sum_{i=m}^n \binom{n}{i} Pm^i (1-Pm)^{n-i} > P(L|L) \sum_{i=m}^n \binom{n}{i} Pf^i (1-Pf)^{n-i} + P(O|L) \sum_{i=m}^n \binom{n}{i} (1-Pm)^i Pm^{n-i}$$

$$P(O|O) \sum_{i=m}^n \binom{n}{i} (1-Pm)^i Pm^{n-i} + P(L|O) \sum_{i=m}^n \binom{n}{i} Pf^i (1-Pf)^{n-i} > P(O|O) \sum_{i=m}^n \binom{n}{i} Pm^i (1-Pm)^{n-i} + P(L|O) \sum_{i=m}^n \binom{n}{i} (1-Pf)^i Pf^{n-i}$$

Si ottiene quindi:

$$\frac{PL \sum_{i=m}^n \binom{n}{i} ((1-Pf)^{i+1} Pf^{n-i} - Pf^i (1-Pf)^{n-i+1})}{(1-Pf)PL + PmPO} + \frac{PO \sum_{i=m}^n \binom{n}{i} (Pm^{i+1} (1-Pm)^{n-i} - (1-Pm)^i Pm^{n-i+1})}{(1-Pf)PL + PmPO} > 0$$

Figura 4.7: Incentivo al comportamento sincero per banda libera con $n = 3$ e $m = 2$.

$$\frac{PO \sum_{i=m}^n \binom{n}{i} ((1-Pm)^{i+1} Pm^{n-i} - Pm^i (1-Pm)^{n-i+1})}{(1-Pm)PO + PfPL} + \frac{PL \sum_{i=m}^n \binom{n}{i} (Pf^{i+1} (1-Pf)^{n-i} - (1-Pf)^i Pf^{n-i+1})}{(1-Pm)PO + PfPL} > 0$$

Ora è possibile analizzare in che modo variazioni di m e n influiscono sugli equilibri del sistema. PL e PO si suppongono entrambe pari a 0.5: come si è visto nel caso precedente, al crescere di PL crescerà il peso di Pf nei grafici, mentre al crescere di PO crescerà quello di Pm .

In Figura 4.7 e 4.8 sono rappresentati i grafici per $n = 3$ e $m = 2$, ossia quando un report viene pagato se almeno 2 dei 3 rater sono concordi con esso. Rispetto al caso a singolo rater è cresciuta l'area dove gli incentivi per un certo comportamento sono alti.

Con condizioni molto più restrittive, ossia $n = 10$ e $m = 9$, i grafici sono quelli in Figura 4.9 e 4.10, mentre con condizioni molto generose, $n = 10$ e $m = 1$, si hanno i grafici in Figura 4.11 e 4.12. Come si può notare, in entrambi i casi si hanno vaste aree in cui gli incentivi per un certo comportamento sono vicini a zero: quindi se la precisione dei nodi è sufficientemente alta si dovranno preferire funzioni con un valore di m intorno alla metà di quello di n , perchè hanno il giusto grado di severità.

Figura 4.8: Incentivo al comportamento sincero per banda occupata con $n = 3$ e $m = 2$.

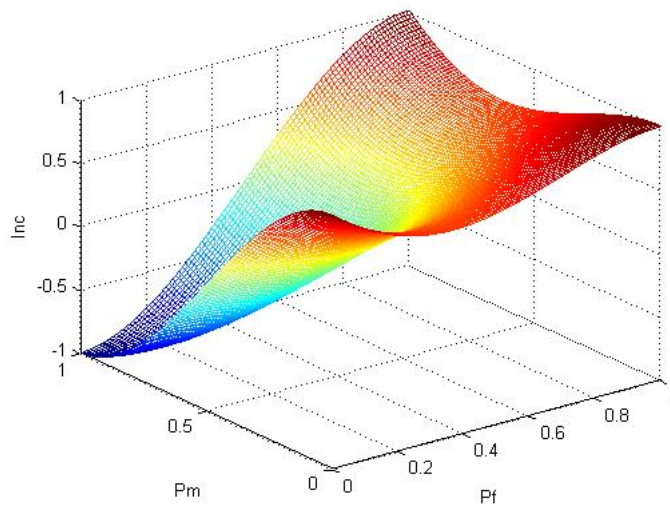


Figura 4.9: Incentivo al comportamento sincero per banda libera con $n = 10$ e $m = 9$.

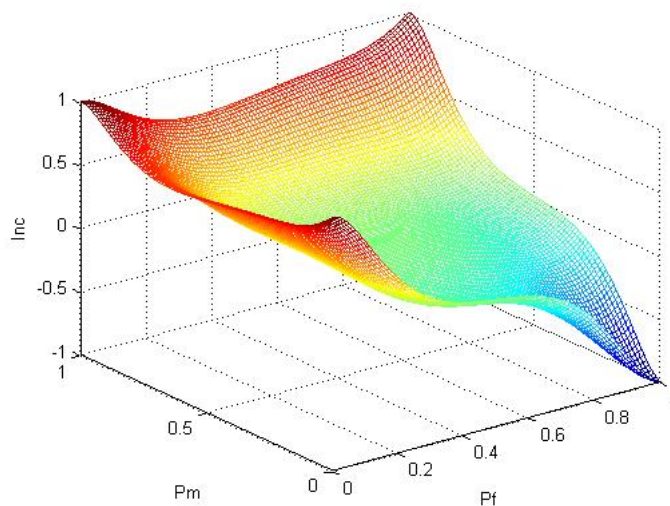


Figura 4.10: Incentivo al comportamento sincero per banda occupata con $n = 10$ e $m = 9$.

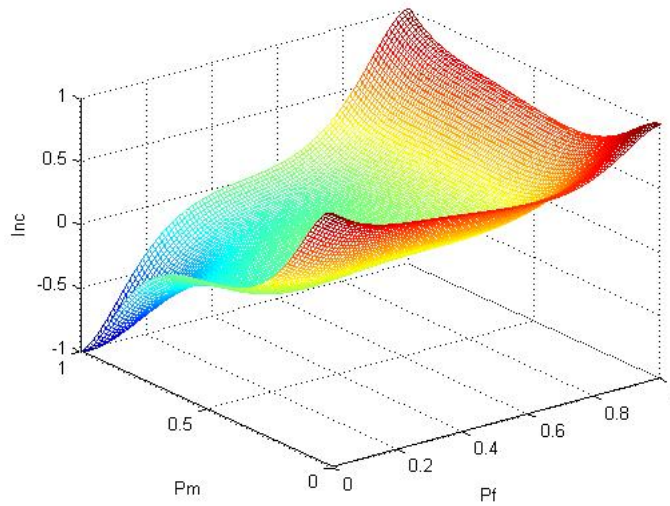


Figura 4.11: Incentivo al comportamento sincero per banda libera con $n = 10$ e $m = 1$.

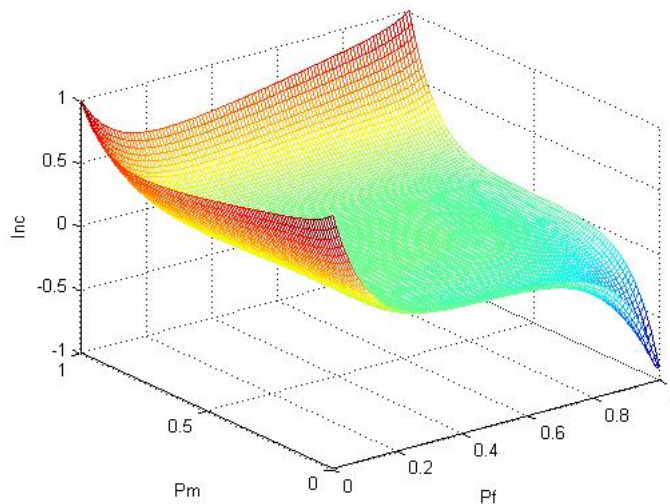
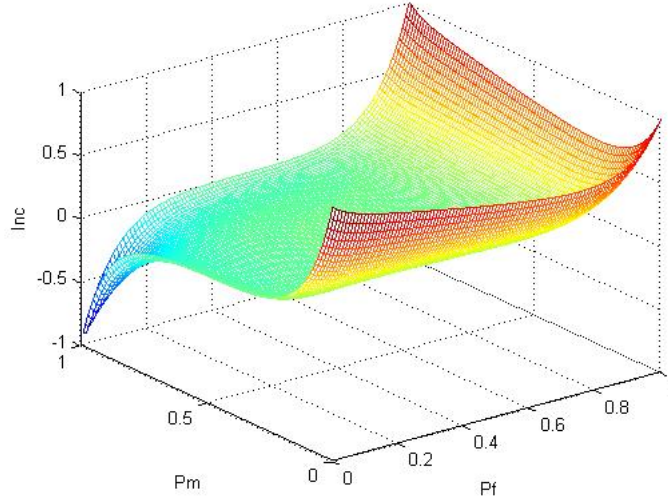


Figura 4.12: Incentivo al comportamento sincero per banda occupata con $n = 10$ e $m = 1$.



4.5 Singolo rater, presenza di trusted report

Si torna ora al caso a rater singolo, ma si introducono i trusted report. Sia quindi k la probabilità che la valutazione di un nodo venga confrontata con un rater di tipo trusted, la cui valutazione è sempre corretta.

La situazione dei payoff è analoga a quella in Tabella 4.1, tuttavia essa viene impiegata solo con probabilità $1-k$, in quanto con probabilità k si opera il confronto con il rater trusted. I payoff attesi relativi al comportamento sincero diventano quindi:

$$E(L|L) = kP(L|L) + (1-k)(P(L|L)(1-Pf) + P(O|L)Pm)$$

$$E(O|O) = kP(O|O) + (1-k)(P(O|O)(1-Pm) + P(L|O)Pf)$$

mentre quelli relativi al comportamento non sincero sono:

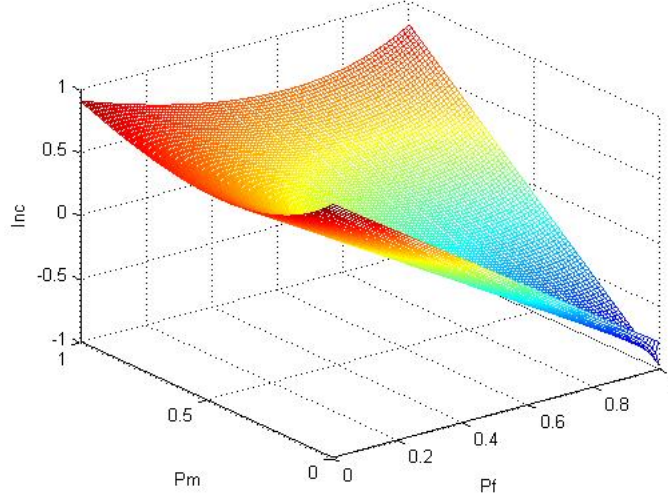
$$E(O|L) = kP(O|L) + (1-k)(P(L|L)Pf + P(O|L)(1-Pm))$$

$$E(L|O) = kP(L|O) + (1-k)(P(O|O)Pm + P(L|O)(1-Pf))$$

Come in precedenza, si incentiva il comportamento sincero imponendo:

$$kP(L|L) + (1-k)(P(L|L)(1-Pf) + P(O|L)Pm) > kP(O|L) + (1-k)(P(L|L)Pf + P(O|L)(1-Pm))$$

Figura 4.13: Incentivo al comportamento sincero per banda libera con $k = 0.1$ e $PL = PO = 0.5$.



$$kP(O|O) + (1 - k)(P(O|O)(1 - Pm) + P(L|O)Pf) > kP(L|O) + (1 - k)(P(O|O)Pm + P(L|O)(1 - Pf))$$

che diventano:

$$\frac{PL(2Pf^2(1 - k) + Pf(2k - 3) + 1) + PO(2Pm^2(1 - k) - Pm)}{(1 - Pf)PL + PmPO} > 0$$

$$\frac{PL(2Pf^2(1 - k) - Pf) + PO(2Pm^2(1 - k) + Pm(2k - 3) + 1)}{(1 - Pm)PO + PfPL} > 0$$

Supponendo $PL = PO = 0.5$, con $k = 0.1$ si hanno i grafici in Figura 4.13 e 4.14. Si può notare come dei 3 punti di massimo che erano presenti in assenza di trusted report si sia conservato solo quello associato alle valutazioni corrette: gli altri due, associati a situazioni in cui sbagliava sia il nodo che il suo rater, sono stati 'abbassati' di un valore proporzionale a k .

Per comprendere meglio l'effetto di k sugli equilibri si considerino i grafici in Figura 4.15 e 4.16, ottenuti con $k = 0.5$. Si può notare che al crescere di k cresce l'incentivo verso un comportamento sincero per Pf e Pm entrambe prossime a 0, mentre cala altrove.

Tuttavia, gli effetti di un k grande per valori estremi di PL e PO non sono sempre positivi. Infatti, sempre per $k = 0.5$ ma con $PL = 0.9$ e $PO = 0.1$, i grafici sono quelli riportati in Figura 4.17 e 4.18. L'effetto dei trusted

Figura 4.14: Incentivo al comportamento sincero per banda occupata con $k = 0.1$ e $PL = PO = 0.5$.

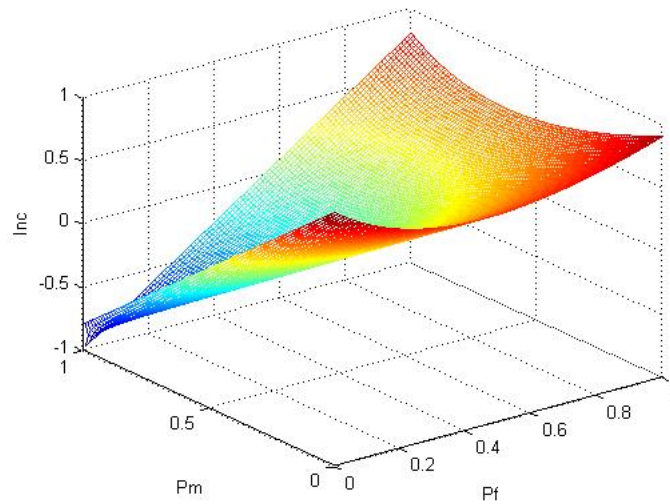


Figura 4.15: Incentivo al comportamento sincero per banda libera con $k = 0.5$ e $PL = PO = 0.5$.

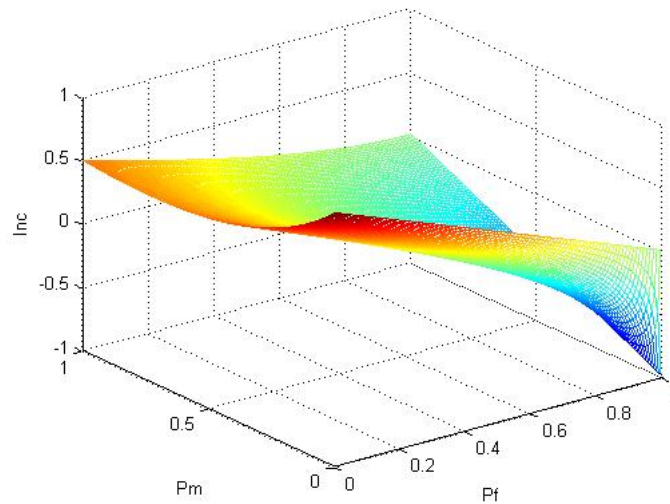


Figura 4.16: Incentivo al comportamento sincero per banda occupata con $k = 0.5$ e $PL = PO = 0.5$.

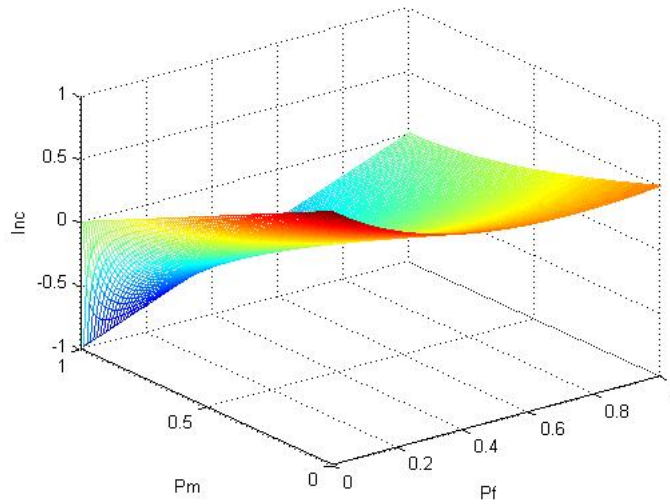


Figura 4.17: Incentivo al comportamento sincero per banda libera con $k = 0.5$ e $PL = 0.9$, $PO = 0.1$.

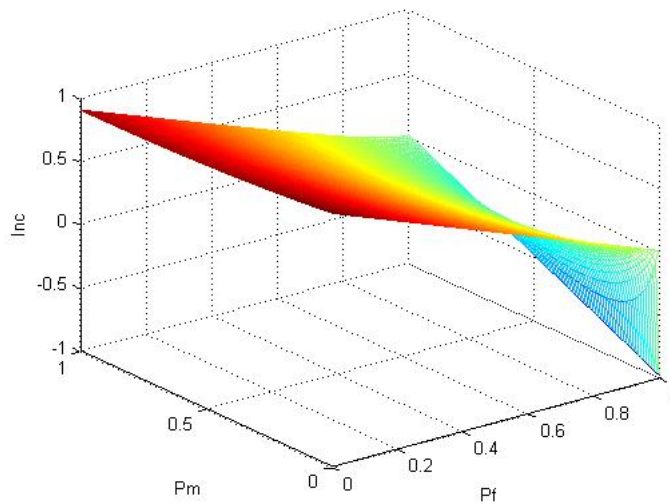


Figura 4.18: Incentivo al comportamento sincero per banda occupata con $k = 0.5$ e $PL = 0.9$, $PO = 0.1$.

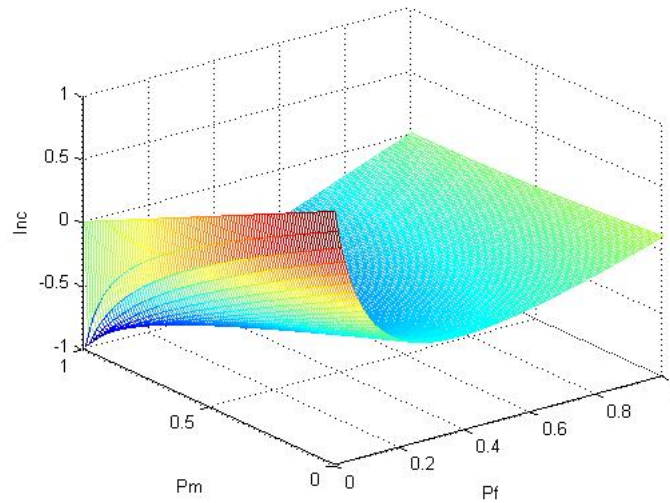


Figura 4.19: Incentivo al comportamento sincero per banda libera con $k = 0.5$ e $PL = 0.1$, $PO = 0.9$.

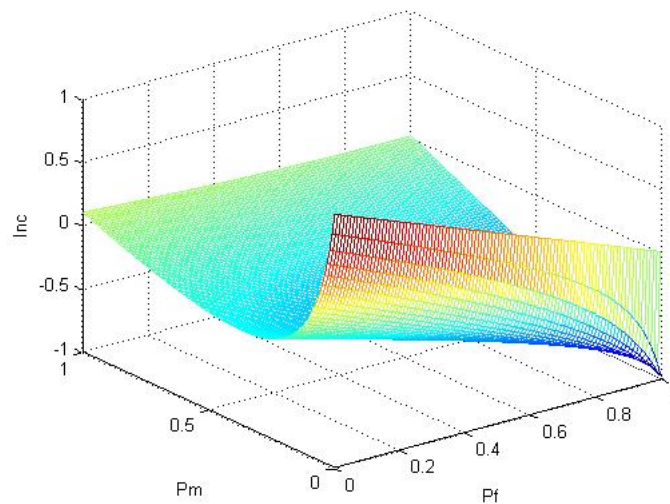
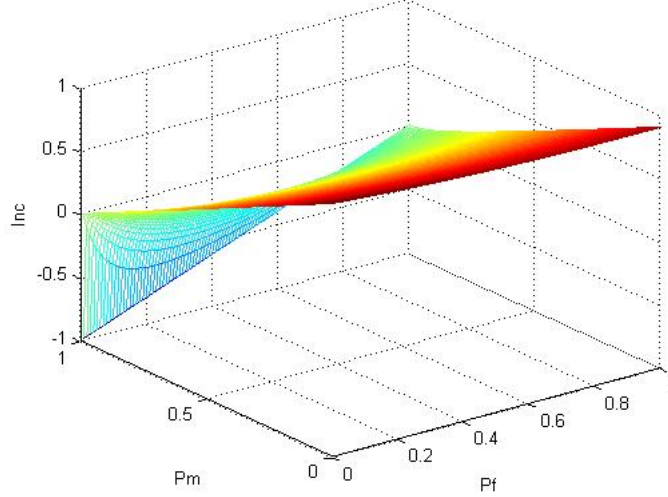


Figura 4.20: Incentivo al comportamento sincero per banda occupata con $k = 0.5$ e $PL = 0.1$, $PO = 0.9$.



report è quindi positivo quando la banda viene rilevata come libera, ma negativo quando viene rilevata come occupata (caso che dovrebbe tuttavia essere piuttosto raro con simili valori delle probabilità a priori). Se invece $PL = 0.1$ e $PO = 0.9$ succede il contrario: si può notare infatti dai grafici in Figura 4.19 e 4.20 che il comportamento sincero viene ora incentivato quando la banda sembra occupata.

Infine, è anche possibile trovare k^* , ossia il minimo valore di k per cui le due precedenti disequazioni sono verificate:

$$k^* = \frac{PL(-2Pf^2 + 3Pf - 1) + PO(-2Pm^2 + Pm)}{2PL(-Pf^2 + Pf) - 2POPm^2}$$

$$k^* = \frac{PL(-2Pf^2 + Pf) + PO(-2Pm^2 + 3Pm - 1)}{-2PLPf^2 + 2PO(-Pm^2 + Pm)}$$

k rappresenta una probabilità, perciò il suo valore deve essere compreso tra 0 e 1. Se dalle due precedenti equazioni risultano valori di k^* negativi significa che il comportamento sincero sarà sempre incentivato, mentre se risultano valori maggiori di 1 significa che non potrà mai esserlo.

