



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

INTRODUZIONE	1
CAPITOLO 1.....	3
1.1. SOFTWARE DEFINED RADIO	3
1.2. SOFTWARE DEFINED RADIO E COGNITIVE RADIO.....	4
1.3. DEFINIZIONE E CARATTERISTICHE DELLE COGNITIVE RADIO	5
1.3.1. Definizione	7
1.3.2. Attori e scenari operativi	8
1.3.3. Caratteristiche	9
1.3.4. Ciclo cognitivo.....	12
1.4. TECNICHE DI SPECTRUM SENSING.....	15
1.4.1. Energy Detector	15
1.4.2. Waveform-based Sensing.....	16
1.4.3. Matched Filtering.....	16
1.4.4. Cyclostationary-based Sensing.....	16
1.4.5. Radio Identification-based Sensing.....	16
1.5. TEMPERATURA DI INTERFERENZA	17
CAPITOLO 2.....	18
2.1. COOPERATIVE SPECTRUM SENSING	18
2.1.1. Elementi del Cooperative Spectrum Sensing.....	18
2.1.2. Tecniche di Cooperazione	20
2.1.3. Tecniche di Fusione nel CSS Centralizzato.....	21
2.1.4. Cooperative Spectrum Sensing con Trusted Node	23
2.2. SICUREZZA NEL COOPERATIVE SPECTRUM SENSING.....	24
2.2.1. Vulnerabilità Generali del CSS	24
2.2.2. Spectrum Sensing Data Falsification	26
CAPITOLO 3.....	30
3.1. MODELLO DI SISTEMA.....	30
3.2. ALGORITMO DI REPUTAZIONE CONVENZIONALE DI CSS	31
3.3. METODO PROPOSTO.....	33
3.3.1. Passaggio tra liste.....	35
3.4. POSSIBILE OTTIMIZZAZIONE DEL METODO PROPOSTO	36
3.4.1. Esempio di funzionamento del passaggio tra liste con parametri ottimizzati	37
3.5. SCENARIO DI COOPERATIVE SPECTRUM SENSING UTILIZZATO.....	38

CAPITOLO 4.....	40
4.1. SVILUPPO.....	40
4.1.1. <i>Scrum</i>	41
4.1.2. <i>Product Backlog</i>	41
4.2. FASI DEL PROGETTO.....	43
4.2.1. <i>Fase 1: Spectrum Sensing con Energy Detector</i>	44
4.2.2. <i>Fase 2: Metodi di Energy Detector</i>	47
4.2.3. <i>Fase 3: Cooperative Spectrum Sensing</i>	49
4.2.4. <i>Fase 4: Cooperative Spectrum Sensing Basato su Reputazione</i>	55
4.2.5. <i>Fase 5: Nuovo metodo di Cooperative Spectrum Sensing Basato su Reputazione</i>	56
4.2.6. <i>Fase 6: Cooperative Spectrum Sensing con Trusted Node</i>	58
4.2.7. <i>Fase 7: Funzioni di Utilità</i>	61
CAPITOLO 5.....	63
5.1. ELEMENTI DI MISURA DELLE PERFORMANCE	63
5.2. RISULTATI	64
5.2.1. <i>Scenario di CSS con il 3.3% di utenti malevoli</i>	65
5.2.2. <i>Scenario di CSS con il 6.6% di utenti malevoli</i>	71
5.2.3. <i>Scenario di CSS con il 10% di utenti malevoli</i>	77
CONCLUSIONI E SVILUPPI FUTURI.....	84
BIBLIOGRAFIA	86

INDICE DELLE FIGURE

FIGURA 1: ARCHITETTURA DI UN SDR IDEALE [1].....	4
FIGURA 2: OCCUPAZIONE SPETTRALE [1].....	6
FIGURA 3: METODI DI SPECTRUM SENSING [3].....	10
FIGURA 4: CICLO COGNITIVO SECONDO MITOLA III [4].....	13
FIGURA 5: PUNTI FONDAMENTALI DEL CICLO COGNITIVO	14
FIGURA 6: METODI DI IDENTIFICAZIONE A CONFRONTO [9].....	15
FIGURA 7: TEMPERATURA DI INTERFERENZA [1].....	17
FIGURA 8: ELEMENTI DEL COOPERATIVE SPECTRUM SENSING [11].....	19
FIGURA 9: COOPERATIVE SPECTRUM SENSING (A) CENTRALIZZATO (B) DISTRIBUITO (C) ASSISTITO [11]	21
FIGURA 10: TASSONOMIA DEI PARAMETRI DEL BYZANTINE ATTACK.....	26
FIGURA 11: MODELLI DI BYZANTINE ATTACK [15]	28
FIGURA 12: DECISIONE GLOBALE DEL METODO PROPOSTO DI CSS	35
FIGURA 13: DECISIONE GLOBALE DEL METODO PROPOSTO DI CSS CON TN.....	36
FIGURA 14: ESEMPIO DI FUNZIONAMENTO DELL'ALGORITMO PROPOSTO DI COOPERATIVE SPECTRUM SENSING. (A) ISTANTE INIZIALE, (B) ISTANTE K=0, (C) ISTANTE K=18, (D) ISTANTE K=22.....	37
FIGURA 15: MODELLO DI DOMINIO FASE 1.....	44
FIGURA 16: DIAGRAMMA DELLE CLASSI FASE 1.....	45
FIGURA 17: DIAGRAMMA DELLE CLASSI PER LA GENERAZIONE DEL GRAFICO	46
FIGURA 18: DIAGRAMMA DELLE CLASSI FASE 2.....	48
FIGURA 19: MODELLO DI DOMINIO FASE 3	50
FIGURA 20: DIAGRAMMA DELLE CLASSI FASE 3.....	51
FIGURA 21: MODELLO DI DOMINIO FASE 3.1	52
FIGURA 22: DIAGRAMMA DELLE CLASSI FASE 3.1	54
FIGURA 23: DIAGRAMMA DELLE CLASSI DEL FUSION CENTER.....	55
FIGURA 24: DIAGRAMMA DELLE CLASSI DEL FUSION CENTER CON L'INSERIMENTO DELLA REPUTAZIONE	56
FIGURA 25: DIAGRAMMA DI FLUSSO SUL FUNZIONAMENTO DEL METODO DI CSS PROPOSTO.....	57
FIGURA 26: DIAGRAMMA DELLE CLASSI FASE 6.....	60
FIGURA 27: DIAGRAMMA DELLE CLASSI DELLE FUNZIONI DI UTILITÀ.....	62
FIGURA 28: GRAFICO DELLA PROBABILITÀ DI IDENTIFICAZIONE DELL'UTENTE PRIMARIO IN FUNZIONE DELL'SNR. 3,3% DI UTENTI MALEVOLI ALWAYS FREE.....	65
FIGURA 29: GRAFICO DELLA PROBABILITÀ DI IDENTIFICAZIONE DELL'UTENTE PRIMARIO IN FUNZIONE DELL'SNR. 3,3% DI UTENTI MALEVOLI OPPOSITE	66
FIGURA 30: GRAFICO DELLA PROBABILITÀ DI IDENTIFICAZIONE DELL'UTENTE PRIMARIO IN FUNZIONE DELL'SNR. 3,3% DI UTENTI MALEVOLI SMART ALWAYS FALSE.....	66
FIGURA 31: UTENTI ESCLUSI CON 3,3% DI UTENTI MALEVOLI ALWAYS FREE	67

