
UNIVERSITÀ DEGLI STUDI ROMA TRE

Dipartimento di Ingegneria

---

Corso Di Laurea Magistrale In

INGEGNERIA INFORMATICA

# PROGETTAZIONE E SVILUPPO DI TECNICHE DI DIFESA DA ATTACCHI DI SPECTRUM SENSING DATA FALSIFICATION (SSDF) BASATE SULLA REPUTAZIONE DI UTENTI SECONDARI IN RETI COGNITIVE

Tesi di Laurea di

PIETRO CORONAS

**Relatore**

FRANCESCO BENEDETTO

**Correlatore**

ANTONIO TEDESCHI

Anno Accademico 2014/2015

# Ringraziamenti

Desidero ringraziare il Professor Benedetto e il Dott. Tedeschi per la grande disponibilità e cortesia dimostratemi, e per tutto l'aiuto fornito nella realizzazione di questa tesi.
Un sentito ringraziamento alla mia ragazza Stefania, per essermi sempre stata vicino e avermi aiutato nei momenti di difficoltà. Il suo amore mi ha permesso di raggiungere questo traguardo.
Desidero inoltre ringraziare i miei amici della *Compagnia dello Stanzone*, per avermi dato supporto e amicizia nei momenti di difficoltà.
Un ultimo ringraziamento a mia madre Rita, a mio fratello Francesco e a tutta la mia famiglia per essermi stati vicino durante il mio percorso di studi.

# Indice

# INDICE DELLE FIGURE

# Introduzione

Lo sviluppo tecnologico dell'ultimo decennio ha portato ad un incremento dei sistemi di telecomunicazioni che si basano sul wireless, con conseguente saturazione dello spettro disponibile. Come confermano diverse misurazioni riguardo l'occupazione spettrale, l'assegnazione dello spettro da parte delle agenzie governative secondo un meccanismo di licenze ha portato ad un suo utilizzo non efficiente. La tecnologia emergente delle *Cognitive Radio* è considerata come una promettente soluzione alla scarsità dello spettro disponibile e al sottoutilizzo della risorsa spettrale assegnata. Una delle caratteristiche principali degli utenti cognitivi è la capacità di analizzare l'ambiente radio *(Spectrum Sensing)* per identificare le frequenze non utilizzate dall'utente licenziatario della banda, dette *White Space* o *Spectrum Hole*. Esistono molte tecniche di *Spectrum Sensing* definite in letteratura e tra esse *l'Energy Detector* è considerato una soluzione convenzionale, grazie alla sua semplicità di realizzazione e alla bassa complessità computazionale. Altri tipi di approccio analizzano i momenti di ordine superiore, le proprietà ciclostazionarie del segnale o le funzioni di autocorrelazione. Il limite di queste tecniche è l'alta complessità computazionale che richiedono. In aggiunta, potrebbe essere molto difficile ottenere una decisione affidabile riguardo l'occupazione spettrale quando i dispositivi cognitivi effettuano *Spectrum Sensing* in modo indipendente. Perciò, recenti approcci propongono una fase *di Sensing* tramite cooperazione tra dispositivi, in cui la decisione globale è ottenuta tramite combinazione delle decisioni locali di ogni dispositivo CR coinvolto nella comunicazione. Lo *Spectrum Sensing Cooperativo* (CSS) aumenta le performance di *Spectrum Sensing* e porta ad un migliore utilizzo dello spettro. Tuttavia a causa dell'apertura dei bassi strati dello stack protocollare, il CSS è vulnerabile ad attacchi di *Data Falsification* (SSDF). L'obiettivo di questi attacchi è danneggiare le performance e l'affidabilità del CSS attraverso la falsificazione dei dati di Spectrum Sensing locale. Per superare gli attacchi SSDF sono state proposte soluzioni basate sulla reputazione degli utenti, in modo da identificare gli attaccanti nel minor tempo possibile e limitare gli effetti dell'attacco sulla cooperazione.

Scopo di questa tesi è proporre un valido metodo di *Spectrum Sensing Cooperativo* basato sulla reputazione degli utenti, mostrandone l'efficacia e le performance tramite confronto con un metodo convenzionale. Il metodo proposto definisce la reputazione tramite tre liste in cui gli utenti si muovono dinamicamente. Gli utenti avranno un peso nella decisione globale in base alla lista di appartenenza. La particolarità del metodo è la sua capacità di distinguere gli attaccanti da utenti secondari che si trovano in una temporanea situazione non ottimale di *Spectrum Sensing*. La principale differenza tra il metodo convenzionale e quello proposto è che il primo, una volta escluso un utente, non permette un suo eventuale rientro nella comunicazione mentre quello proposto, grazie all'aggiornamento continuo della reputazione anche degli utenti esclusi, permette il rientro nella comunicazione degli utenti esclusi. Nel Capitolo 1 verranno definiti i concetti di *Software Defined Radio, Cognitive Radio* e le principali tecniche di *Spectrum Sensing*. Nel Capitolo 2 verrà fatta un'analisi sullo *Spectrum Sensing Cooperativo* tramite definizione delle sue caratteristiche principali, delle sue vulnerabilità e verranno inoltre definitivi i principali scenari operativi. Nel Capitolo 3 verranno descritti in dettaglio i metodi di *Cooperative Spectrum Sensing* convenzionale e quello proposto, oggetto di questa tesi. Verrà illustrato il modello di sistema, comune ai due metodi, e le tecniche di gestione della reputazione. Nel capitolo 4 verrà descritto il software che è stato sviluppato per la realizzazione delle simulazioni tramite diagrammi delle classi e modelli di dominio. L'obiettivo è la realizzazione di un prodotto software caratterizzato dalla facilità d'uso, dal gran numero di funzionalità e dalla facile modificabilità. Verrà inoltre descritto *Scrum*, il framework di sviluppo utilizzato per la realizzazione del software. Nel capitolo 5 i due metodi verranno confrontati in base a 3 parametri: la probabilità di identificazione dell'utente primario in funzione della variazione del rapporto segnale rumore, l'individuazione degli utenti malevoli presenti nella comunicazione e il numero di utenti leciti esclusi e, infine, la probabilità di identificazione dell'utente primario in base alla variazione della probabilità di falso allarme.