Ora si cercherà di comprendere meglio l'andamento di k^* al variare di Pf e Pm . Per $PL = PO = 0.5$ osservando i grafici, riportati in Figura 4.21 e 4.22, delle curve di livello dei denominatori delle due espressioni, ci

Figura 4.21: Linee di livello del denominatore di k^* per banda libera.

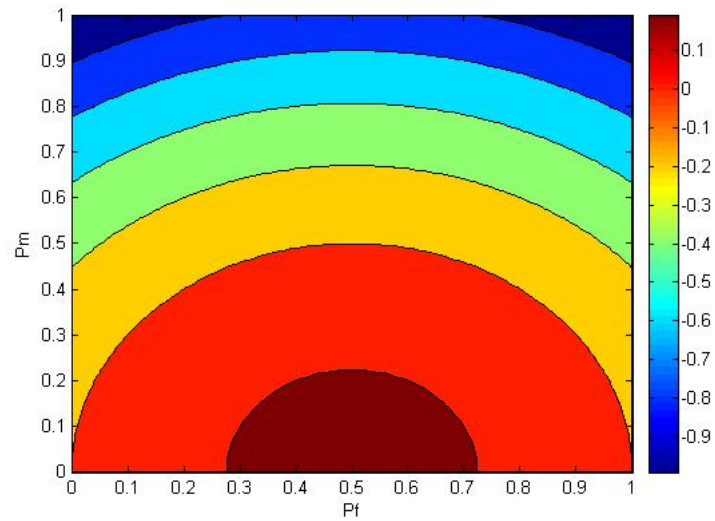


Figura 4.22: Linee di livello del denominatore di k^* per banda occupata.

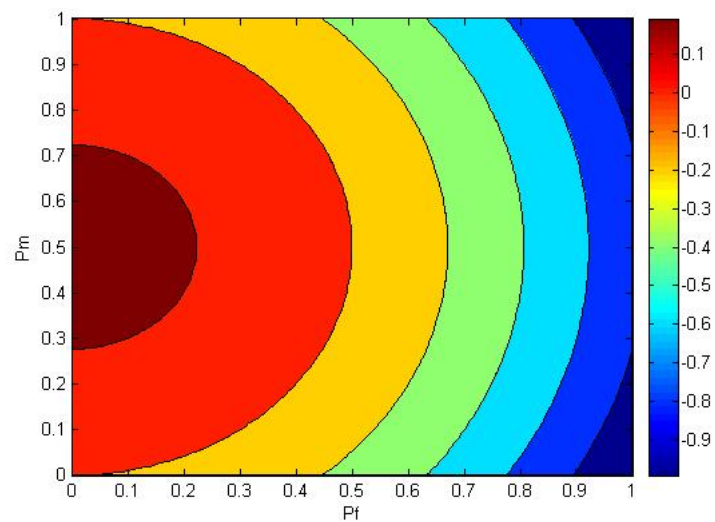


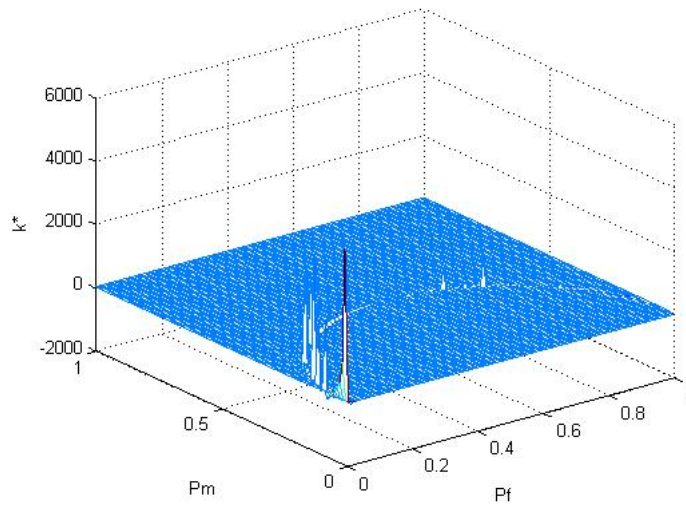
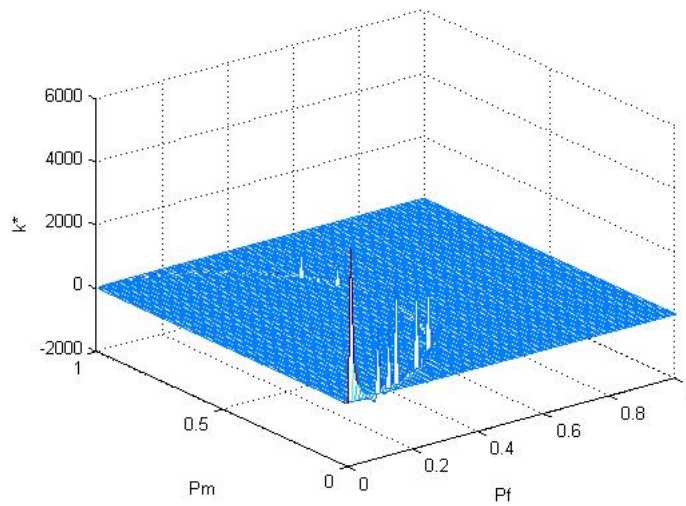
Figura 4.23: Andamento di k^ per banda libera.**Figura 4.24: Andamento di k^* per banda occupata.*

Figura 4.25: Andamento parziale di k^* per banda libera.

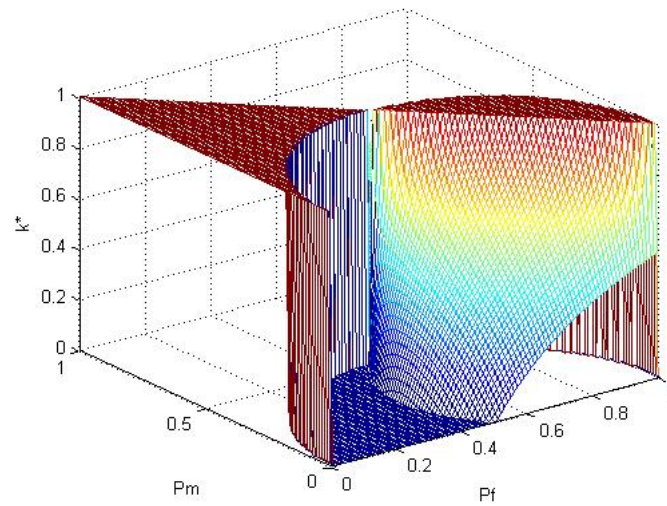


Figura 4.26: Andamento parziale di k^* per banda occupata.

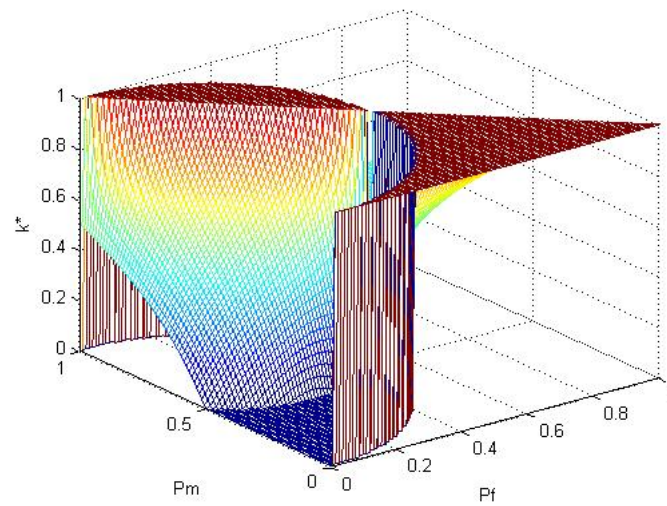
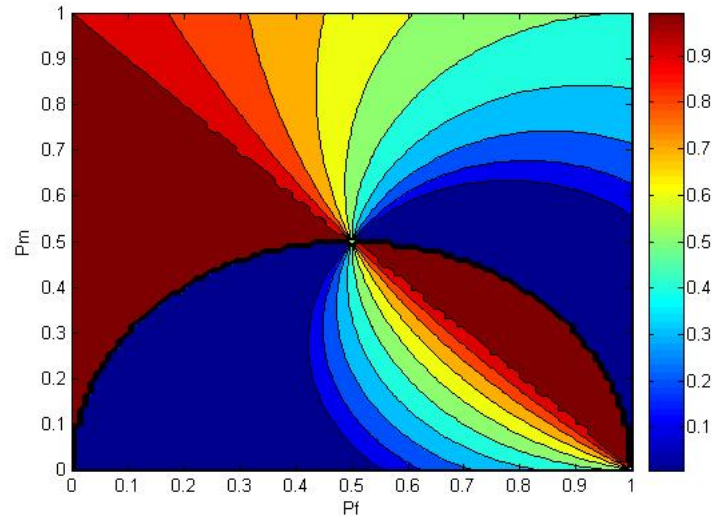
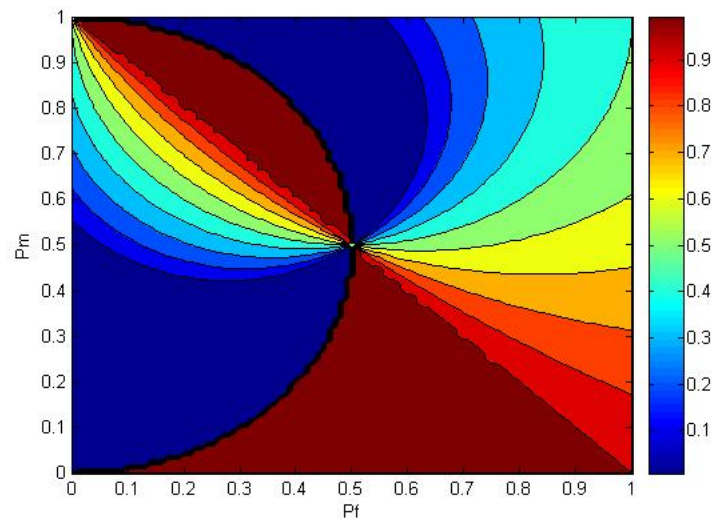


Figura 4.27: Linee di livello di k^ per banda libera.**Figura 4.28: Linee di livello di k^* per banda occupata.*

si rende conto che essi vanno a zero in diversi punti, posti lungo delle linee simili a semicirconferenze. Un grafico lineare sarà quindi poco significativo, in quanto i valori di picco che si registreranno presso gli zeri del denominatore 'appiattiranno' tutti gli altri. Ciò è confermato in Figura 4.23 e 4.24, da cui risulta come lungo le semicirconferenze corrispondenti alle linee di livello zero nei grafici dei denominatori si abbiano picchi di k^* . Si passi allora ai grafici rappresentati in Figura 4.25 e 4.26, in cui i valori di k^* maggiori di 1 sono stati ridotti a 1 e quelli minori di 0 posti a 0. In questo modo è in effetti possibile discernere l'andamento generale delle due funzioni. Considerando infine i grafici delle loro curve di livello in Figura 4.27 e 4.28 si possono anche trarre delle conclusioni.

Le zone rappresentate in blu scuro corrispondono a valori di k^* minori di 0: si tratta di zone dove non sono necessari i trusted report per avere un comportamento sincero da parte dei nodi. Le zone rappresentate in rosso scuro, d'altra parte, corrispondono a valori di k^* maggiori di 1, dove il comportamento non sarà quindi mai sincero. In ogni grafico vi sono due zone di questo tipo, ma le uniche potenzialmente problematiche sono quelle associate a valori di Pf e Pm relativamente bassi: si tratta quindi di quella più a sinistra nel primo grafico e di quella più in basso nel secondo. Le zone rappresentate con colorazione intermedia corrispondono infine a valori di k^* compresi tra 0 e 1, e sono quindi zone su cui a seconda del valore di k può essere imposto o meno un comportamento sincero. Infine si può notare come tutte le zone vadano ad intersecarsi nel punto centrale del grafico, associato a $Pf = Pm = 0.5$: ciò è giustificato dal fatto che solo in quel punto una strategia vale l'altra, dato che sia dicendo la verità sia mentendo si hanno il 50% di possibilità di sbagliare.

4.6 n rater, presenza di trusted report

Ora verrà preso in considerazione il caso in cui si hanno sia n rater sia una probabilità k di vedere una valutazione confrontata con un trusted report. Questi report vengono considerati in maniera diversa rispetto ai report non trusted: ossia quando una valutazione giunge all'aggregatore, esso la può confrontare o con n rater, o con un singolo trusted report. Un report viene pagato se il rater trusted o almeno m degli n rater concordano con esso.

La situazione dei payoff è analoga a quella in Tabella 4.2, ma essa viene impiegata solo con probabilità $1 - k$. Quindi i payoff attesi per il comporta-

mento sincero sono:

$$E(L|L) = kP(L|L) + (1-k)(P(L|L) \sum_{i=m}^n \binom{n}{i} (1-Pf)^i Pf^{n-i} + P(O|L) \sum_{i=m}^n \binom{n}{i} Pm^i (1-Pm)^{n-i})$$

$$E(O|O) = kP(O|O) + (1-k)(P(O|O) \sum_{i=m}^n \binom{n}{i} (1-Pm)^i Pm^{n-i} + P(L|O) \sum_{i=m}^n \binom{n}{i} Pf^i (1-Pf)^{n-i})$$

Quelli relativi al comportamento non sincero sono invece:

$$E(O|L) = kP(O|L) + (1-k)(P(L|L) \sum_{i=m}^n \binom{n}{i} Pf^i (1-Pf)^{n-i} + P(O|L) \sum_{i=m}^n \binom{n}{i} (1-Pm)^i Pm^{n-i})$$

$$E(L|O) = kP(L|O) + (1-k)(P(O|O) \sum_{i=m}^n \binom{n}{i} Pm^i (1-Pm)^{n-i} + P(L|O) \sum_{i=m}^n \binom{n}{i} (1-Pf)^i Pf^{n-i})$$

Imponendo l'incentivo al comportamento sincero deve essere:

$$kP(L|L) + (1-k)(P(L|L) \sum_{i=m}^n \binom{n}{i} (1-Pf)^i Pf^{n-i} + P(O|L) \sum_{i=m}^n \binom{n}{i} Pm^i (1-Pm)^{n-i}) >$$

$$kP(O|L) + (1-k)(P(L|L) \sum_{i=m}^n \binom{n}{i} Pf^i (1-Pf)^{n-i} + P(O|L) \sum_{i=m}^n \binom{n}{i} (1-Pm)^i Pm^{n-i})$$

$$kP(O|O) + (1-k)(P(O|O) \sum_{i=m}^n \binom{n}{i} (1-Pm)^i Pm^{n-i} + P(L|O) \sum_{i=m}^n \binom{n}{i} Pf^i (1-Pf)^{n-i}) >$$

$$kP(L|O) + (1-k)(P(O|O) \sum_{i=m}^n \binom{n}{i} Pm^i (1-Pm)^{n-i} + P(L|O) \sum_{i=m}^n \binom{n}{i} (1-Pf)^i Pf^{n-i})$$

che si può riscrivere come:

$$\frac{PL(k(1-Pf)+(1-k) \sum_{i=m}^n \binom{n}{i} ((1-Pf)^{i+1} Pf^{n-i} - Pf^i (1-Pf)^{n-i+1}))}{(1-Pf)PL+PmPO} - \frac{PO(kPm+(1-k) \sum_{i=m}^n \binom{n}{i} ((1-Pm)^i Pm^{n-i+1} - Pm^{i+1} (1-Pm)^{n-i}))}{(1-Pf)PL+PmPO} > 0$$

$$\frac{PO(k(1-Pm)+(1-k) \sum_{i=m}^n \binom{n}{i} ((1-Pm)^{i+1} Pm^{n-i} - Pm^i (1-Pm)^{n-i+1}))}{(1-Pm)PO+PfPL} - \frac{PL(kPf+(1-k) \sum_{i=m}^n \binom{n}{i} ((1-Pf)^i Pf^{n-i+1} - Pf^{i+1} (1-Pf)^{n-i}))}{(1-Pm)PO+PfPL} > 0$$

In una situazione ragionevole, con $PL = PO = 0.5$, $n = 3$, $m = 2$ e $k = 0.1$, l'andamento della differenza di payoff tra comportamento sincero e non è quello rappresentato nei grafici riportati in Figura 4.29 e 4.30. Alzando notevolmente il numero di rater, cercando sempre di mantenere un giusto grado di severità ($n = 10$, $m = 5$), e la frequenza dei trusted report ($k = 0.5$) la situazione cambia in linea con i comportamenti già individuati nelle sezioni precedenti. Ciò si evince dai grafici in Figura 4.31 e 4.32.

Figura 4.29: Incentivo al comportamento sincero per banda libera con $n = 3$, $m = 2$, $k = 0.1$ e $PL = PO = 0.5$.

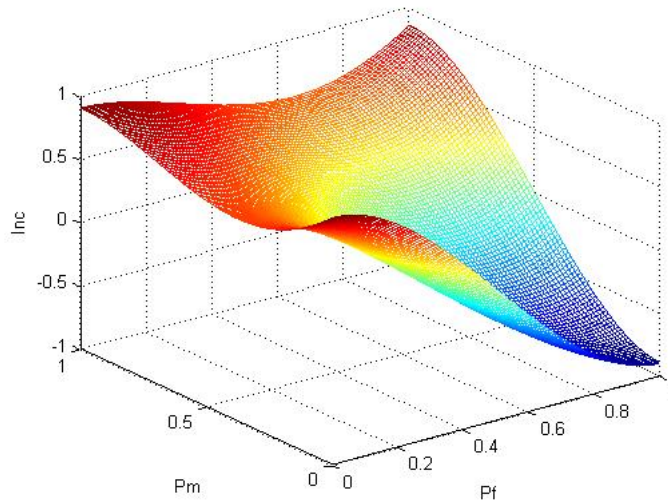


Figura 4.30: Incentivo al comportamento sincero per banda occupata con $n = 3$, $m = 2$, $k = 0.1$ e $PL = PO = 0.5$.

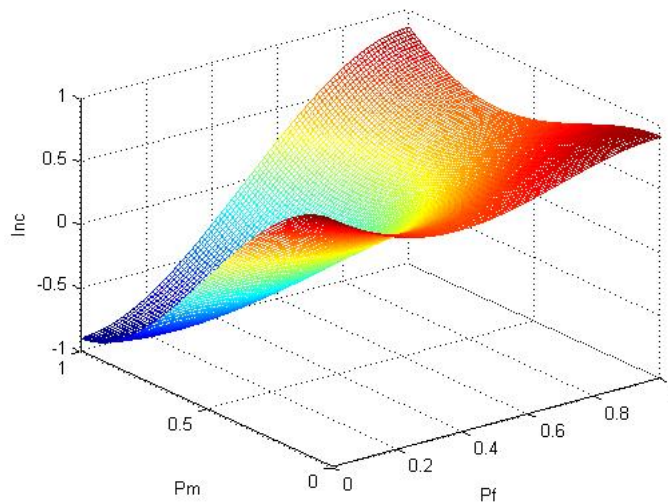


Figura 4.31: Incentivo al comportamento sincero per banda libera con $n = 10$, $m = 5$, $k = 0.5$ e $PL = PO = 0.5$.

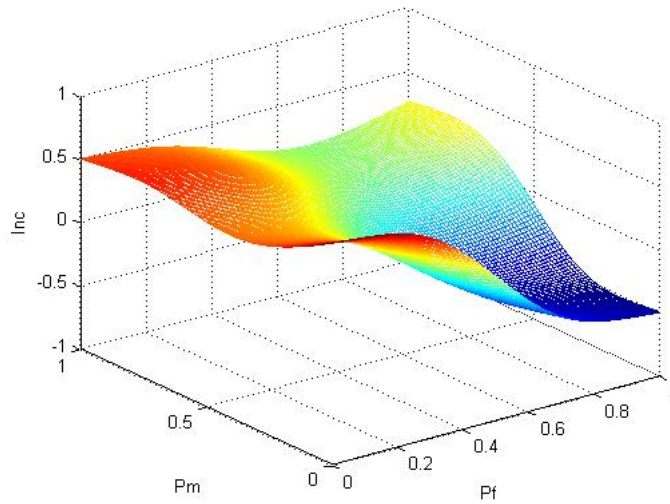


Figura 4.32: Incentivo al comportamento sincero per banda occupata con $n = 10$, $m = 5$, $k = 0.5$ e $PL = PO = 0.5$.

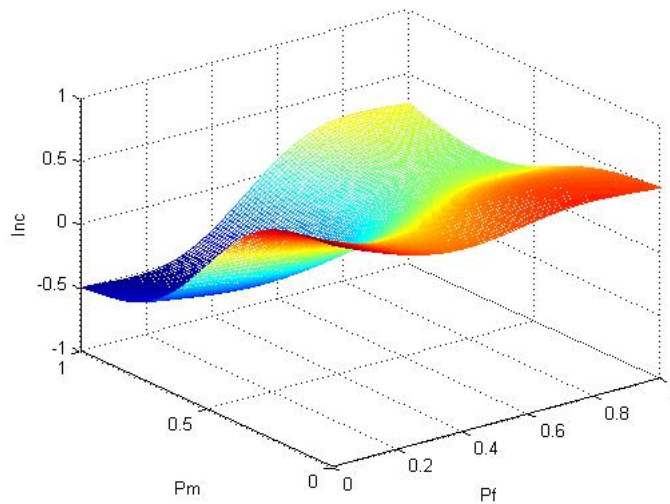


Figura 4.33: Incentivo al comportamento sincero per banda libera con $n = 10$, $m = 5$, $k = 0.5$ e $PL = 0.9$, $PO = 0.1$.

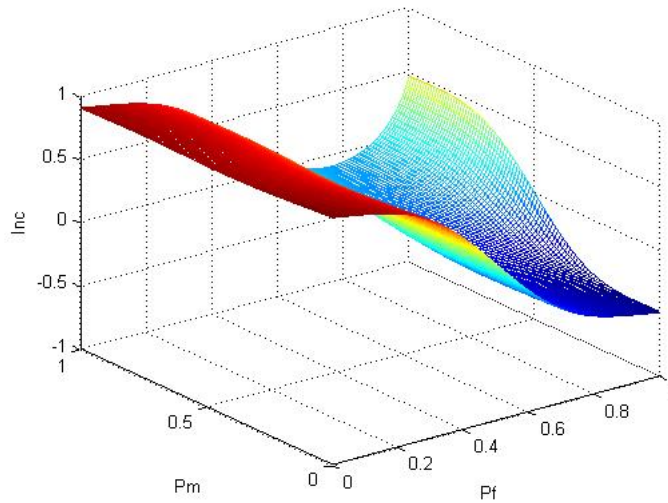


Figura 4.34: Incentivo al comportamento sincero per banda libera con $n = 10$, $m = 5$, $k = 0.5$ e $PL = 0.9$, $PO = 0.1$.