FIGURA 32: UTENTI ESCLUSI CON 3,3% DI UTENTI MALEVOLI OPPOSITE.....	68
FIGURA 33: UTENTI ESCLUSI CON 3,3% DI UTENTI MALEVOLI SMART ALWAYS FALSE.....	68
FIGURA 34: CURVE ROC CON IL 3,3% DI UTENTI MALEVOLI ALWAYS FREE.....	69
FIGURA 35: CURVE ROC CON IL 3,3 % DI UTENTI MALEVOLI OPPOSITE.....	70
FIGURA 36: CURVE ROC CON IL 3,3 % DI UTENTI MALEVOLI SMART ALWAYS FALSE.....	70
FIGURA 37: GRAFICO DELLA PROBABILITÀ DI IDENTIFICAZIONE DELL'UTENTE PRIMARIO IN FUNZIONE DELL'SNR. 6,6% DI UTENTI MALEVOLI ALWAYS FREE.....	71
FIGURA 38: GRAFICO DELLA PROBABILITÀ DI IDENTIFICAZIONE DELL'UTENTE PRIMARIO IN FUNZIONE DELL'SNR. 6,6% DI UTENTI MALEVOLI OPPOSITE.....	72
FIGURA 39: GRAFICO DELLA PROBABILITÀ DI IDENTIFICAZIONE DELL'UTENTE PRIMARIO IN FUNZIONE DELL'SNR. 6,6% DI UTENTI MALEVOLI SMART ALWAYS FALSE.....	72
FIGURA 40: UTENTI ESCLUSI CON 6,6% DI UTENTI MALEVOLI ALWAYS FREE	73
FIGURA 41: UTENTI ESCLUSI CON 6,6% DI UTENTI MALEVOLI OPPOSITE.....	74
FIGURA 42: UTENTI ESCLUSI CON 6,6% DI UTENTI MALEVOLI SMART ALWAYS FALSE.....	74
FIGURA 43: CURVE ROC CON IL 6,6% DI UTENTI MALEVOLI ALWAYS FREE.....	75
FIGURA 44: CURVE ROC CON IL 6,6 % DI UTENTI MALEVOLI OPPOSITE.....	75
FIGURA 45: CURVE ROC CON IL 6,6 % DI UTENTI MALEVOLI SMART ALWAYS FALSE.....	76
FIGURA 46: GRAFICO DELLA PROBABILITÀ DI IDENTIFICAZIONE DELL'UTENTE PRIMARIO IN FUNZIONE DELL'SNR. 10% DI UTENTI MALEVOLI ALWAYS FREE.....	77
FIGURA 47: GRAFICO DELLA PROBABILITÀ DI IDENTIFICAZIONE DELL'UTENTE PRIMARIO IN FUNZIONE DELL'SNR. 10% DI UTENTI MALEVOLI OPPOSITE	78
FIGURA 48: GRAFICO DELLA PROBABILITÀ DI IDENTIFICAZIONE DELL'UTENTE PRIMARIO IN FUNZIONE DELL'SNR. 10% DI UTENTI MALEVOLI SMART ALWAYS FALSE.....	78
FIGURA 49: UTENTI ESCLUSI CON 10% DI UTENTI MALEVOLI ALWAYS FREE.....	79
FIGURA 50: UTENTI ESCLUSI CON 10% DI UTENTI MALEVOLI OPPOSITE.....	80
FIGURA 51: UTENTI ESCLUSI CON 10% DI UTENTI MALEVOLI SMART ALWAYS FALSE.....	80
FIGURA 52: CURVE ROC CON IL 10% DI UTENTI MALEVOLI ALWAYS FREE	81
FIGURA 53: CURVE ROC CON IL 10 % DI UTENTI MALEVOLI OPPOSITE.....	82
FIGURA 54: CURVE ROC CON IL 10 % DI UTENTI MALEVOLI SMART ALWAYS FALSE.....	82

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.