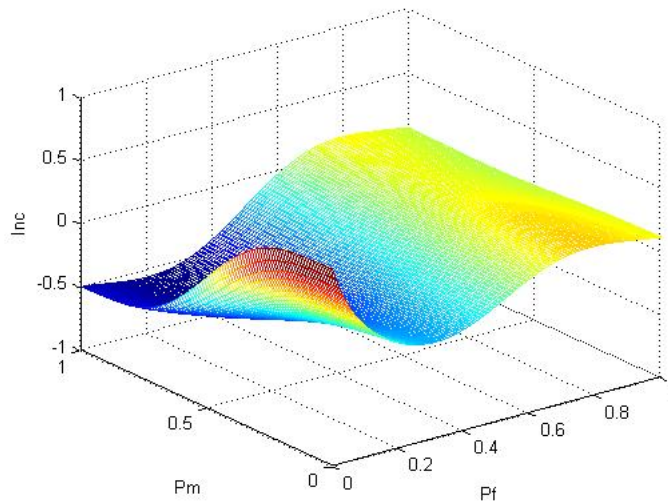


Figura 4.35: Incentivo al comportamento sincero per banda libera con $n = 10$, $m = 5$, $k = 0.5$ e $PL = 0.1$, $PO = 0.9$.

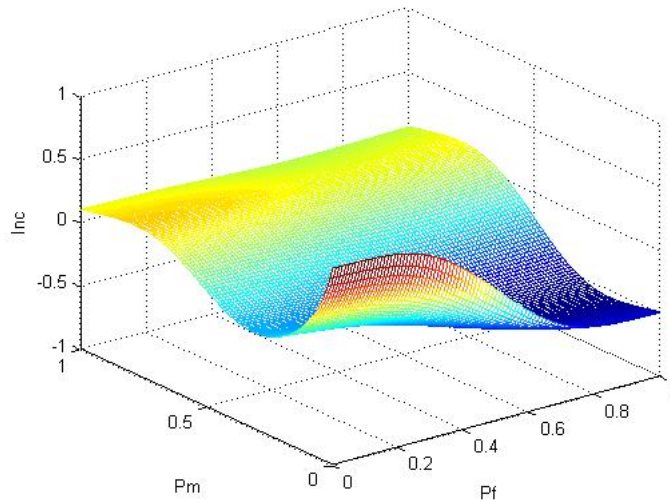
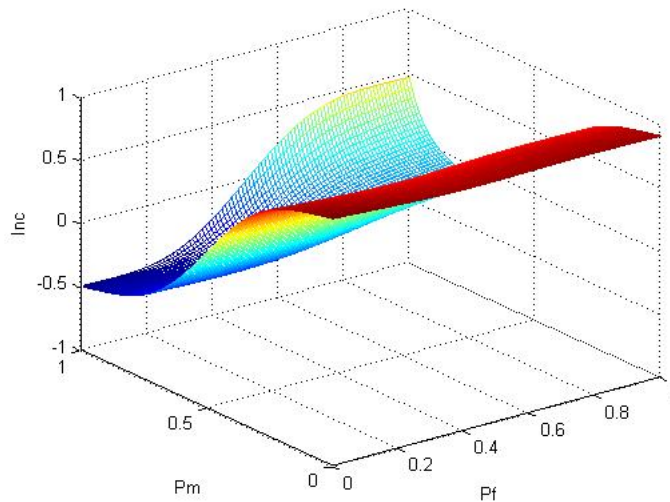


Figura 4.36: Incentivo al comportamento occupata per banda libera con $n = 10$, $m = 5$, $k = 0.5$ e $PL = 0.1$, $PO = 0.9$.



Per concludere è necessario valutare l'andamento dell'incentivo al comportamento sincero al variare di PL e PO . Per $PL = 0.9$ e $PO = 0.1$ i due grafici precedenti diventano quelli riportati in Figura 4.33 e 4.34, mentre per $PL = 0.1$ e $PO = 0.9$ la situazione si inverte, come è chiaro dai grafici in Figura 4.35 e 4.36. Anche in questo caso si può notare come, per probabilità a priori sullo stato della banda molto sbilanciate, l'effetto di un alto valore di k non sia sempre positivo.

4.7 Sintesi dei risultati

Dopo questa analisi degli equilibri del sistema al variare di PO , PL , Pf , Pm , n , m e k si possono trarre alcune conclusioni.

- Si può notare come grande sia l'influenza sugli equilibri dei valori delle probabilità a priori relative allo stato della banda. Infatti quando PL si avvicina a 1 il comportamento sincero in caso di rilevazione di banda libera è incentivato per piccoli valori di Pf , mentre in caso di banda occupata (situazione in teoria poco frequente) è incentivato per grandi valori di Pf . Quando invece è PO a tendere a 1 succede il contrario: in caso di rilevazione di banda libera (che è ora la situazione rara) sono grandi valori di Pm a incentivare il comportamento sincero, in caso di banda occupata piccoli valori di Pm . Di conseguenza se, come auspicabile, sia Pf che Pm dovessero assumere valori piccoli, potrebbero sorgere problemi per certi valori delle probabilità a priori.
- Nelle situazioni con diversi rater ciò che è importante è che la funzione di pagamento abbia il giusto grado di severità. Ciò si ha per valori di m vicini alla metà di n . Funzioni troppo generose o troppo restrittive portano a incentivi vicini allo zero per molti valori di Pf e Pm . Dato che è auspicabile che il sistema promuova sempre un comportamento onesto, tali funzioni vanno evitate.
- Al crescere di k cresce l'incentivo verso un comportamento sincero in caso di Pf e Pm entrambe basse, mentre cala se almeno uno di questi valori è troppo alto. Tuttavia a questo effetto se ne sovrappone un altro: quando PL si avvicina a 1, il crescere di k incrementa notevolmente l'incentivo per un comportamento sincero in caso di rilevazione di banda libera, mentre questo stesso incentivo crolla in caso di rilevazione di banda occupata. Se è invece PO ad avvicinarsi a 1 il crollo dell'incentivo per la sincerità si ha in caso di rilevazione di banda libera, e l'incremento in caso di banda occupata. Quando si usano i trusted

report è quindi necessario prestare particolare attenzione ai valori delle probabilità a priori relative allo stato della banda.

- Tramite adeguati valori di k si può imporre un comportamento sincero o meno per numerosi valori di Pf e Pm . Tuttavia per alcune coppie di tali valori il comportamento sincero non potrà mai essere incentivato, mentre per altre non potrà mai essere incentivato quello disonesto.

Capitolo 5

Estensioni al modello

Vengono ora presentate alcune possibili modifiche o estensioni al sistema visto nel Capitolo 3, al fine di renderlo più elastico. La prima parte è dedicata ad alcune considerazioni sulle interferenze mentre la seconda affronta il problema di nodi con precisioni diverse. Nella terza parte si considera una situazione in cui l'aggregatore sia a sua volta un utente opportunistico. Nella quarta si studia infine come sfruttare nel modello informazioni a priori relative all'utilizzo che il trasmettitore primario fa di una certa frequenza.

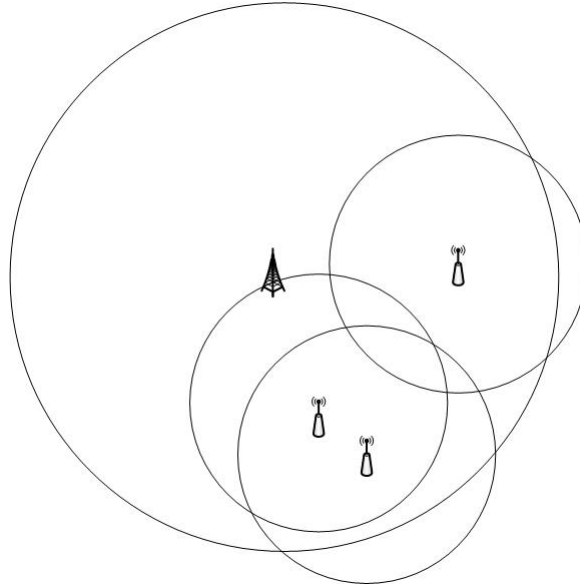
5.1 Considerazioni sulle interferenze

Come si è visto nel Capitolo 3, il sistema presentato lavora in modo abbastanza conservativo. Infatti, non appena un numero sufficiente di misurazioni rileva trasmissioni in corso da parte di un trasmettitore primario, allora una certa banda viene considerata occupata e il suo utilizzo opportunistico impedito. Tuttavia non sempre le interferenze sarebbero dannose; nel caso non lo fossero, gli utenti secondari potrebbero trasmettere comunque, migliorando ulteriormente lo sfruttamento delle frequenze disponibili. Approcci di questo tipo richiedono la conoscenza della *topografia* della rete.

5.1.1 Omogeneità dello stato delle banda nella rete

Il sistema fornisce a ogni nodo la stessa valutazione, perciò è importante che lo stato della banda sia omogeneo all'interno della rete. Se così non fosse la banda in esame potrebbe risultare libera per un nodo e occupata per un altro, con gravi ripercussioni sui loro payoff. Inoltre, impedendo di trasmettere a nodi che si trovino sufficientemente lontani dagli utenti primari da non rilevare le loro trasmissioni, si avrebbe spesso uno spreco di banda.

Figura 5.1: Esempio di rete in cui lo stato della banda è omogeneo.



Per questi motivi, se lo stato di una certa frequenza non è omogeneo all'interno della rete, è bene suddividere la stessa in reti più piccole, ognuna con il suo aggregatore. Ovviamente si potrebbe anche mantenere un solo aggregatore: esso dovrà però assegnare a ogni nodo soltanto rater che appartengano alla stessa sottorete di cui fa parte il nodo, e per ognuna di esse dovrà gestire una diversa istanza della funzione di aggregazione.

In Figura 5.1 è rappresentata una rete di tre dispositivi secondari in cui lo stato della banda è omogeneo.

5.1.2 L'influsso del raggio di interferenza

Posto che lo stato della banda sia omogeneo vi possono essere due situazioni, a seconda che le distanze tra i nodi siano o meno piccole rispetto al raggio di interferenza dei dispositivi secondari. Se lo sono allora si dovrà evitare che diversi nodi inizino a trasmettere sulla stessa banda poichè si ostacolerebbero l'un l'altro. Al contrario, ogni nodo dovrà avere la possibilità di trasmettere in modo esclusivo per un certo intervallo di tempo su una certa banda. Questa situazione è rappresentata in Figura 5.2. Nel caso invece in cui le distanze tra i nodi siano, come in Figura 5.3, grandi rispetto al raggio di interferenza allora su una stessa banda, identificata come libera, potranno trasmettere diversi operatori secondari senza pericolo di ostacolarsi a vicenda.

Figura 5.2: Esempio di rete in cui i dispositivi secondari si ostacolerebbero a vicenda.

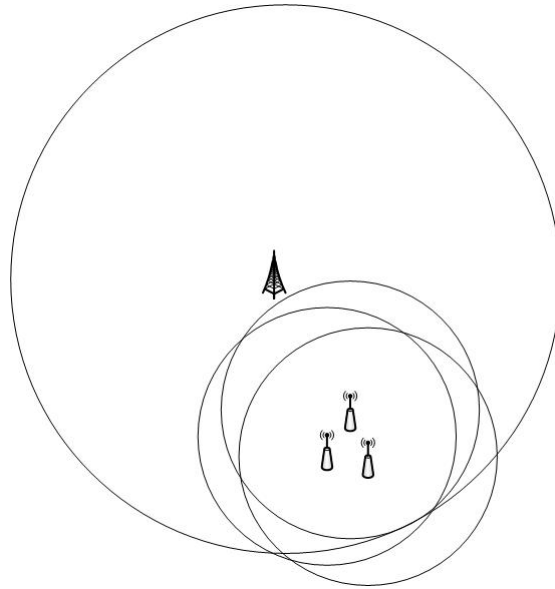


Figura 5.3: Esempio di rete in cui i dispositivi secondari non si ostacolerebbero a vicenda.

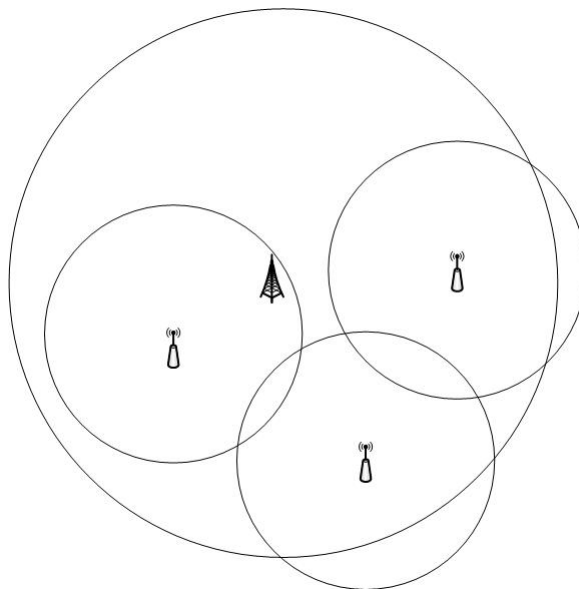
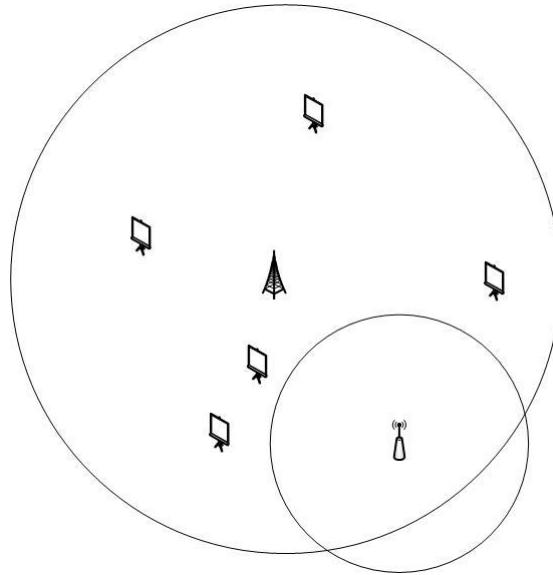


Figura 5.4: Esempio di interferenza non dannosa.



Per affrontare questo problema è possibile ricorrere a una *clusterizzazione* della rete, che raggruppi nello stesso cluster nodi abbastanza vicini da crearsi interferenza l'uno con l'altro. In questo modo, in un dato momento, si potrà dare la possibilità di trasmettere a un solo nodo per ogni cluster.

5.1.3 La posizione dei ricevitori

L'ultimo aspetto da considerare è la posizione dei ricevitori. Se un certo nodo sapesse di non avere nessun ricevitore primario nel suo raggio di interferenza allora potrebbe iniziare a trasmettere su una certa banda anche nel caso in cui essa fosse già occupata da una trasmissione dell'operatore primario. Infatti il suo utilizzo opportunistico della frequenza non disturberebbe nessuno. Questa situazione è rappresentata in Figura 5.4. Considerazioni analoghe potrebbero essere applicate anche ai ricevitori dei singoli nodi al fine di valutare la dannosità di interferenze reciproche tra dispositivi secondari che trasmettano contemporaneamente.

Anche questo affinamento passa attraverso la creazione di sottoreti o cluster, stavolta sulla base delle posizioni dei ricevitori. Tuttavia non è semplice tenere traccia di esse, quindi ottimizzazioni basate sulla loro conoscenza sono di difficile applicazione.

5.2 Precisione dei nodi in sistemi reali

Durante lo studio degli equilibri del sistema si è assunto che tutti i nodi avessero le medesime caratteristiche. Questa assunzione non è evidentemente accettabile in un sistema reale, dove ogni nodo presenterà delle differenze rispetto a ogni altro, a diversi livelli.

- In primo luogo vi saranno certamente differenze a livello tecnologico tra gli strumenti che i diversi nodi utilizzeranno per fare sensing sulla frequenza in esame: alcuni saranno più precisi, altri meno.
- Inoltre sia la conformazione naturale del territorio sia la presenza di determinate strutture artificiali può favorire la ricezione del segnale presso alcuni nodi e renderla più difficoltosa presso altri.
- Infine l'intensità del segnale emesso dallo stesso trasmettitore primario varierà a seconda della distanza, perciò nodi più o meno lontani da esso affronteranno difficoltà diverse nella fase di sensing.

Questi fattori, e altri ancora, si tradurranno essenzialmente in una probabilità di miss e una probabilità di falso allarme variabili da nodo a nodo. Per gestire in modo ottimale la rete l'aggregatore dovrà essere quindi a conoscenza dei valori di queste probabilità, o perlomeno di ragionevoli approssimazioni di essi, associati a ogni nodo che voglia fornire informazioni al sistema.

5.2.1 Scelta della probabilità di miss

Il primo passo nella progettazione di una rete è la scelta del valore della probabilità di miss globale Q_m che il sistema dovrà raggiungere: da esso deriverà poi il valore della probabilità di falso allarme globale Q_f . Come già detto, si agisce in questo modo poichè un miss è normalmente considerato un errore più grave rispetto a un falso allarme.

Noti i valori di P_m dei singoli nodi, o almeno delle loro approssimazioni, si potrà poi scegliere una funzione di pagamento tale che il vincolo su Q_m sia rispettato e un equilibrio della sincerità sia imposto. Se si vuole tenere conto del diverso livello di precisione dei vari nodi ciò può essere fatto tramite una clusterizzazione della rete, ed eventualmente una *funzione di pagamento dinamica*.

5.2.2 Clusterizzazione

Obiettivo della clusterizzazione è suddividere una rete in un certo numero di sottoreti, dette cluster, i cui nodi presentino caratteristiche simili. Fatto ciò si potranno usare gli stessi valori di Pf e Pm per ogni nodo di uno stesso cluster. Per suddividere la rete può essere utile considerare che, tipicamente, tutti i nodi all'interno di uno stesso cluster dispongono di strumenti di rilevazione di precisione simile, risentono delle stesse influenze ambientali e si trovano a distanze simili dal trasmettitore primario.

Una volta definiti i cluster, per ognuno di essi sarà necessario implementare un'adeguata funzione di pagamento. Essa dovrà soddisfare due vincoli, ossia portare a una probabilità di miss globale inferiore a Qm e incentivare un comportamento sincero da parte dei nodi. Per verificare ciò si considera, all'interno del cluster, il nodo con la Pm maggiore, e si impostano i parametri k , n e m in base a essa. Come si è visto in precedenza, i trusted report servono soprattutto per imporre l'equilibrio della sincerità, quindi per raggiungere la precisione richiesta sarà più conveniente lavorare con i valori di n e m .

Per quanto riguarda i rater, un qualunque nodo della rete potrà essere rater per qualunque altro nodo, perciò per ottenere le funzioni di pagamento dei singoli cluster sarà necessario mettersi nel caso pessimo, ossia quello in cui i rater siano il meno possibile precisi. Ciò significa che la loro probabilità di miss deve essere considerata pari a Pm_{MAX} , ossia la Pm associata al nodo meno preciso dell'intero sistema. Potrà quindi rivelarsi opportuno imporre un massimo alla probabilità di miss dei nodi che possono contribuire al sensing, per evitare di dover implementare funzioni di pagamento troppo restrittive.

Con questa tecnica a ogni nodo sarà associato un cluster, e a ogni cluster una funzione di pagamento adeguata alla precisione dei nodi che ne fanno parte. Le informazioni in ingresso al sistema saranno perciò vagliate in base alla loro affidabilità, pur conservando gli equilibri desiderati. Ovviamente si potrebbe giungere anche a una personalizzazione totale, con cluster da un singolo elemento.

5.2.3 Funzione di pagamento dinamica

Come ulteriore affinamento della tecnica di clusterizzazione vista in precedenza si potrebbe introdurre una funzione di pagamento variabile in modo dinamico. I valori di k , n e m dipenderebbero allora dai valori delle Pm dei rater che intervengono a valutare le informazioni inviate da un certo nodo. Questa dipendenza si aggiungerebbe a quella dalla Pm del cluster a cui il

nodo appartiene. Tutto ciò implicherebbe un meccanismo che, in seguito alla valutazione di ogni singolo rater, aggiorni la probabilità che le informazioni inviate siano vere, e che si accorga se e quando è il momento di procedere al pagamento. Come già detto in precedenza, per avere la probabilità di miss globale desiderata sarà più utile lavorare sul numero dei rater che sulla probabilità dei trusted report. Con un approccio di questo tipo l'imposizione dell'equilibrio relativo al comportamento sincero andrebbe effettuata assegnando alle Pf e Pm dei rater i valori medi di precisione dei nodi del sistema.

Se associato alla clusterizzazione questo approccio garantirebbe al sistema un funzionamento praticamente ottimale, a prezzo di una accresciuta complessità, e consentirebbe anche a nodi dalla bassissima precisione di contribuire efficacemente al sensing.

5.2.4 Esempio di applicazione

Come esempio di applicazione di quanto detto si consideri una rete il cui nodo meno preciso abbia una probabilità di miss $Pm_{MAX} = 0.4$. Per quanto riguarda la tecnica della clusterizzazione, si ipotizzi che il nodo meno preciso del cluster in esame presenti $Pm = 0.1$. Se si vuole ottenere una probabilità di miss globale $Qm = 0.01$ sarà necessario scegliere un numero adeguato di rater per valutare le misurazioni fornite dai nodi appartenenti al cluster. Per $m = n = 2$ si avrebbe, limitandosi per semplicità al caso di valutazioni di tipo 'banda libera':

$$Qm_L = Pm \cdot Pm_{MAX}^2 = 0.016$$

e il sistema non sarebbe abbastanza preciso. Con $m = n = 3$ si avrebbe invece:

$$Qm_L = Pm \cdot Pm_{MAX}^3 = 0.0064$$

e il vincolo su Qm_L sarebbe rispettato. A questo punto sarebbe sufficiente ripetere l'analisi per Qm_O e verificare che il comportamento sincero sia l'equilibrio di Nash a payoff massimo del sistema per avere una rete che soddisfi i requisiti.

Introducendo ora una funzione di pagamento dinamica, se le informazioni fornite da un nodo appartenente allo stesso cluster visto in precedenza venissero valutate da un rater $r1$ con $Pm_{r1} = 0.15$ si avrebbe:

$$Qm_L = Pm \cdot Pm_{r1} = 0.015$$

Figura 5.5: Problemi e soluzioni nel caso di aggregatore distribuito.

Il nodo aggregatore potrebbe...	Una soluzione per evitarlo sarebbe...
Mentire riguardo alla valutazione trusted del database (per manipolare il pagamento un nodo)	Associare alla valutazione la <i>firma digitale</i> del database
Mentire riguardo alla valutazione del rater (per manipolare il pagamento un nodo)	Richiedere che il rater confermi la sua valutazione al nodo precedente
Usare come rater non la valutazione successiva, ma una a scelta (per manipolare il pagamento di un nodo)	Associare a ogni valutazione un <i>timestamp</i> per poterne mantenere l'ordine temporale
Invocare il database più o meno spesso di quanto previsto (per danneggiare il sistema)	Rendere le condizioni di invocazione del database indipendenti dal nodo aggregatore (per esempio legandole ai valori delle timestamp dei nodi)

e quindi non si potrebbe ancora procedere al pagamento. Se a ciò si aggiungesse la valutazione di un rater r_2 con $Pm_{r_2} = 0.1$ si avrebbe:

$$Qm_L = Pm \cdot Pm_{r_1} \cdot Pm_{r_2} = 0.0015$$

e il vincolo su Qm_L sarebbe ora rispettato con soli due rater, rispetto ai tre del caso precedente. Come detto, in questo caso lo studio degli equilibri andrebbe fatto usando i valori medi delle Pf e Pm dei possibili rater.

5.3 Aggregatore distribuito

L'aggregatore non deve necessariamente essere un'entità a sé stante: si potrebbe pensare che siano gli stessi nodi, a turno, a svolgere questo ruolo. Per quanto riguarda la precisione del sistema e gli equilibri di Nash nulla cambia rispetto alla situazione considerata fino a ora, con aggregatore dedicato.

Per esempio, essendo i nodi numerati, può venire naturale pensare che ogni nodo i svolga il ruolo di aggregatore per un periodo di tempo T , per poi cedere questa funzione al nodo $i + 1$. In questo modo i compiti dell'aggregatore sono equamente distribuiti tra tutti i nodi. Tuttavia ora l'aggregatore,

Figura 5.6: Funzionamento del sistema con aggregatore distribuito.

Istante	Evento	Descrizione
0	Passaggio del ruolo di aggregatore da $i - 1$ a i	$i - 1$ comunica a i numero di nodo 0, valore v_0 e timestamp t_0 dell'ultima valutazione ricevuta.
1	i riceve una valutazione dal nodo 1 con valore v_1 e timestamp t_1	i combina t_0 e t_1 e determina che il rater di 0 debba essere il database. Quindi contatta il database, comunica la valutazione del database (con relativa firma digitale) a 0, effettua il pagamento e invita N_1 a comunicare t_1 a 0.
2	i riceve una valutazione dal nodo 2 con valore v_2 e timestamp t_2	i combina t_1 e t_2 e determina che il rater di 1 debba essere 2. Quindi effettua il pagamento e invita N_2 a comunicare v_2 e t_2 a 1.
3	Passaggio del ruolo di aggregatore da i a $i + 1$	i comunica a $i + 1$ numero di nodo 2, valore v_2 e timestamp t_2 dell'ultima valutazione ricevuta.

non essendo più un'entità trusted, può trarre benefici indebiti dal suo status in diversi modi. In Tabella 5.5 viene riassunto come questo possa succedere, e quali potrebbero essere le possibili soluzioni.

Inserendo nel sistema i meccanismi di sicurezza esposti in Tabella 5.5 esso avrebbe un funzionamento come quello riportato in Tabella 5.6. Poiché ogni nodo può confrontare la timestamp della propria valutazione con quella della valutazione successiva, e alla fine del proprio turno l'aggregatore può comunicare il numero di un solo nodo in attesa di essere pagato, l'aggregatore deve rispettare l'effettivo ordinamento delle valutazioni. Inoltre, grazie alla firma digitale del database e al fatto che ogni nodo ha un contatto diretto con il suo rater, l'aggregatore non può mentire sui valori delle valutazioni. Infine non si può barare nemmeno sulla frequenza delle invocazioni del database, poiché sono determinate dalle timestamp delle valutazioni dei nodi.

5.4 Stima delle caratteristiche di una frequenza

A volte si dispone di informazioni aggiuntive relative all'utilizzo che un operatore primario fa di una certa frequenza, ed esse potrebbero essere sfruttate per rendere più efficiente il sensing operato su quella stessa frequenza. Viene ora esposto come tali informazioni possano essere incorporate nel modello presentato.

5.4.1 Il duty cycle

Nel capitolo precedente si è studiato l'andamento degli equilibri al variare della probabilità di miss, di quella di falso allarme, dell'incidenza dei trusted report e del numero di rater. Nel fare ciò sono state introdotte due probabilità che indicano caratteristiche intrinseche della banda su cui si opera il sensing: la probabilità che in un qualsiasi momento la banda sia libera, PL , e quella che sia occupata, PO .

In situazioni reali, quando si studia lo stato di occupazione di una data banda, si usano due grandezze per caratterizzarlo. La prima è la *densità di potenza spettrale*, PSD , e rappresenta la quantità di energia ricevuta sulla banda. La seconda è il *duty cycle*, ossia la frazione di tempo durante la quale la banda è considerata occupata. Il suo significato è quindi sostanzialmente lo stesso di PO .

Riprendendo concetti visti nel Capitolo 2, il metodo normalmente utilizzato nello spectrum sensing è quello della energy detection [6]. Innanzitutto si deve quindi scegliere un valore di soglia γ , poi si operano N rilevazioni sulla banda in esame. Una rilevazione consiste in un certo intervallo di tempo passato a misurare l'energia trasmessa sulla banda. Nella rilevazione t si parlerà di banda occupata se questa supera il valore soglia, altrimenti la banda andrà considerata libera [17]. In formule si può scrivere:

$$\Omega_t = \begin{cases} 0 & \text{se } PSD_t < \gamma \\ 1 & \text{se } PSD_t \geq \gamma \end{cases}$$

dove Ω_t indica lo stato della banda nella rilevazione t . Di conseguenza il duty cycle si ottiene in questo modo:

$$DC = \frac{\sum_{t=1}^N \Omega_t}{N}$$

Trattandosi di dati statistici, duty cycle e grandezze quali le durate degli intervalli di tempo in cui la banda è libera o occupata possono essere rappresentati da adeguate distribuzioni di probabilità. Inoltre, le durate degli

intervalli possono spesso (ma non sempre, in quanto in certe situazioni si hanno segni di correlazione) essere considerate delle *variabili aleatorie i.i.d.* La loro distribuzione varia a seconda del carico sulla banda: una distribuzione *lognormale 'a code alte'* è per esempio adatta a rappresentare la durata degli intervalli in cui la banda è libera se il carico è basso, o la durata degli intervalli in cui è occupata se il carico è alto. Altre distribuzioni spesso usate sono quella *geometrica*, quella *esponenziale* e quella *di Pareto* [18] [19].

Per quanto riguarda il duty cycle, si può notare come valori prossimi a 0 o a 1 siano molto frequenti. Ciò suggerisce l'uso di una distribuzione β :

$$f_b(x; \alpha, \beta) = \frac{1}{B(\alpha, \beta)} x^{\alpha-1} (1-x)^{\beta-1}, x \in (0, 1)$$

dove α e β sono i parametri che controllano il comportamento della distribuzione e B è l'*integrale* β :

$$B(\alpha, \beta) = \int_0^1 t^{\alpha-1} (1-t)^{\beta-1} dt$$

Poichè una distribuzione β non giunge mai ai valori 0 e 1 è opportuno operare una modifica in questa direzione. Siano $p_{DC=0}$ e $p_{DC=1}$ le probabilità relative rispettivamente a una banda sempre libera e a una banda sempre occupata. La distribuzione β può allora essere modificata in questo modo:

$$f_{mb}(x; \alpha, \beta) = p_{DC=0} \cdot \delta(x) + (1 - p_{DC=0} - p_{DC=1}) \cdot f_b(x; \alpha, \beta) + p_{DC=1} \cdot \delta(x-1),$$

$$x \in [0, 1]$$

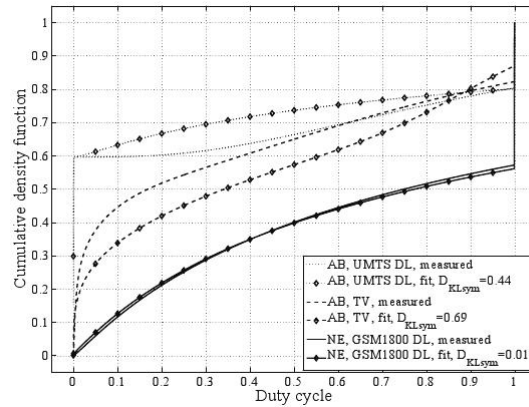
dove $\delta(x)$ è il *delta di Dirac*. Facendo variare i valori di α , β , $p_{DC=0}$ e $p_{DC=1}$ diventa così possibile avere le distribuzioni del duty cycle in diversi contesti [17].

5.4.2 Contributo del duty cycle al modello degli equilibri

Le informazioni relative al valore del duty cycle e alla sua distribuzione possono essere utilizzate per ricavare adeguati valori per PL e PO da utilizzare nel modello. Infatti, come si è già detto, il valore del duty cycle corrisponde sostanzialmente al valore di PO , e quindi da esso si può ricavare anche PL .

Gli andamenti delle distribuzioni possono invece essere utilizzati per conferire solidità al sistema. Se non si è certi del valore di PO (e quindi di quello di PL) è infatti possibile determinare, in base alla distribuzione del duty cycle, un intervallo di confidenza in cui è ragionevole ritenere che esso cada. A questo punto si tratta di analizzare l'andamento degli equilibri di Nash del sistema al variare di PO all'interno di tale intervallo. Come

Figura 5.7: Esempi di distribuzioni del duty cycle in diversi contesti.



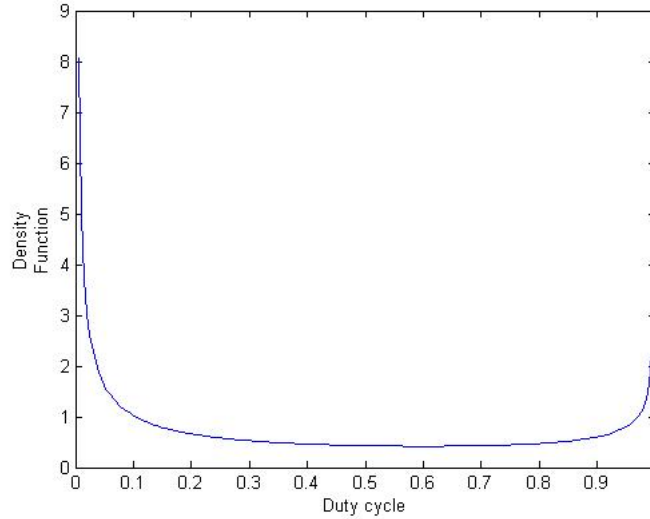
si è visto nel Capitolo 4 un comportamento sincero è conveniente solo per adeguate combinazioni dei valori di precisione dei nodi, dei parametri della funzione di aggregazione e delle probabilità a priori relative allo stato della banda. Una volta determinato il valore di PO che, all'interno dell'intervallo di confidenza scelto, richiede le condizioni più restrittive sui valori degli altri parametri, si impone l'incentivo al comportamento sincero in base a esso, e automaticamente tale comportamento sarà imposto sull'intero intervallo.

5.4.3 Un esempio applicativo: il caso delle frequenze TV

Il caso delle frequenze TV è particolarmente importante nell'ambito dello spectrum sensing. Infatti è in questo campo che si attendono i primi sistemi in grado di occupare dinamicamente le bande che di volta in volta si liberano, secondo lo standard IEEE 802.22 [12]. Modelli relativi allo stato di occupazione di questo genere di frequenze sono perciò fondamentali.

Osservazioni sperimentali operate tra Germania e Olanda attorno alla frequenza di 770 MHz sono andate a studiare il duty cycle in diversi contesti applicativi, tra cui quello televisivo [17]. In Figura 5.7 sono riportati alcuni dei risultati ottenuti relativamente alle distribuzioni dei duty cycle. In base a misurazioni di questo genere è possibile ricavare i parametri α , β , $p_{DC=0}$ e $p_{DC=1}$ della distribuzione β modificata vista in precedenza che a essi meglio si adatta. Nel caso delle frequenze TV, per un valore soglia $\gamma = -107\text{ dB}$ (valore che era effettivamente stato preso in considerazione dalla FCC

Figura 5.8: Densità di probabilità del duty cycle per frequenze TV.



per applicazioni di *cognitive radio* [18]), sono risultati i seguenti parametri:

$$\alpha = 0.294$$

$$\beta = 0.534$$

$$p_{DC=0} = 0.005$$

$$p_{DC=1} = 0.140$$

La densità di probabilità corrispondente a questi valori è rappresentata in Figura 5.8. Come si può notare, il duty cycle è spesso prossimo a 0 o prossimo a 1, e solo più raramente assume valori intermedi.

Queste informazioni sono preziose per la scelta dei valori di PO e PL da utilizzare nello studio degli equilibri. Infatti, nel caso in cui si pensi che il duty cycle abbia valore vicino a 0 è opportuno cautelarsi e considerare l'intervallo di valori compresi tra 0 e 0.1, dato che contiene valori relativamente frequenti. Allo stesso modo se risulta un valore prossimo a 1 conviene considerare l'intervallo da 0.95 a 1. Il caso in cui risulti un duty cycle con valore lontano da 0 e da 1 è piuttosto raro, e stando alla distribuzione teorica di DC anche considerando un intervallo ampio attorno al valore sperimentale la probabilità di includere quello effettivo non cresce in maniera soddisfacente.

Capitolo 6

Analisi in simulazione

In questo capitolo vengono presentati i risultati di una serie di simulazioni svolte al fine di determinare valori ottimali per i parametri del modello sviluppato nel Capitolo 3. Il software utilizzato è *MATLAB*, mentre il codice è riportato nell'Appendice A. Nella prima sezione viene presentato il contesto generale in cui si sono svolte le simulazioni, mentre nella seconda e nella terza si studiano le prestazioni del sistema al variare rispettivamente della precisione del sensing e del numero dei nodi maliziosi. Nella quarta sezione a variare è la durata degli intervalli tra i cambi di stato della frequenza su cui si opera il sensing. Infine nella quinta sezione si cercano di determinare valori ottimali per k in contesti più complessi.

6.1 Contesto generale

Come detto, le simulazioni sono state svolte in *MATLAB* con il codice riportato nell'Appendice A. Esso simula l'evoluzione nel tempo di una rete per spectrum sensing costruita sul modello presentato nel Capitolo 3. Ogni nodo possiede quindi dei crediti, che può spendere per avere da un aggregatore informazioni sullo stato di una certa frequenza e che può incrementare fornendo sempre all'aggregatore valutazioni sullo stato di questa stessa frequenza che vengano poi confermate da un certo numero di rater. Alcuni parametri del modello hanno lo stesso valore in ogni simulazione: essi sono presentati in Tabella 6.1. Si può notare come il costo del servizio sia abbastanza basso rispetto all'entità del pagamento: questo per cercare di evitare che i nodi possano finire i crediti ed essere quindi esclusi dal sistema.

Figura 6.1: Parametri comuni a ogni simulazione.

Parametro	Valore
Numero dei nodi	1000
Crediti iniziali	5
Costo del servizio	1
Entità del pagamento	2
Numero di rilevazioni	1000

6.2 Studio degli effetti degli errori di sensing

Lo studio degli errori di sensing consiste nel valutare come i valori di Pf e Pm associati ai singoli nodi, e per semplicità considerati uguali per ognuno di essi, influiscano sulle probabilità di miss e di falso allarme globali del sistema. In questo contesto le probabilità di avere nodi non sinceri sono state poste a 0 e lo stato della banda costante. I trusted report sono stati disattivati, in quanto non servono per aumentare la precisione del sensing ma per disincentivare comportamenti disonesti.

6.2.1 Probabilità di miss globale

La prima analisi è centrata sull'andamento della probabilità di miss globale del sistema al variare della funzione di aggregazione. In Figura 6.2, 6.3 e 6.4 sono riportati i risultati ottenuti assegnando a n rispettivamente i valori 3, 5 e 10, e facendo variare m da 1 a n . Nel fare ciò a ogni nodo vengono associati dei valori di Pf e Pm pari a 0.1, e lo stato della banda è ovviamente supposto costantemente occupato.

Si può notare come i risultati migliori si ottengano in figura 6.4, per valori di m attorno a 5. Questo perchè la funzione di aggregazione deve avere il giusto grado di severità: funzioni molto generose generano molti miss perchè è troppo facile che una valutazione errata venga confermata, mentre funzioni troppo restrittive ne generano ancora di più perchè troppo spesso valutazioni corrette non vengono confermate. Al crescere di n la granularità che è possibile attribuire alla severità della funzione variando il valore di m diventa più fine, e quindi si possono avere prestazioni migliori.

Ora si passa all'analisi della probabilità di miss globale al variare da 0 a 0.5 dei valori di Pf e Pm dei singoli nodi, utilizzando per n i tre valori visti in precedenza e per m il valore che di volta in volta ha generato le prestazioni

Figura 6.2: Probabilità di miss globale in funzione di m con $n = 3$ e $P_f = P_m = 0.1$.

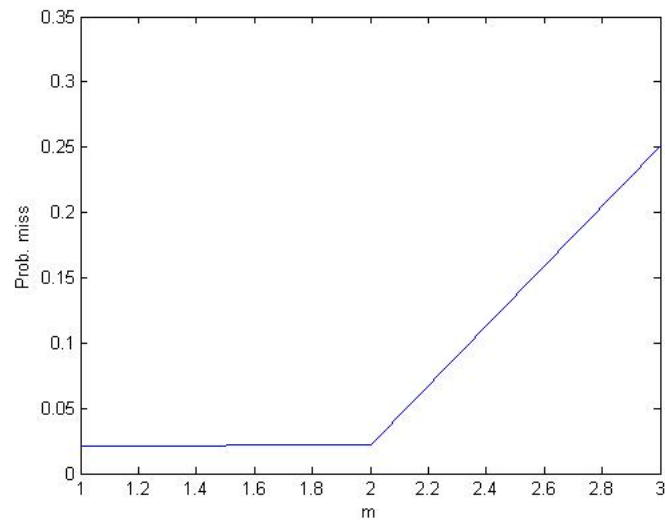


Figura 6.3: Probabilità di miss globale in funzione di m con $n = 5$ e $P_f = P_m = 0.1$.

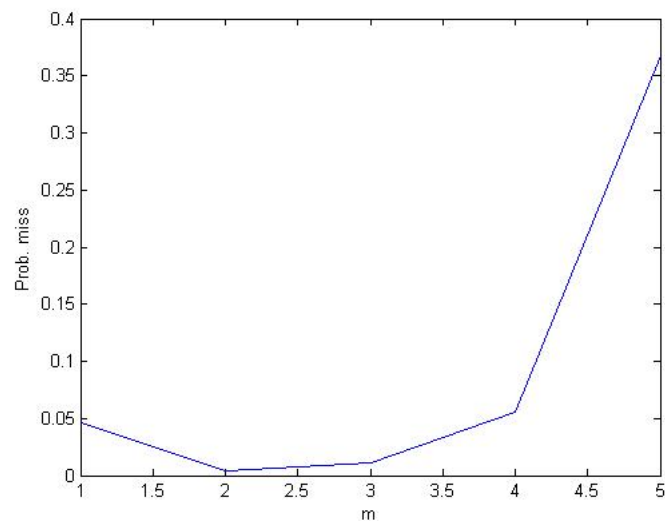
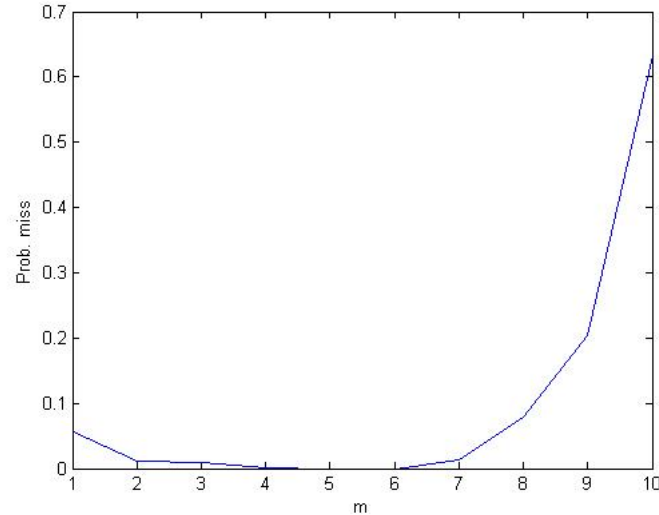


Figura 6.4: Probabilità di miss globale in funzione di m con $n = 10$ e $Pf = Pm = 0.1$.



migliori, quindi rispettivamente 1, 2 e 5. I risultati sono riportati in Figura 6.5, 6.6 e 6.7.

Si può notare che anche al variare dei valori associati alle probabilità di errore dei singoli nodi funzioni di aggregazione con n alto si comportano meglio di funzioni di aggregazione con n basso. Per questo motivo nelle successive analisi si considereranno principalmente funzioni del tipo m -su-10. Per concludere, come caso particolare, si presentano in Figura 6.8 le prestazioni di un sistema a singolo rater.

6.2.2 Probabilità di falso allarme globale

Ora si passa allo studio dell'andamento della probabilità di falso allarme globale del sistema. Per come è strutturato il modello i risultati saranno del tutto analoghi a quelli emersi nello studio dei miss presentato nella sezione precedente, per cui l'analisi sarà ora meno approfondita. Per averne conferma in Figura 6.9 vengono riportati i risultati ottenuti con funzione di aggregazione del tipo m -su-10, per m che va da 1 a 10, e Pf e Pm costanti e pari a 0.1. In Figura 6.10 la funzione di aggregazione è invece 5-su-10 e a variare è la precisione dei singoli nodi. Trattandosi di uno studio sui falsi allarmi lo stato della banda è supposto costantemente libero.

Figura 6.5: Probabilità di miss globale in funzione di P_f e P_m con $n = 3$ e $m = 1$.

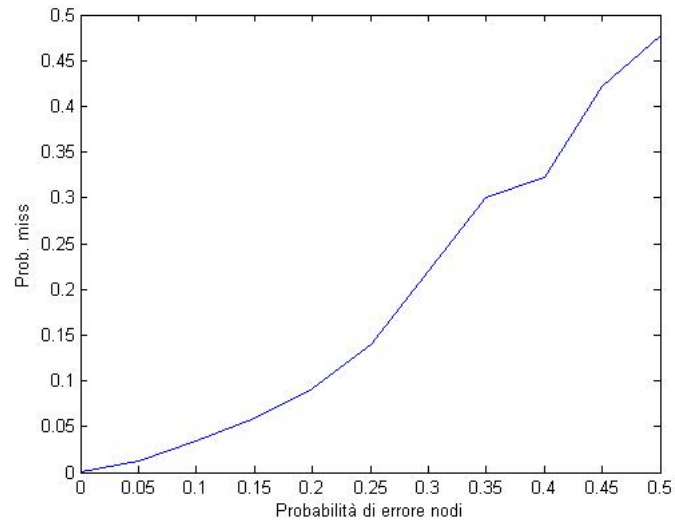


Figura 6.6: Probabilità di miss globale in funzione di P_f e P_m con $n = 5$ e $m = 2$.

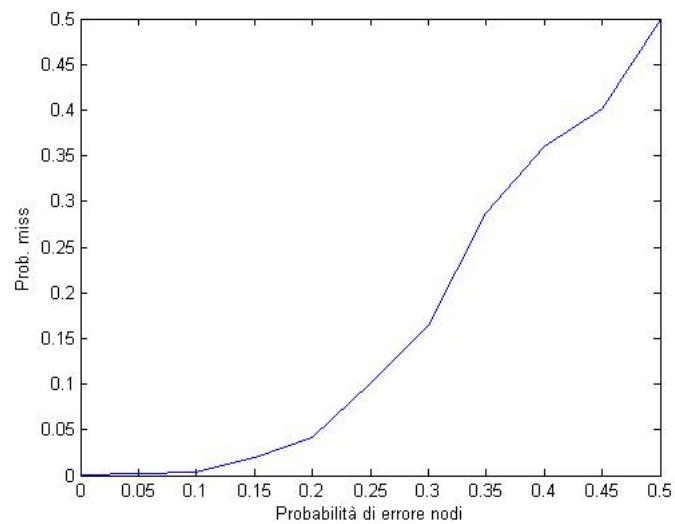


Figura 6.7: Probabilità di miss globale in funzione di P_f e P_m con $n = 10$ e $m = 5$.

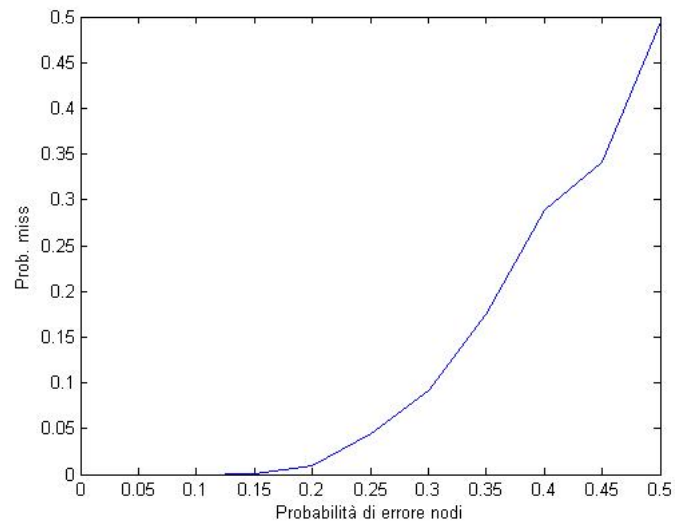


Figura 6.8: Probabilità di miss globale in funzione di P_f e P_m con singolo rater.

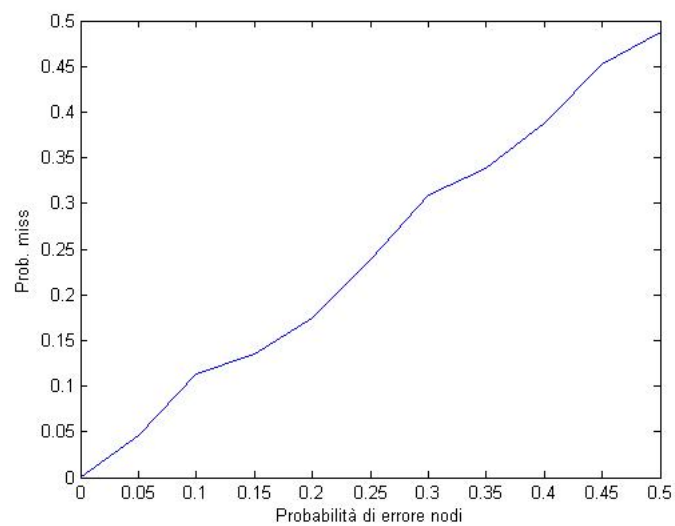


Figura 6.9: Probabilità di falso allarme globale in funzione di m con $n = 10$ e $P_f = P_m = 0.1$.

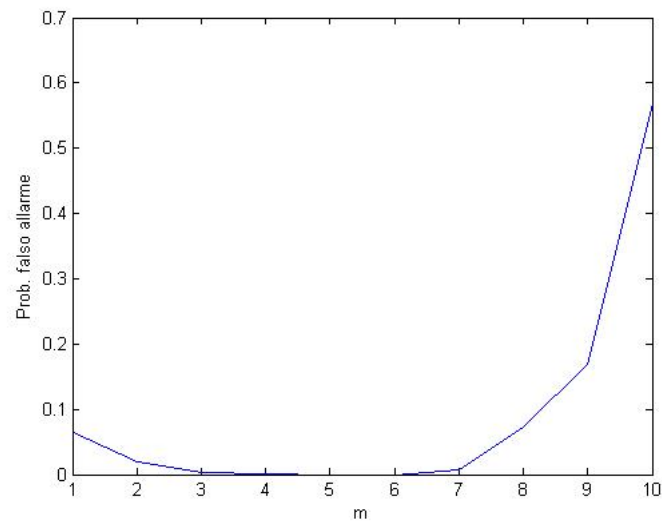


Figura 6.10: Probabilità di falso allarme globale in funzione di P_f e P_m con $n = 10$ e $m = 5$.

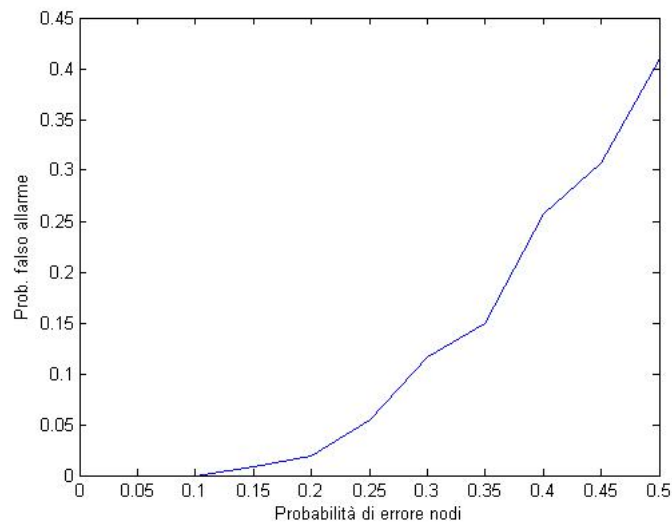
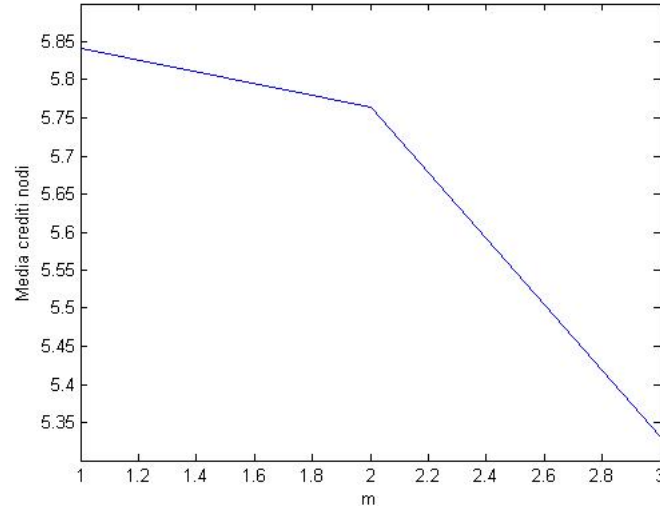


Figura 6.11: Media dei crediti residui dei nodi in funzione di m con $n = 3$ e $Pf = Pm = 0.1$.



6.2.3 Crediti dei nodi

Per concludere l'analisi relativa alla precisione del sensing si considera l'andamento dei valori dei crediti residui dei nodi al termine dei 1000 passi di simulazione al variare della funzione di aggregazione in un contesto dove ogni nodo abbia $Pf = Pm = 0.1$. I risultati sono riportati in Figura 6.11, 6.12 e 6.13, dove m varia da 1 a n e n assume rispettivamente i tre valori già incontrati in precedenza: 3, 5 e 10.

Trattandosi di nodi sempre sinceri, ognuno dei quali possiede inizialmente 5 crediti, è auspicabile che la media dei crediti residui, al termine delle simulazioni, sia maggiore di 5. Ciò è praticamente sempre verificato, a parte in Figura 6.13 per $m = 10$. In corrispondenza dei valori di m che garantiscono le prestazioni migliori a livello di miss e falsi allarmi per i tre valori di n presi in considerazione il numero di crediti residui è sempre intorno a 5.8, un valore vicino al massimo possibile: ciò significa che in quel caso i nodi hanno un forte incentivo a contribuire al sensing.

Passando all'analisi dell'andamento dei crediti al variare della precisione dei nodi, con le tre funzioni di aggregazione emerse come ottimali nello studio delle prestazioni del sistema (ossia 1-su-3, 2-su-5 e 5-su-10) si ottengono i risultati riportati rispettivamente in Figura 6.14, 6.15 e 6.16.

In questo caso le tre funzioni di aggregazione si comportano in modo

Figura 6.12: Media dei crediti residui dei nodi in funzione di m con $n = 5$ e $Pf = Pm = 0.1$.

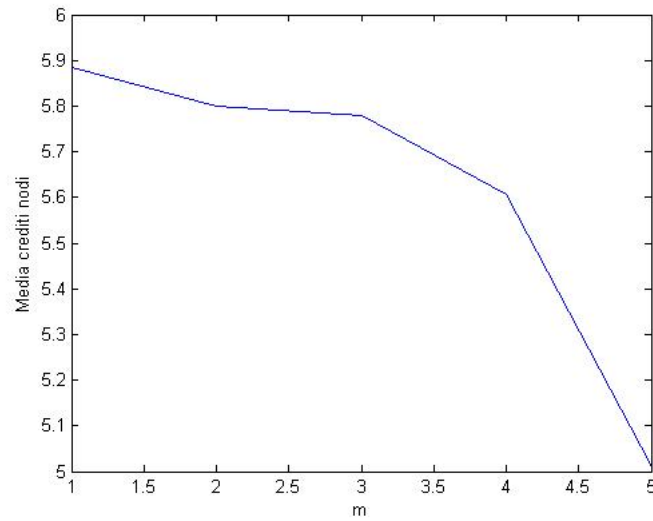


Figura 6.13: Media dei crediti residui dei nodi in funzione di m con $n = 10$ e $Pf = Pm = 0.1$.

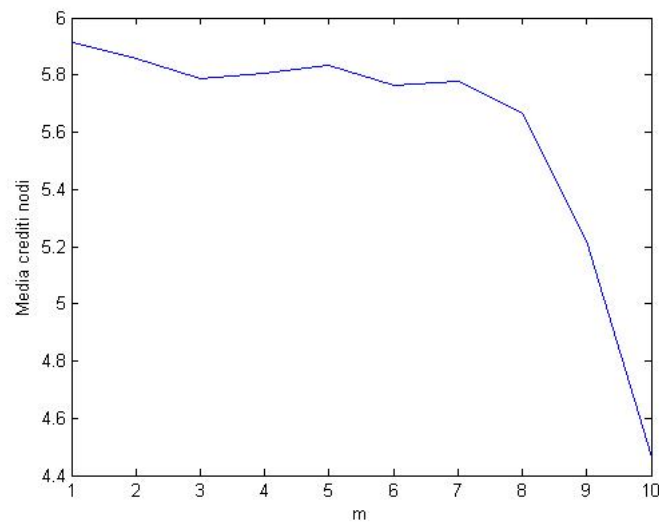


Figura 6.14: Media dei crediti residui dei nodi in funzione di P_f e P_m con $n = 3$ e $m = 1$.

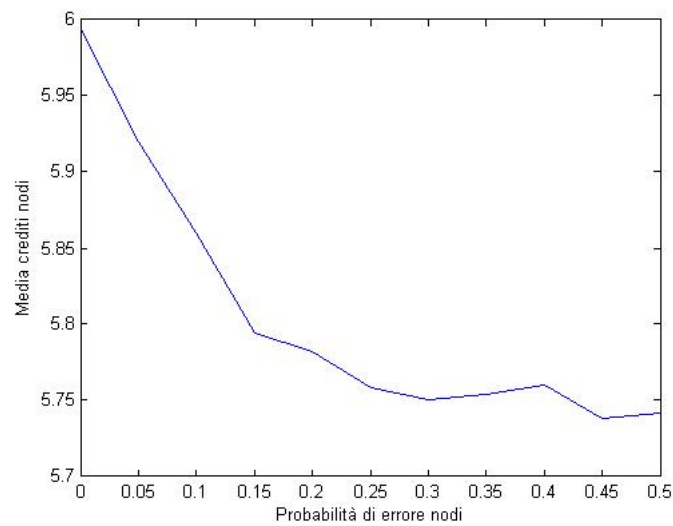


Figura 6.15: Media dei crediti residui dei nodi in funzione di P_f e P_m con $n = 5$ e $m = 2$.

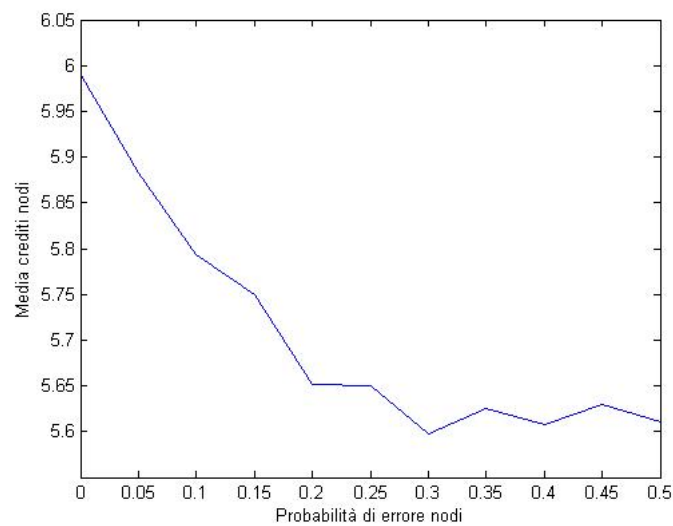
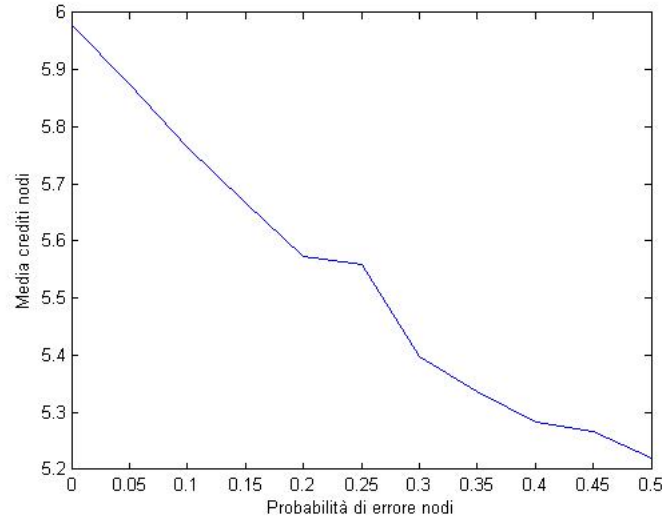


Figura 6.16: Media dei crediti residui dei nodi in funzione di Pf e Pm con $n = 10$ e $m = 5$.

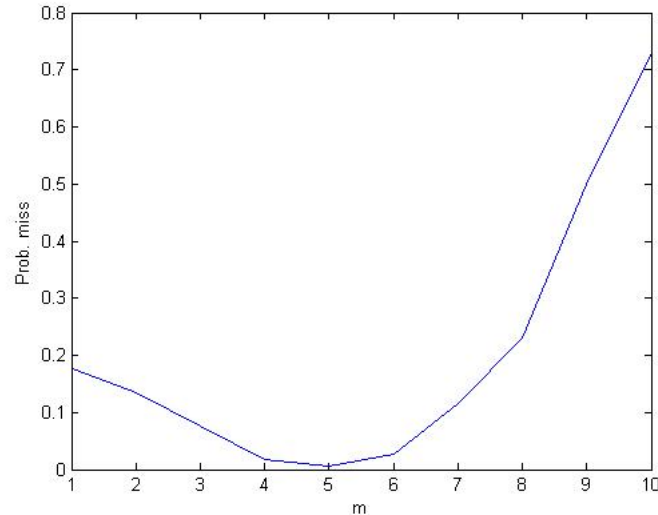


piuttosto diverso, con quelle associate a $n = 3$ e $n = 5$ che, al crescere dell'imprecisione dei nodi oltre una certa soglia, tendono ad assestarsi su valori di crediti medi residui più alti rispetto a quella associata a $n = 10$. Tuttavia, per valori di Pf e Pm più contenuti, le tre funzioni hanno un andamento simile. In ogni caso il valore dei crediti residui non scende mai sotto il valore iniziale di 5: ciò significa che, in linea con i valori associati a costi e pagamenti, in questo contesto per non avere convenienza a partecipare al sensing è necessario avere una probabilità di errore maggiore del 50%.

6.3 Studio degli effetti dei nodi maliziosi

In questa sezione viene studiato come la presenza di nodi maliziosi possa influire sulle prestazioni del sistema. Tali nodi cercano di danneggiare la rete, perciò invieranno sempre valutazioni opposte al loro belief: se a loro la banda sembra occupata diranno che è libera, e viceversa. In questa fase gli errori di sensing vengono trascurati, e lo stato della banda è considerato costante. Vengono però introdotti i trusted report, per valutare il loro impatto sui comportamenti disonesti.

Figura 6.17: Probabilità di miss globale in funzione di m con nodi maliziosi, $n = 10$ e $k = 0$.



6.3.1 Probabilità di miss globale

Si consideri una rete in cui il 20% dei nodi sia di tipo malizioso. In Figura 6.17, 6.18 e 6.19 viene presentato l'andamento della probabilità di miss del sistema al variare della funzione di aggregazione. Essa assume una forma del tipo m -su-10, con m che va da 1 a 10: tale funzione è quella che ha dato i risultati migliori nei test condotti nella sezione precedente. Nelle tre figure k assume rispettivamente i valori di 0, 0.2 e 0.5. Dato che si lavora sui miss, la banda viene supposta costantemente occupata.

Come era lecito immaginarsi, al crescere di k cala la probabilità di miss. Tuttavia la dipendenza più evidente è quella da m : essa mostra che, anche in presenza di nodi maliziosi, i valori che garantiscono le prestazioni migliori sono gli stessi valori che le garantivano in presenza di errori di sensing. Un valore di m intorno alla metà di quello di n si conferma quindi una buona scelta.

Ora si passa a studiare le prestazioni del sistema in dipendenza dalla percentuale dei nodi maliziosi sul totale dei nodi della rete, che viene fatta variare dallo 0% al 100%. Ancora una volta k assume i valori di 0, 0.2 e 0.5, e i risultati sono riportati rispettivamente in Figura 6.20, 6.21, 6.22. La funzione di aggregazione è quella che è emersa come ottimale nel caso precedente, con $m = 5$.

Figura 6.18: Probabilità di miss globale in funzione di m con nodi maliziosi, $n = 10$ e $k = 0.2$.

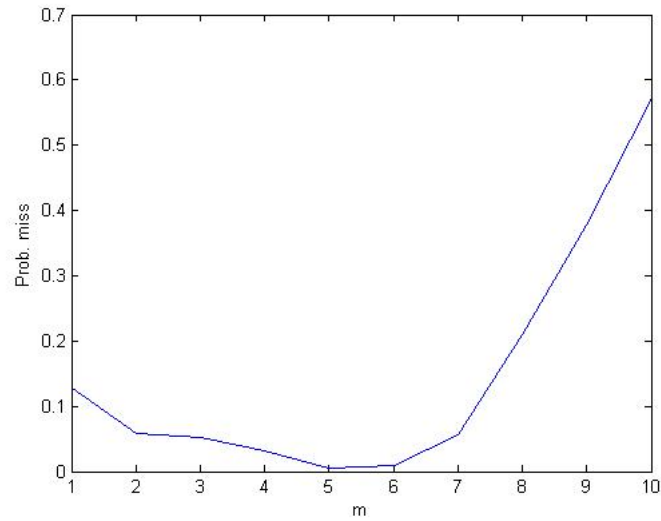


Figura 6.19: Probabilità di miss globale in funzione di m con nodi maliziosi, $n = 10$ e $k = 0.5$.

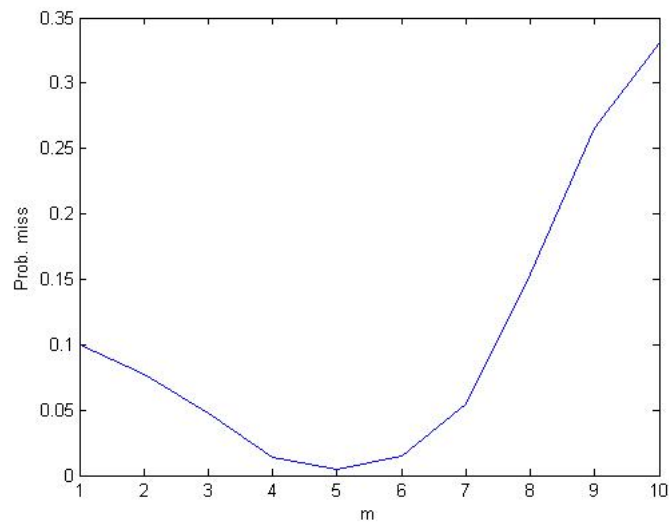


Figura 6.20: Probabilità di miss globale in funzione della probabilità di nodo malizioso con $n = 10$, $m = 5$ e $k = 0$.

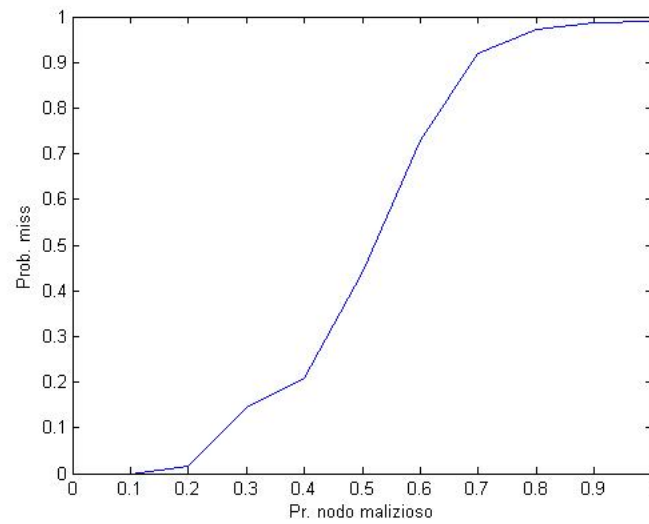


Figura 6.21: Probabilità di miss globale in funzione della probabilità di nodo malizioso con $n = 10$, $m = 5$ e $k = 0.2$.

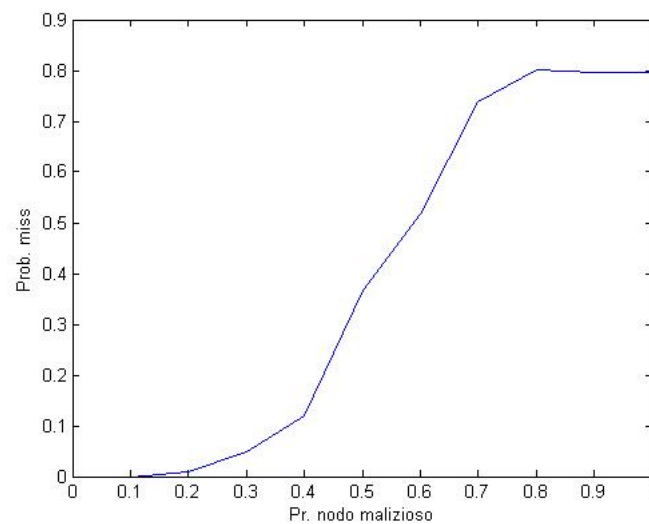
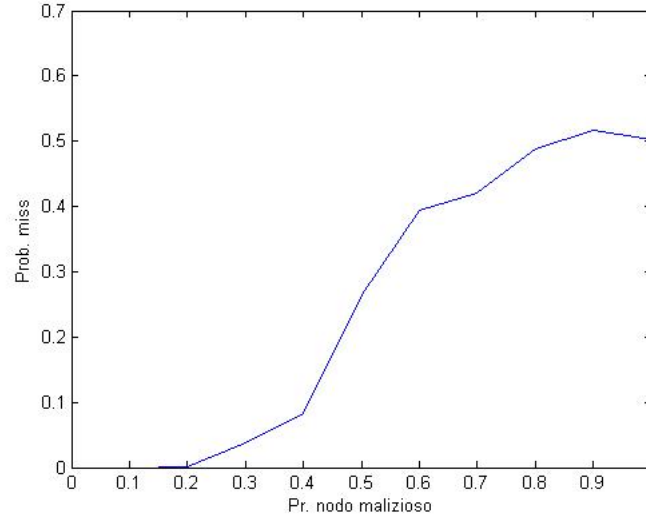


Figura 6.22: Probabilità di miss globale in funzione della probabilità di nodo malizioso con $n = 10$, $m = 5$ e $k = 0.5$.



Con $k = 0$ le prestazioni del sistema sono buone solo fino a una probabilità di nodo malizioso pari a 0.2. Valori di k più alti sembra che possano rendere in qualche modo gestibili situazioni in cui fino al 30% dei nodi è malizioso, ma i risultati non sono brillanti. Del resto i trusted report servono per incentivare comportamenti, solo secondariamente sono utili per migliorare le prestazioni fissati i comportamenti stessi.

6.3.2 Probabilità di falso allarme globale

Ora l'analisi viene condotta sulla probabilità di falso allarme globale, ancora una volta in un contesto dove il 20% dei nodi sono maliziosi. Per come è impostato il problema ci si aspettano ovviamente risultati analoghi a quelli ottenuti per i miss globali. Ciò è confermato in Figura 6.23 e 6.24, perciò ulteriori analisi vengono tralasciate. Nella prima figura è riportato il valore della probabilità di falso allarme globale al variare di m da 1 a 10, con $n = 10$ e $k = 0.2$. Nella seconda a variare è la probabilità che un nodo sia malizioso, con funzione di aggregazione del tipo 5-su-10 e $k = 0.2$. In entrambi i casi la banda è supposta costantemente libera.

Figura 6.23: Probabilità di falso allarme globale in funzione di m con nodi maliziosi, $n = 10$ e $k = 0.2$.

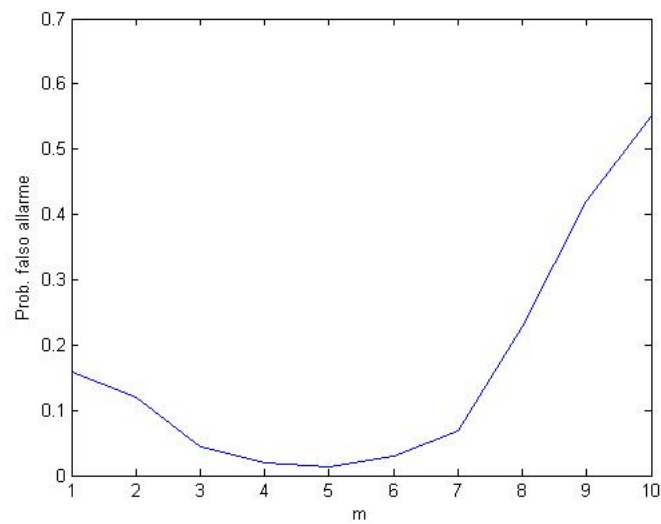


Figura 6.24: Probabilità di falso allarme globale in funzione della probabilità di nodo malizioso con $n = 10$, $m = 5$ e $k = 0.2$.

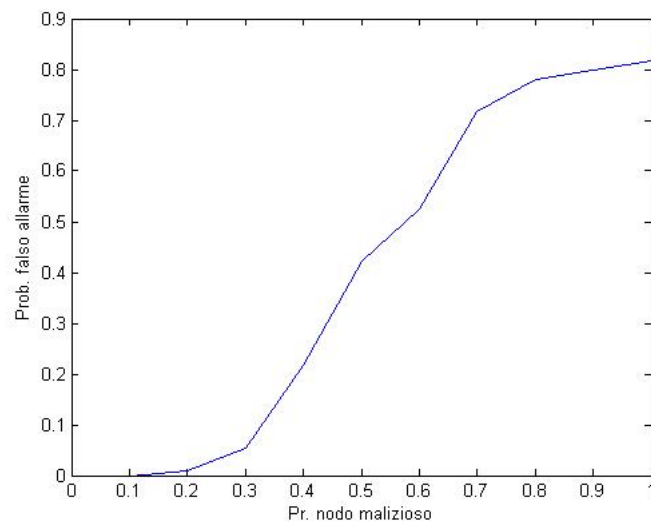
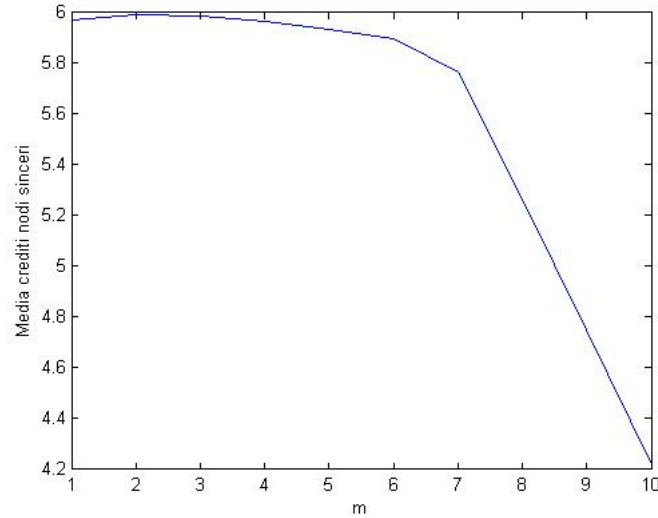


Figura 6.25: Media dei crediti residui dei nodi sinceri in funzione di m con nodi maliziosi, $n = 10$ e $k = 0$.



6.3.3 Crediti dei nodi

L'analisi si sposta ora sull'andamento dei crediti dei nodi, sia sinceri che maliziosi. Analogamente ai casi precedenti si inizia con lo studio delle variazioni dovute al valore di m che va da 1 a 10, con n fisso invece a 10, in un contesto dove il 20% dei nodi sono maliziosi. In Figura 6.25, 6.26 e 6.27 è riportato il valore medio dei crediti residui dei nodi sinceri, al termine dei 1000 passi di simulazione, con k rispettivamente pari a 0, 0.2 e 0.5. In Figura 6.28, 6.29 e 6.30 la stessa indagine è condotta per i nodi maliziosi.

Poichè ogni nodo ha inizialmente 5 crediti il risultato auspicabile è che al termine della simulazione i nodi sinceri abbiano mediamente un numero di crediti maggiore di 5 e quelli maliziosi un numero minore di 5. La prima condizione è verificata, per $k = 0$, se m non supera 8, mentre per valori di k maggiori sono tollerati valori di m anche più alti. Per verificare la seconda condizione con $k = 0$ sono invece necessari valori di m almeno pari a 3, e al crescere di k questa soglia minima decresce. Valori di m compresi tra 4 e 6, che già si sono rivelati ottimali per le prestazioni del sistema, si rivelano quindi ottimali anche per l'andamento dei crediti dei nodi.

Come già in precedenza, anche ora si fissa a 5-su-10 la funzione di pagamento, e si studia l'andamento dei crediti al variare della probabilità di nodo malizioso, che viene fatta andare da 0 a 1. In Figura 6.31, 6.32 e 6.33

Figura 6.26: Media dei crediti residui dei nodi sinceri in funzione di m con nodi maliziosi, $n = 10$ e $k = 0.2$.

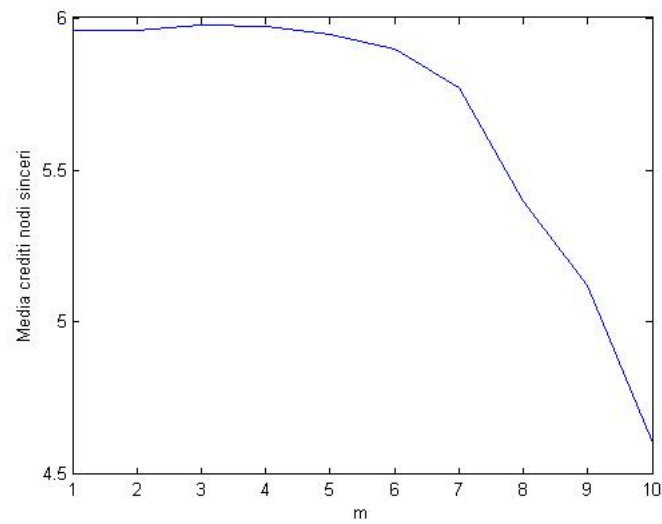


Figura 6.27: Media dei crediti residui dei nodi sinceri in funzione di m con nodi maliziosi, $n = 10$ e $k = 0.5$.

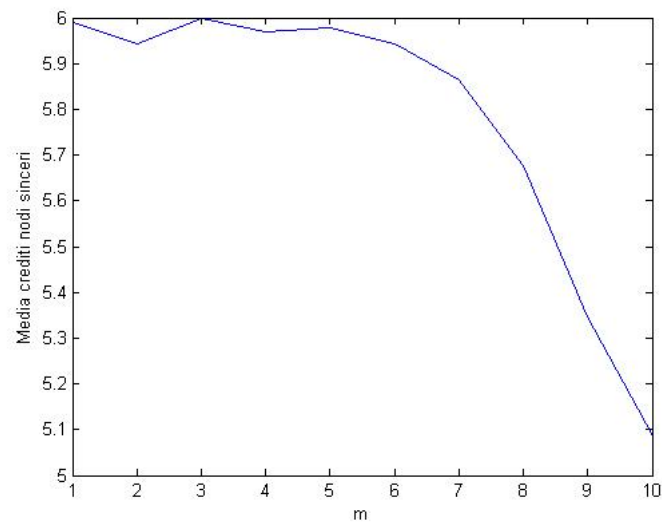


Figura 6.28: Media dei crediti residui dei nodi maliziosi in funzione di m con nodi maliziosi, $n = 10$ e $k = 0$.

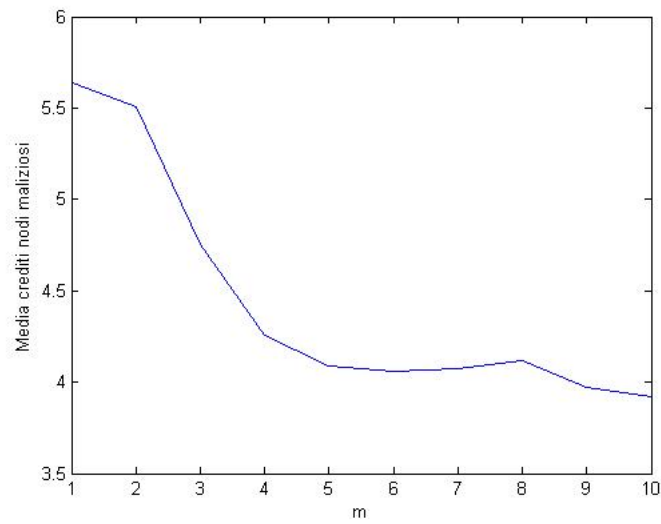


Figura 6.29: Media dei crediti residui dei nodi maliziosi in funzione di m con nodi maliziosi, $n = 10$ e $k = 0.2$.

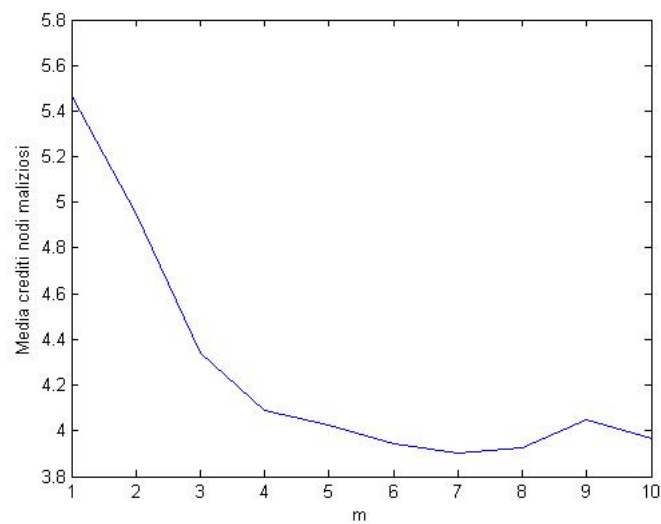
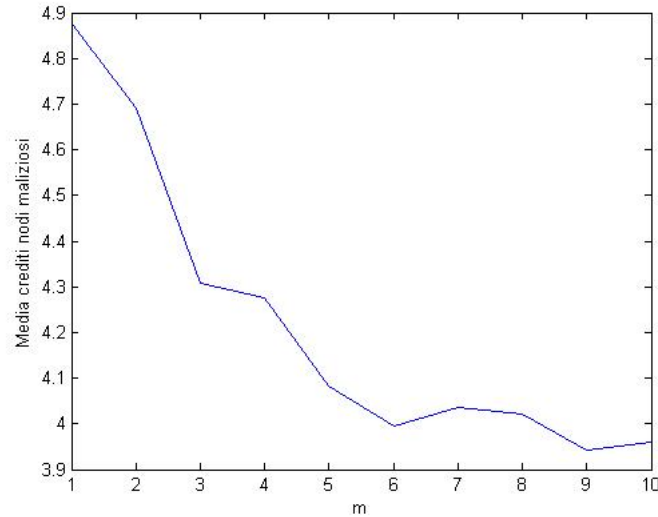


Figura 6.30: Media dei crediti residui dei nodi maliziosi in funzione di m con nodi maliziosi, $n = 10$ e $k = 0.5$.



è rappresentata la situazione dei nodi sinceri per k rispettivamente pari a 0, 0.2 e 0.5, mentre in Figura 6.34, 6.35 e 6.36 si analizzano alla stessa maniera i nodi maliziosi.

Anche in questo caso è auspicabile che, al termine della simulazione, i nodi sinceri abbiano mediamente un numero di crediti maggiore di 5, mentre quelli maliziosi un numero minore di 5. La prima condizione è verificata, in assenza di trusted report, in contesti in cui i nodi maliziosi sono meno del 50%, mentre per k pari a 0.5 è verificata anche se i nodi maliziosi sono la quasi totalità dei nodi della rete. Per verificare la seconda condizione senza usare i trusted report è invece necessario che i nodi maliziosi non superino il 40%, mentre con $k = 0.5$ la condizione è soddisfatta anche se essi sfiorano il 100%. In ogni caso da queste analisi non si è potuto apprezzare il vero valore dei trusted report in quanto in esse il comportamento dei nodi è statico. Infatti i nodi maliziosi cercano semplicemente di danneggiare il sistema e non reagiscono agli incentivi. I trusted report sono invece più utili con nodi egoisti, ossia nodi che vogliono esclusivamente massimizzare il proprio guadagno.

Figura 6.31: Media dei crediti residui dei nodi sinceri in funzione della probabilità di nodo malizioso con $n = 10$, $m = 5$ e $k = 0$.

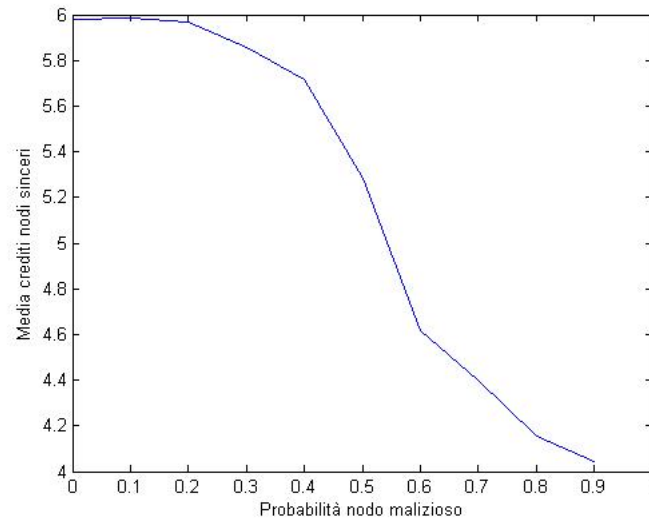


Figura 6.32: Media dei crediti residui dei nodi sinceri in funzione della probabilità di nodo malizioso con $n = 10$, $m = 5$ e $k = 0.2$.

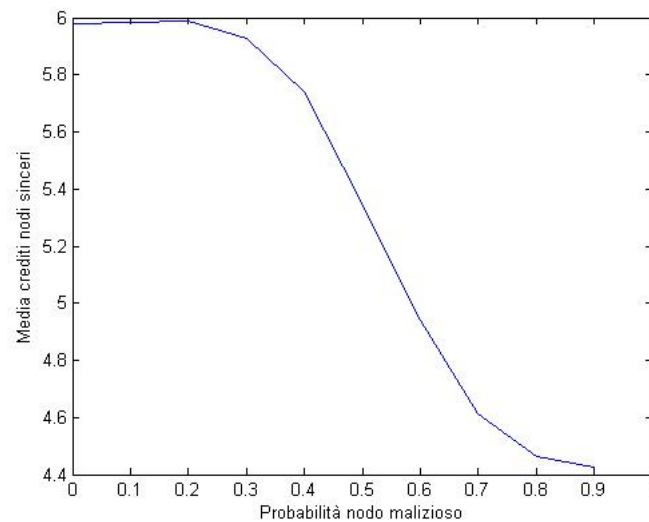


Figura 6.33: Media dei crediti residui dei nodi sinceri in funzione della probabilità di nodo malizioso con $n = 10$, $m = 5$ e $k = 0.5$.

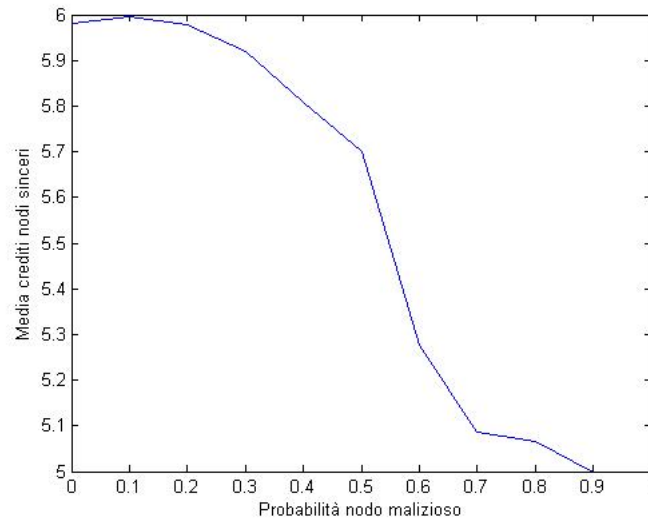


Figura 6.34: Media dei crediti residui dei nodi maliziosi in funzione della probabilità di nodo malizioso con $n = 10$, $m = 5$ e $k = 0$.

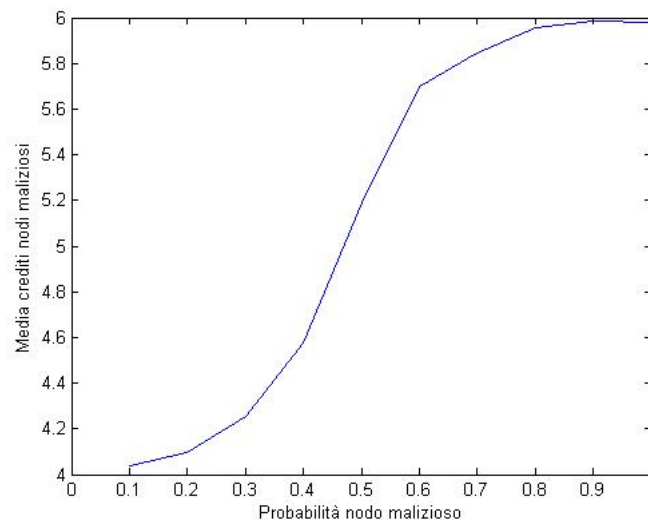


Figura 6.35: Media dei crediti residui dei nodi maliziosi in funzione della probabilità di nodo malizioso con $n = 10$, $m = 5$ e $k = 0.2$.

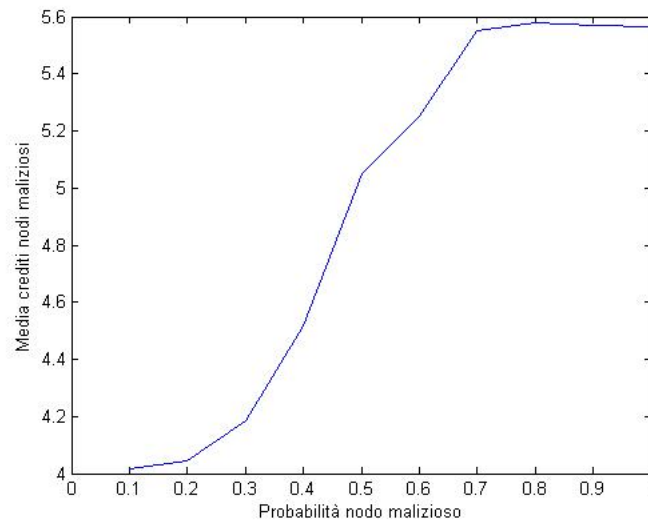


Figura 6.36: Media dei crediti residui dei nodi maliziosi in funzione della probabilità di nodo malizioso con $n = 10$, $m = 5$ e $k = 0.5$.

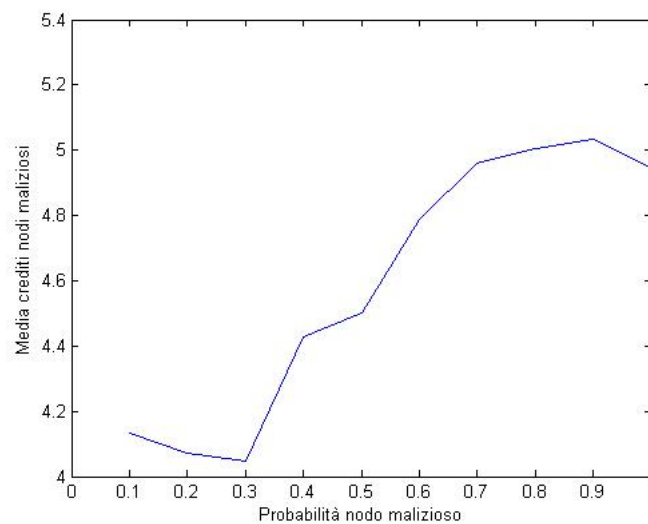
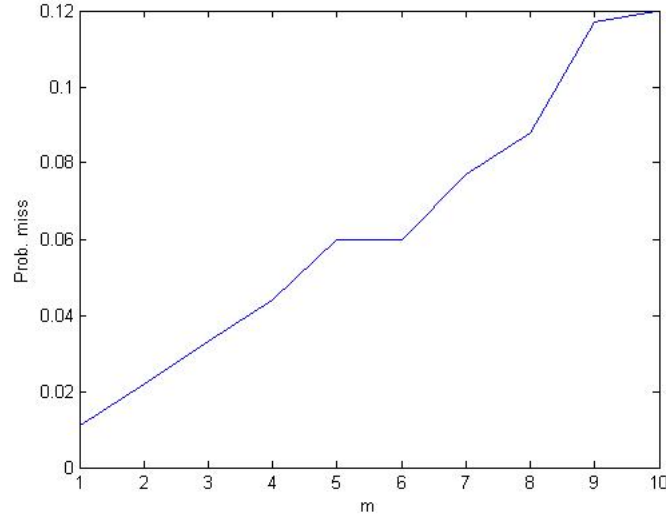


Figura 6.37: Probabilità di miss globale in funzione di m con randomizzazione ogni 20 passi e $n = 10$.



6.4 Studio degli effetti dei cambiamenti di stato della banda

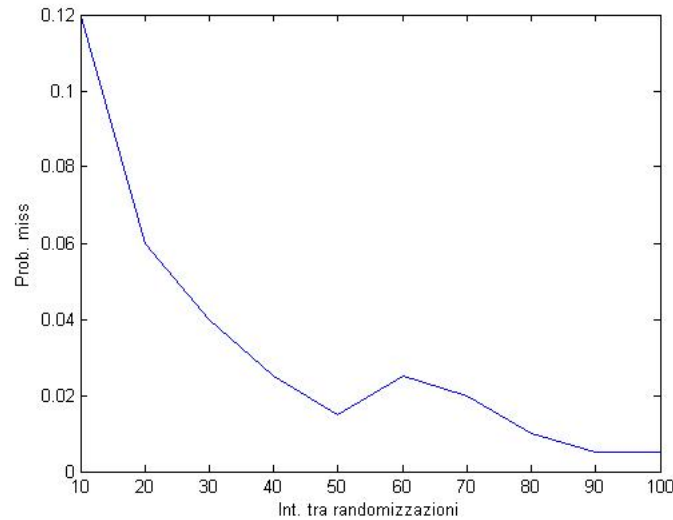
L'ultimo aspetto da prendere in considerazione è come i cambiamenti di stato della banda su cui si opera il sensing possano influenzare l'accuratezza dello stesso. Tale aspetto non è stato considerato nello studio degli equilibri di Nash del sistema ma si ricollega al concetto di correlazione tra segnali in istanti successivi presente nel modello di Jurca-Faltings. In questo contesto si suppone che i nodi siano tutti sinceri e che non ci sia il rischio di errori di sensing. Ancora una volta i trusted report sono stati disattivati, in quanto essi servono solo per scoraggiare comportamenti diversi da quello sincero.

6.4.1 Probabilità di miss globale

Il primo passo è determinare l'andamento della probabilità di miss globale al variare di m da 1 a 10 (con n sempre fisso a 10) in un contesto dove ogni 20 passi della simulazione lo stato della banda viene randomizzato, con $PL = PO = 0.5$. I risultati sono riportati in Figura 6.37.

A differenza di tutti gli altri casi ora al crescere di m le prestazioni del sistema decrescono fin da subito. Questo potrebbe portare a preferire, per

Figura 6.38: Probabilità di miss globale in funzione dell'intervallo tra le randomizzazioni dello stato della banda con $n = 10$ e $m = 5$.



prestazioni simili in merito a errori di sensing e presenza di nodi maliziosi, valori di m il più possibile bassi.

Assegnando a m ancora una volta il valore 5 e facendo variare l'intervallo tra le randomizzazioni della banda da 10 a 100 passi si ottiene, per la probabilità di miss globale, il grafico in Figura 6.38.

Cercando di ignorare le oscillazioni dovute alla casualità delle simulazioni dal grafico si può dedurre che, con una funzione di pagamento del tipo 5-su-10, le prestazioni del sistema si assestano su buoni valori solo se tra una randomizzazione e la successiva avvengono almeno 50 passi della simulazione. A questo punto è lecito domandarsi se funzioni di aggregazione in precedenza scartate perchè inferiori a livello di gestione di errori di sensing e nodi maliziosi possano rivelarsi invece buone in questo nuovo contesto. Per avere una risposta vengono proposti i grafici in Figura 6.39 e 6.40, costruiti con funzioni di pagamento rispettivamente del tipo a singolo rater e 2-su-5.

Le prestazioni migliori si raggiungono ora con il sistema a singolo rater mentre la funzione di aggregazione 2-su-5 offre comunque risultati migliori della funzione 5-su-10. Ciò significa che per fare sensing su bande il cui stato cambia in maniera relativamente veloce è bene cercare di abbassare, oltre che il valore di m , anche quello di n .

Figura 6.39: Probabilità di miss globale in funzione dell'intervallo tra le randomizzazioni dello stato della banda per singolo rater.

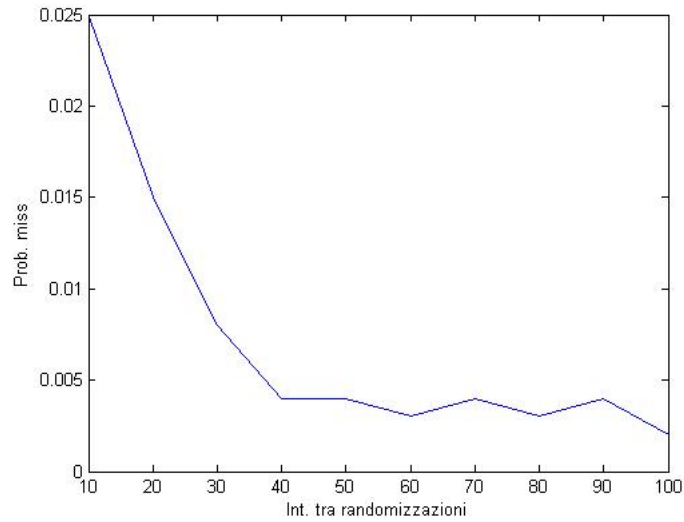


Figura 6.40: Probabilità di miss globale in funzione dell'intervallo tra le randomizzazioni dello stato della banda con $n = 5$ e $m = 2$.

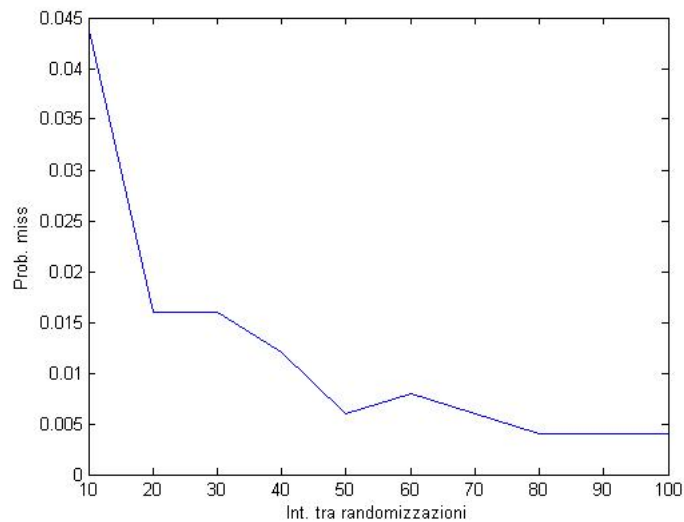
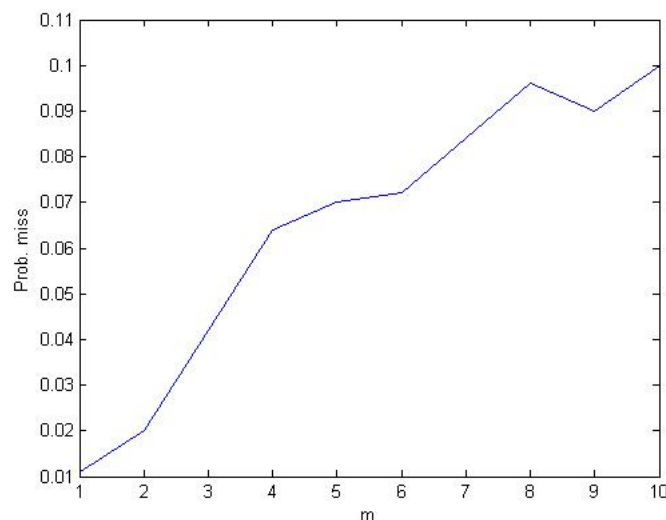


Figura 6.41: Probabilità di falso allarme globale in funzione di m con randomizzazione ogni 20 passi e $n = 10$.



6.4.2 Probabilità di falso allarme globale

Si passa ora allo studio dell'andamento della probabilità di falso allarme globale al variare della funzione di pagamento, sempre in un contesto dove ogni 20 passi della simulazione lo stato della banda viene randomizzato (con $PL = PO = 0.5$). m va da 1 a 10 mentre n , come sempre, è pari a 10. I risultati sono riportati in Figura 6.41, e si confermano analoghi a quelli incontrati nel caso della probabilità di miss. In Figura 6.42 a variare è invece l'intervallo tra le randomizzazioni dello stato della banda, mentre m viene fissato a 5. Lo studio di altre funzioni di aggregazione viene tralasciato per via delle analogie tra il caso dei falsi allarmi e quello dei miss.

6.4.3 Crediti dei nodi

L'ultima fase dell'analisi degli effetti sul sistema dei cambi di stato della banda prevede lo studio dell'andamento dei crediti residui dei nodi al termine delle simulazioni. Come al solito si inizia ponendo n a 10 e facendo variare m da 1 a 10, con randomizzazioni ($PL = PO = 0.5$) ogni 20 passi. Si ottiene così il grafico in Figura 6.43.

In questo caso il valore della media dei crediti dei nodi è sempre maggiore di 5 in quanto l'impatto dei cambiamenti di stato della banda sull'economia

Figura 6.42: Probabilità di falso allarme globale in funzione dell'intervallo tra le randomizzazioni dello stato della banda con $n = 10$ e $m = 5$.

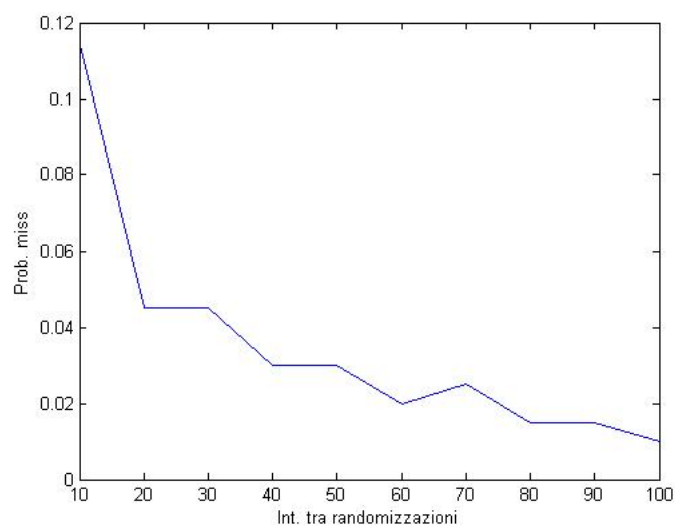


Figura 6.43: Media dei crediti residui dei nodi in funzione di m con randomizzazioni ogni 20 passi e $n = 10$.

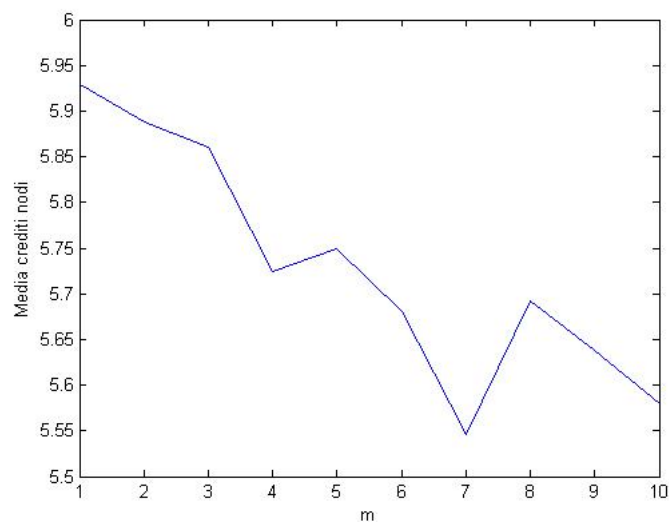
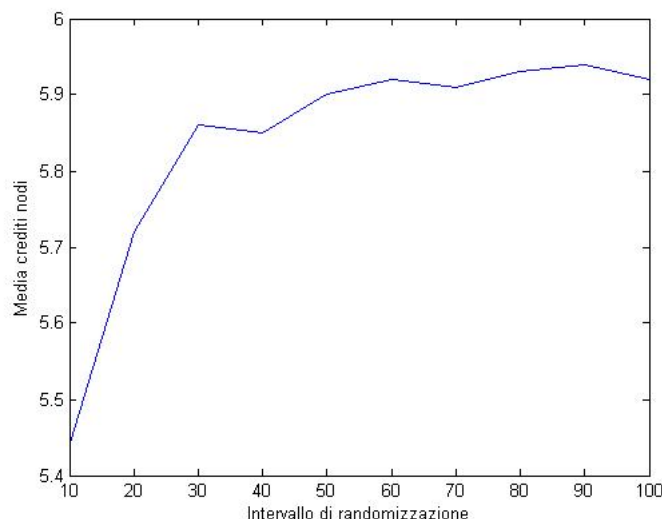


Figura 6.44: Media dei crediti residui dei nodi in funzione dell'intervallo tra le randomizzazioni dello stato della banda con $n = 10$ e $m = 5$.



del sistema non è molto forte, almeno per quanto riguarda l'intervallo considerato. In ogni caso tale valore cala, con grandi oscillazioni, al crescere di m .

L'analisi dell'andamento dei crediti residui dei nodi al termine delle simulazioni al variare da 10 a 100 dell'intervallo tra le randomizzazioni, con m fisso e pari a 5, produce invece il grafico in Figura 6.44.

Si può notare come non vi siano rischi di scendere sotto il valore di 5, tuttavia per intervalli di randomizzazione al di sotto dei 30 passi di simulazione la convenienza che hanno i nodi nel partecipare al sensing cala vistosamente. Come già fatto nel caso dell'andamento della probabilità di miss globale, anche ora vengono considerate altre due funzioni di pagamento, quella a singolo rater e quella del tipo 2-su-5. I risultati, nel medesimo contesto, sono presentati in Figura 6.45 e 6.46.

Gli andamenti dei due grafici sono simili a quello del grafico relativo alla funzione 5-su-10 ma ora l'entità del calo del valore dei crediti residui al diminuire dell'intervallo di randomizzazione è molto più piccolo, a causa del minor numero di miss e falsi allarmi generati da queste due funzioni.

Figura 6.45: Media dei crediti residui dei nodi in funzione dell'intervallo tra le randomizzazioni dello stato della banda per singolo rater.

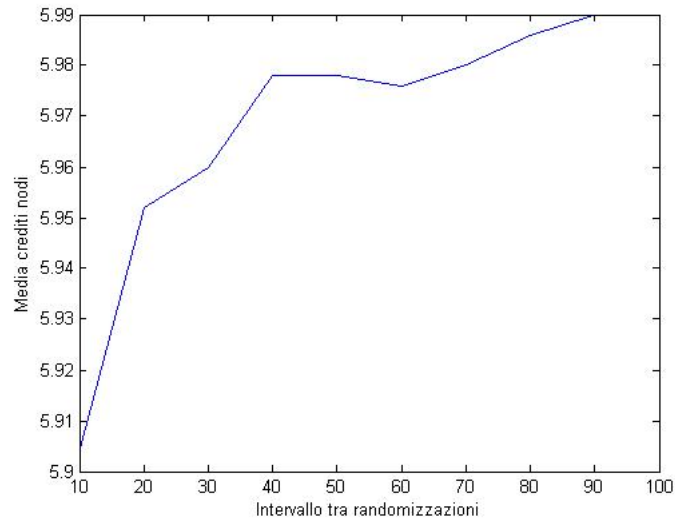


Figura 6.46: Media dei crediti residui dei nodi in funzione dell'intervallo tra le randomizzazioni dello stato della banda con $n = 5$ e $m = 2$.

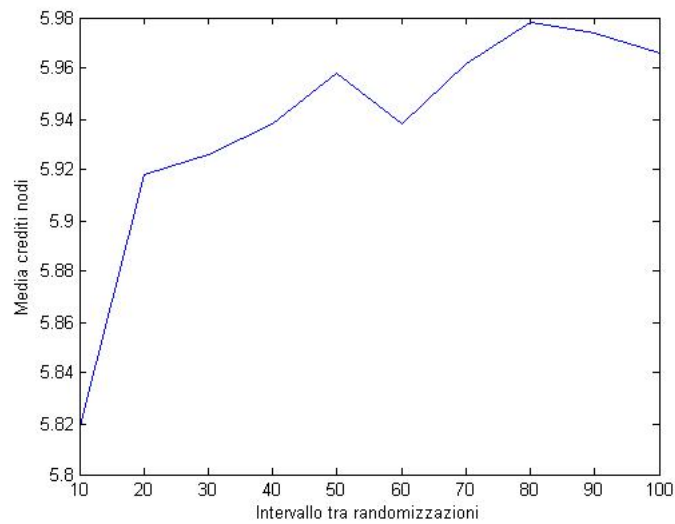


Figura 6.47: Valori dei parametri di una rete tipo.

Parametro	Valore
Pf	0.1
Pm	0.1
n	5
m	2
PL	0.5
PO	0.5
Int. di randomizzazione	20

6.5 Studio degli effetti dei nodi egoisti

Per comprendere meglio l'utilità dei trusted report è necessario considerare nodi egoisti, ossia nodi che cercano esclusivamente di massimizzare il proprio numero di crediti. Come si è visto da un punto di vista teorico tali nodi, se sufficientemente numerosi, tenderanno a formare una coalizione, ossia a riportare tutti lo stesso valore fisso come stato della banda su cui operano il sensing. Se invece i nodi egoisti non sono sufficientemente numerosi, o se i trusted report sono abbastanza frequenti, allora essi avranno convenienza a passare a un comportamento sincero.

Il progettista di una rete è difficile che disponga di informazioni relative a quanti dei nodi che vi si collegheranno saranno sinceri e quanti invece egoisti. Per questo motivo nel scegliere il valore di k sembra sensato partire dal presupposto che, nella peggiore delle ipotesi, i nodi egoisti costituiranno il 100% del totale. Sotto questa premessa si consideri una rete tipo, con le caratteristiche riportate in Tabella 6.47: si tratta di una combinazione di valori già incontrata e valutata come buona nelle sezioni precedenti. L'intervallo tra le randomizzazioni dello stato della banda è relativamente basso, quindi si è scelta una funzione di aggregazione piuttosto compatta, ma tuttavia in grado di gestire la non eccelsa precisione dei nodi.

Se i nodi sono tutti egoisti potrebbero accordarsi relativamente a un valore di coalizione e riportarlo sempre. In questa situazione, facendo variare da 0 a 1 la probabilità dei trusted report, si avrebbe un valore medio dei crediti residui per i nodi al termine della simulazione via via decrescente, come si può vedere in Figura 6.48. Se nella stessa rete, e sempre per k variabile da 0 a 1, i nodi si comportassero invece in modo sincero, l'andamento dei crediti sarebbe quello riportato in Figura 6.49.

Figura 6.48: Media dei crediti residui dei nodi coalizzati in funzione di k nella rete tipo.

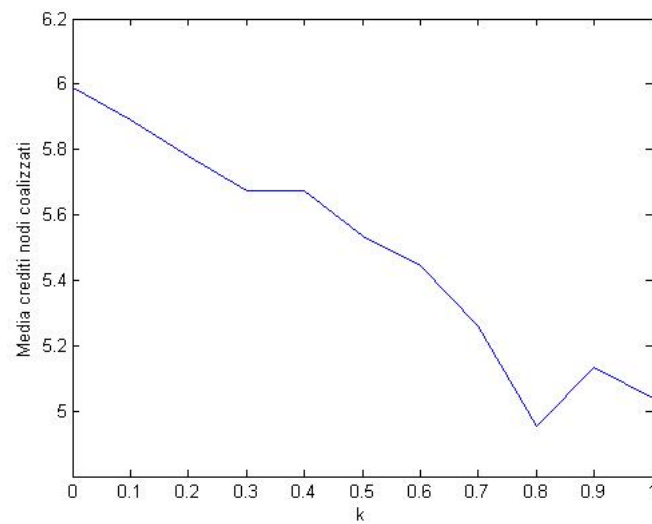


Figura 6.49: Media dei crediti residui dei nodi sinceri in funzione di k nella rete tipo.

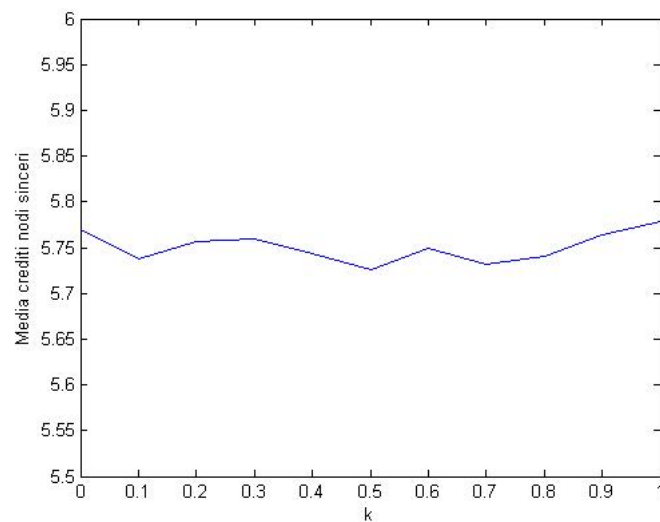
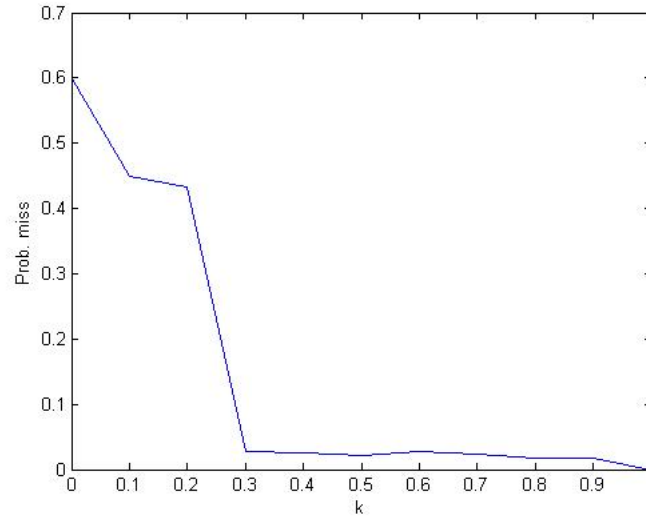


Figura 6.50: Probabilità di miss globale in funzione di k nella rete tipo con valore di coalizione 'banda libera'.



A partire da $k = 0.3$ si ha più convenienza a mantenere un comportamento sincero che a coalizzarsi, quindi nel simulare l'evoluzione di una rete composta esclusivamente da nodi egoisti è necessario prevedere che per valori di k minori di 0.3 i nodi scelgano di coalizzarsi mentre per valori maggiori di 0.3 preferiscano invece essere sinceri.

Il vero effetto dei trusted report su una rete di nodi egoisti è allora quello rappresentato in Figura 6.50, 6.51 e 6.52. Nel primo grafico viene rappresentato l'andamento, in funzione di k , della probabilità di miss globale, nel secondo quello della probabilità di falso allarme globale e nel terzo quello della media dei crediti residui dei nodi.

Come si può notare, il miglioramento delle prestazioni del sistema che si ha quando si raggiunge $k = 0.3$ è drammatico, con la probabilità di miss che crolla da più di 0.4 a meno di 0.03. La probabilità di falso allarme passa 0 a circa 0.025: questo perchè il valore che era stato scelto dalla coalizione era 'banda libera', quindi finchè i nodi erano coalizzati era impossibile che si verificasse un falso allarme. L'andamento dei crediti, infine, parte da un valore molto alto, tipico delle coalizioni in assenza di strumenti per contrastarle, e cala fino a che non si ha $k = 0.3$. A questo punto i nodi cambiano comportamento e lentamente, pur con visibili oscillazioni dovute alla casualità delle simulazioni, il valore dei loro crediti comincia a risalire al crescere

Figura 6.51: Probabilità di falso allarme globale in funzione di k nella rete tipo con valore di coalizione 'banda libera'.

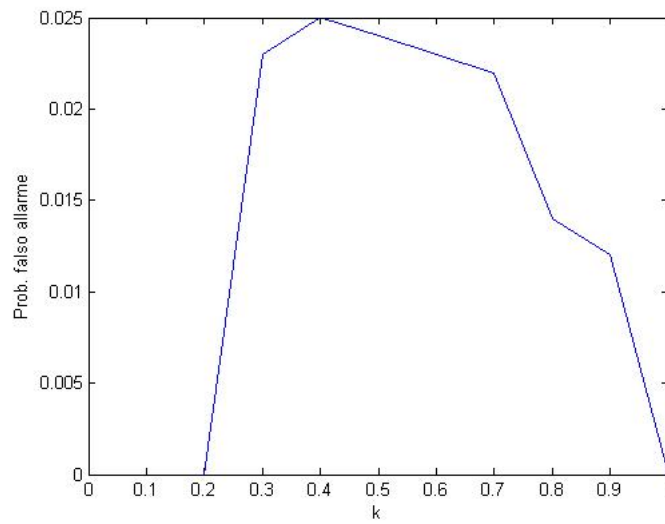


Figura 6.52: Media dei crediti residui dei nodi egoisti in funzione di k nella rete tipo.

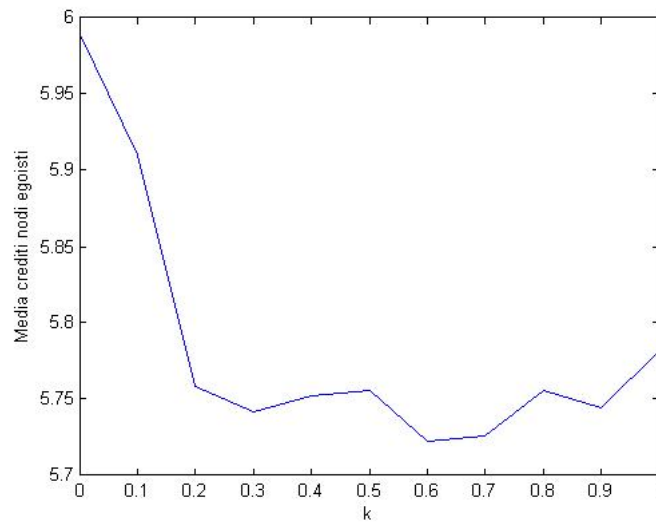
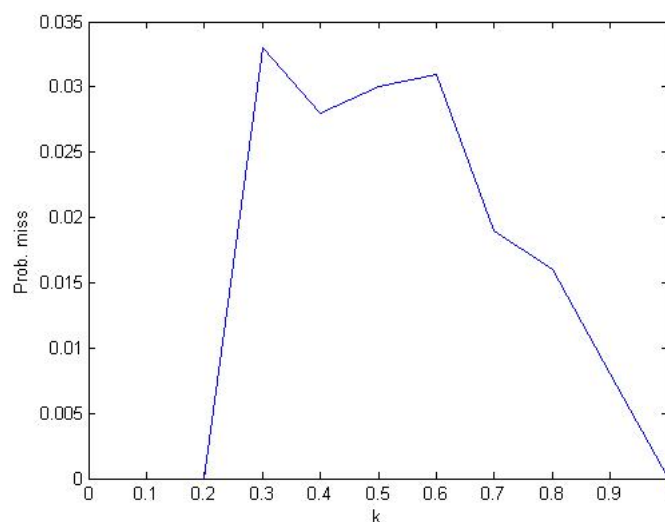


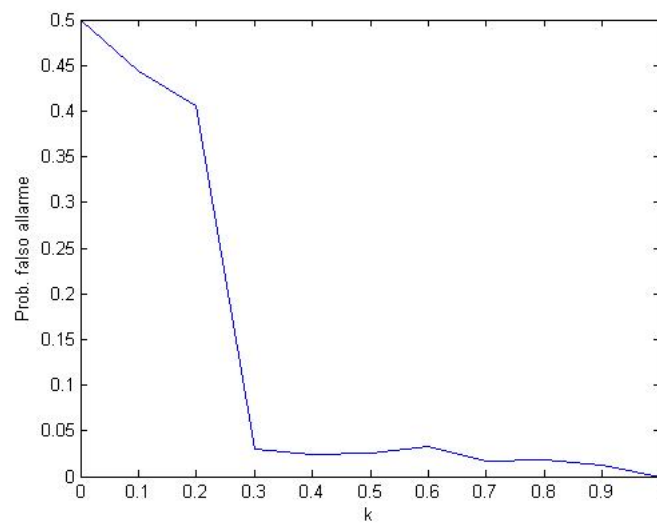
Figura 6.53: Probabilità di miss globale in funzione di k nella rete tipo con valore di coalizione 'banda occupata'.



di k . Per completezza vengono proposti anche i risultati che si otterrebbero se i nodi egoisti scegliessero di coalizzarsi sul valore 'banda occupata': essi sono riportati in Figura 6.53 e 6.54.

Un valore di k pari a 0.3 è un valore piuttosto alto, e garantirlo può essere costoso. Tuttavia in situazioni reali verosimilmente non tutti i nodi saranno egoisti, ed essi difficilmente avranno la possibilità di comunicare in modo semplice e veloce per potersi coalizzare su uno stesso valore. Per questi motivi nella pratica saranno sufficienti valori di k decisamente minori, e sarà necessario usarli solo per giungere all'equilibrio di Nash associato al comportamento sincero: una volta raggiunto, potranno essere disattivati.

Figura 6.54: Probabilità di falso allarme globale in funzione di k nella rete tipo con valore di coalizione 'banda occupata'.



Capitolo 7

Direzioni future di ricerca e conclusioni

7.1 Conclusioni

In questo lavoro si è quindi cercato di illustrare in che modo meccanismi a reputazione derivati dalla teoria dei giochi possano essere utili nel contesto dello spectrum sensing distribuito. Le normative giuridiche e le specifiche tecnologiche che dovranno regolamentare gli accessi opportunistici alle frequenze sotto licenza devono ancora essere definite [4] ma l'interesse che è cresciuto intorno a questi scenari lascia pensare che lo spectrum sensing possa rappresentare davvero una soluzione al problema della scarsità di frequenze disponibili. D'altra parte, i vantaggi che si avrebbero con la condivisione da parte degli utenti delle loro valutazioni sono evidenti [7] [6], quindi il passaggio a sistemi per lo spectrum sensing distribuito sembra immediato.

Come già nelle reti p2p, anche nello spectrum sensing distribuito saranno necessari meccanismi in grado di incentivare i membri della rete a collaborare. Questo obiettivo può essere raggiunto in diversi modi [21] [11] [3] [20]; l'approccio seguito in questo lavoro, come detto, consente di sfruttare gli strumenti forniti dalla teoria dei giochi per spingere gli utenti a tenere un certo comportamento. Ciò avviene imponendo, per mezzo di incentivi, l'equilibrio di Nash legato a tale comportamento. Inoltre tramite l'introduzione dei trusted report si possono scoraggiare le coalizioni, oltre che sfruttare in modo efficiente le informazioni certe fornite dai database che si pensa verranno allestiti [4].

E' stato anche mostrato come il modello presentato possa essere esteso o modificato per gestire situazioni differenti, a seconda della disponibilità o meno di un aggregatore dedicato o della presenza o meno di informazioni

sulla topografia della rete, sul livello di precisione dei singoli rilevatori e sul duty cycle della frequenza in esame. Infine è stata simulata l'evoluzione nel tempo di una rete per spectrum sensing virtuale, per confermare i risultati raggiunti a livello teorico. Nelle simulazioni relative alla presenza di errori nel sensing e di nodi maliziosi si è mostrato che con un'adeguata funzione di aggregazione il numero di miss e di falsi allarmi può essere quasi azzerato. Da altre analisi è poi emerso che anche per cambiamenti piuttosto frequenti dello stato della frequenza su cui si opera il sensing le prestazioni possono essere buone. Infine analizzando il comportamento di nodi egoisti è stato illustrato quali drammatici miglioramenti possa apportare l'introduzione dei trusted report.

7.2 Sviluppi futuri

Il lavoro presentato si presta a ulteriori sviluppi sia per quanto riguarda l'aspetto relativo alle tecnologie impiegate nello spectrum sensing sia per quanto riguarda quello relativo ai sistemi di reputazione basati sulla teoria dei giochi.

Sarebbe per esempio utile un'analisi più dettagliata delle normative e dei protocolli che dovranno regolare l'accesso opportunistico alle frequenze sotto licenza, e come tutto ciò si possa ripercuotere sulle tecnologie impiegate. Lo standard IEEE 802.22 [12] è stato solo accennato, e nessuna seria considerazione è stata fatta relativamente alla precisione che gli strumenti di sensing dovranno effettivamente raggiungere, o ai costi per avere informazioni certe dai database.

Un altro spunto interessante potrebbe riguardare le analisi in simulazione. Esse non prendono in considerazione diversi aspetti che sono invece fondamentali per arrivare ad avere i valori numerici dei parametri che offrono le prestazioni migliori. In primo luogo perchè gli essere umani non possono essere considerati completamente sinceri, egoisti o maliziosi, e nemmeno completamente razionali. Inoltre essi devono sottostare a una serie di limitazioni che non sono state riprodotte nelle simulazioni, per esempio il fatto che formare una coalizione richiede tempo, mezzi e impegno.

Infine si possono certamente ideare altre estensioni e modifiche per il modello, o provare a migliorare, implementare e testare quelle già proposte.

Bibliografia

- [1] Karl Aberer and Zoran Despotovic. On reputation in game theory application on online settings.
- [2] Roberto G. Cascella and Roberto Battiti. Social networking and game theory to foster cooperation.
- [3] Ruiliang Chen, Jung-Min Park, and Kaigui Bian. Robust distributed spectrum sensing in cognitive radio networks.
- [4] Federal Communication Commission, 2008. SECOND REPORT AND ORDER AND MEMORANDUM OPINION AND ORDER.
- [5] Enrico H. Gerding, Kate Larson, and Nicholas R. Jennings. Eliciting expert advice in service-oriented computing. *Artificial Intelligence*, 172.
- [6] Amir Ghasemi and Elvino S. Sousa. Opportunistic spectrum access in fading channels through collaborative sensing. *Journal of Communications*, 2(2), 2007.
- [7] Amir Ghasemi and Elvino S. Sousa. Spectrum sensing in cognitive radio networks: Requirements, challenges and design trade-offs. *IEEE Communications Magazine*, 2008.
- [8] Radu Jurca and Boi Faltings. An incentive compatible reputation mechanism.
- [9] Radu Jurca and Boi Faltings. Enforcing truthful strategies in incentive compatible reputation mechanisms. 2005.
- [10] Radu Jurca and Boi Faltings. Mechanisms for making crowds truthful. *Journal of Artificial Intelligence Research*, 34:209–253, 2009.
- [11] Praveen Kaligineedi, Majid Khabbazi, and Vijay K. Bhargava. Secure cooperative sensing techniques for cognitive radio systems. *IEEE Communications Society*, 2008.

-
- [12] Miguel Lopez-Benitez and Fernando Casadevall. Spectrum occupancy in realistic scenarios and duty cycle model for cognitive radio. *Advances in Electronics and Telecommunications*, 1(1), 2010.
- [13] George J. Mailath and Larry Samuelson. *Repeated Games and Reputations*. Oxford University Press, 2006.
- [14] N. Miller, P. Resnick, and R. Zeckhauser. Eliciting informative feedback: The peer-prediction method. 2005.
- [15] Petteri Nurmi. Bayesian game theory in practice: A framework for online reputation systems. 2005.
- [16] Yoav Shoham and Kevin Leyton-Brown. *MULTIAGENT SYSTEMS, Algorithmic, Game-Theoretic, and Logical Foundations*. Cambridge University Press, 2009.
- [17] Matthias Wellens and Petri Mahonen. Lessons learned from an extensive spectrum occupancy measurement campaign and a stochastic duty cycle model.
- [18] Matthias Wellens, Janne Riihijarvi, and Petri Mahonen. Empirical time and frequency domain models of spectrum use. *Physical Communication* 2, 10(32), 2009.
- [19] Matthias Wellens, Janne Riihijarvi, and Petri Mahonen. Modeling primary system activity in dynamic spectrum access networks by aggregated on/off-processes. *IEEE*, 2009.
- [20] Kun Zeng, Przemyslaw Pawelczak, and Danijela Cabric. Reputation-based cooperative spectrum sensing with trusted nodes assistance. *IEEE Communications Letters*, 14(3), 2010.
- [21] Tingting Zhao and Yuping Zhao. A new cooperative detection technique with malicious user suppression. *IEEE Communications Society*, 2009.
- [22] Aviv Zohar and Jeffrey S. Rosenschein. Mechanisms for information elicitation. *Artificial Intelligence*, 172, 2008.

Appendice A

Simulatore

Questo è il codice sorgente, scritto in *MATLAB*, del software che è stato utilizzato per simulare il comportamento della rete.

```
%simulazione di una rete che opera spectrum sensing
clear all

%parametri
%numero dei nodi
nodes=1000;
%funzione di aggregazione
k=0;
m=5;
n=10;
%crediti iniziali, crediti costo e crediti pagamento
start=5;
cost=1;
pay=2;
%probabilità di nodo malizioso
P_mal=0;
%probabilità nodo coalizzato e valore seguito dalla coalizione
P_col=0;
val_col=0;
%probabilità di nodo egoista e valore di k perchè sia sincero
P_sel=0;
k_min=0.5;
%precisione dei nodi
Pf=0.1;
```

```
Pm=0.1;
%valore di PL e intervallo tra le randomizzazioni dello stato
%della banda
PL=0.5;
int=50;
%passi della simulazione
t=1000;

%output
%probabilità di miss e falso allarme globale
p_miss=0;
p_f_alarm=0;
%valore medio dei crediti residui per nodi sinceri, maliziosi,
%coalizzati ed egoisti
avg_cr_tru=0;
avg_cr_mal=0;
avg_cr_col=0;
avg_cr_sel=0;

%setup
guard=0;
P_col=P_col+P_mal;
P_sel=P_sel+P_col;
behav=rand(1,nodes);
credits=ones(1,nodes).*start;
bs_to_check=zeros(1,n+1);
node_to_check=zeros(1,n+1);
val_to_check=zeros(1,n+1);
n_miss=0;
n_f_alarm=0;
cr_tru=0;
cr_mal=0;
cr_col=0;
cr_sel=0;
n_mal=0;
n_col=0;
n_sel=0;

%t passi di simulazione
for i=1:t
```

```
%ogni int passi si randomizza lo stato della banda
if mod(i,int)==1,
    if rand<PL,
        bs_act=0;
    else
        bs_act=1;
    end
end
%durante ogni passo un nodo random con almeno 1 credito fornisce
%una rilevazione
while guard==0
    node_act=round(rand*nodes);
    if node_act==0,
        node_act=nodes;
    end
    if credits(1,node_act)>0,
        guard=1;
    end
end
guard=0;
%se la banda è libera il nodo ha probabilità Pf di sbagliare
if bs_act==0,
    if rand<Pf,
        %se il livello di sincerità del nodo è sotto P_mal il nodo
        %comunicerà il contrario di ciò che vede
        if behav(1,node_act)<P_mal,
            val_act=0;
        %se è compreso tra P_mal e P_col comunicherà il valore di
        %coalizione
        elseif behav(1,node_act)<P_col,
            val_act=val_col;
        %se è compreso tra P_col e P_sel cercherà di massimizzare il
        %proprio guadagno
        elseif behav(1,node_act)<P_sel,
            if k>=k_min,
                val_act=1;
            else
                val_act=val_col;
            end
        %altrimenti sarà sincero
```

```
    else
        val_act=1;
    end
else
    if behav(1,node_act)<P_mal,
        val_act=1;
    elseif behav(1,node_act)<P_col,
        val_act=val_col;
    elseif behav(1,node_act)<P_sel,
        if k>=k_min,
            val_act=0;
        else
            val_act=val_col;
        end
    else
        val_act=0;
    end
end
end
%se la banda è occupata il nodo ha probabilità Pm di sbagliare
else
    if rand<Pm,
        if behav(1,node_act)<P_mal,
            val_act=1;
        elseif behav(1,node_act)<P_col,
            val_act=val_col;
        elseif behav(1,node_act)<P_sel,
            if k>=k_min,
                val_act=0;
            else
                val_act=val_col;
            end
        else
            val_act=0;
        end
    else
        if behav(1,node_act)<P_mal,
            val_act=0;
        elseif behav(1,node_act)<P_col,
            val_act=val_col;
        elseif behav(1,node_act)<P_sel,
```



```
        m_count=m_count+1;
    end
end
%e si confronta il loro numero con m
if m_count>=m,
    credits(1,node_to_check(1,n+1))=credits(1,node_to_check(1,n+1))+pay;
    %quindi si valuta se si è verificato un miss o un falso
    %allarme
    if val_to_check(1,n+1)==0,
        if bs_to_check(1,n+1)==1,
            n_miss=n_miss+1;
        end
    else
        if bs_to_check(1,n+1)==0,
            n_f_alarm=n_f_alarm+1;
        end
    end
else
    if val_to_check(1,n+1)==0,
        if bs_to_check(1,n+1)==0,
            n_f_alarm=n_f_alarm+1;
        end
    else
        if bs_to_check(1,n+1)==1,
            n_miss=n_miss+1;
        end
    end
end
end
end
end

%il numero di miss e falsi allarmi va normalizzato sui passi di
%simulazione
p_miss=n_miss/t;
p_f_alarm=n_f_alarm/t;

%infine si calcola il valore medio dei crediti residui per nodi
%sinceri, maliziosi, coalizzati ed egoisti
for i=1:nodes
```

```
if behav(1,i)<P_mal,
    cr_mal=cr_mal+credits(1,i);
    n_mal=n_mal+1;
elseif behav(1,i)<P_col,
    cr_col=cr_col+credits(1,i);
    n_col=n_col+1;
elseif behav(1,i)<P_sel,
    cr_sel=cr_sel+credits(1,i);
    n_sel=n_sel+1;
else
    cr_tru=cr_tru+credits(1,i);
end
end
avg_cr_mal=cr_mal/n_mal;
avg_cr_col=cr_col/n_col;
avg_cr_sel=cr_sel/n_sel;
avg_cr_tru=cr_tru/(nodes-n_mal-n_col-n_sel);
```