SDA-COG – Sistema de Detecção de Ataques para Rede de Rádios Cognitivos*

Joffre Gavinho Filho[1], Luiz F. R. C. Carmo[2], Raphael C. S. Machado[2], Luci Pirmez[1]

[1]NCE/IM Universidade Federal do Rio de Janeiro (UFRJ) – Rio e Janeiro, RJ – Brasil

[2]Instituto Nacional de Metrologia (INMETRO) – Duque de Caxias, RJ - Brasil

{joffreufrj,luci.pirmez}@gmail.comr, {rust,rmachado}@inmetro.gov.br

Abstract. *This paper deals with the development of an Attack Detection System (ADS) for Cognitive Radio Networks (CRN) formed by combining two classic intrusion detection mechanisms: location and reputation. The proposal was evaluated by means of simulations of specific CRNs attacks: Primary User Emulation (PUE) and Sense Spectrum False Feedback (SSFF).*

Resumo. *Este trabalho descreve um Sistema de Detecção de Ataques (SDA) para redes de rádios cognitivos a partir da integração dos métodos de detecção por Localização e por Reputação. O sistema é validado através de simulações que avaliam o desempenho do mesmo face aos ataques específicos de emulação do usuário primário (Primary User Emulation - PUE) e falso diagnóstico do sensoriamento do espectro (Sense Spectrum False Feedback - SSFF).*

1. Introdução

A utilização do espectro de freqüência na área de comunicações sem-fio é concedida em seu direito de uso por meio de uma licença (denominada de concessão), fornecida pelos órgãos governamentais responsáveis pela regulamentação e fiscalização das comunicações [Inatel 2009]. O modelo de alocação de bandas do espectro de freqüência no Brasil permite os seguintes tipos de concessões: (i) *Licenciado exclusivo* - direito de uso exclusivo da banda ou canal assegurado por um órgão fiscalizador do espectro por um período pré-determinado, sujeito às limitações da licença; (ii) *Licenciado não exclusivo* - utiliza partes do espectro de frequência onde são concedidas licenças para mais de um usuário, nenhuma entidade tem o controle total desta parte do espectro; e (iii) *Não-licenciado* - utiliza o espectro de frequência sem a necessidade de se obter uma licença e não há um único usuário com direito de uso exclusivo. Medições do espectro de frequência [McHenry 2003] demonstram que a política de alocação estática do espectro é imprópria para o atual cenário de comunicações em redes sem-fio. De acordo com o relatório do FCC (Federal Communications Commission), que é o órgão responsável pelas comunicações nos Estados Unidos [Fcc 2003], a maioria das bandas de espectro atribuídas (bandas licenciadas) não é usada em certos períodos de tempo e/ou em determinadas áreas geográficas, ocasionando o denominado "espaço em branco" (*white space*). Em contrapartida, as bandas de frequências não licenciadas encontram-se saturadas em virtude de sua maciça utilização. Uma forma eficiente para resolver a contradição entre as faixas licenciadas subutilizadas e a disponibilidade limitada em bandas não licenciadas é permitir que os usuários não licenciados (Usuários Secundários - US) acessem dinamicamente as bandas licenciadas, desde que não provoquem a interferência com os proprietários das faixas licenciadas (Usuários Primários - UP).

Nesse contexto, o Rádio Cognitivo (RC) [Mitola III 2009] se apresenta como uma tecnologia promissora que permite o uso dinâmico do espectro de rádio freqüência [Akyildiz 2006a]. Em uma rede formada por RCs, os dispositivos são equipados com rádios

*Artigo financiado com recursos da MCT/FINEP PLATCOG (01.10.0549.00).

que possuem flexibilidade no uso do espectro, com capacidade de detecção de bandas disponíveis, reconfiguração da frequência do rádio e de trocas entre as bandas selecionadas [Akyildiz 2006a], [Akyildiz 2006b] e [Thomas 2005]. Com base nas informações de sensoriamento do espectro, os usuários de rádio acessam as bandas licenciadas oportunisticamente quando nenhum usuário primário as estiver utilizando e, necessariamente, devem deixá-las imediatamente ao detectar a atividade do Usuário Primário (UP). Os Rádios Cognitivos podem ser formalmente definidos como dispositivos de comunicação inteligentes e adaptativos capazes de modificar seus parâmetros de transmissão – tais como: frequência de operação, tipo de modulação, potência de transmissão, protocolos de comunicações e outros – baseados em interações com o ambiente em que operam [Mitola 2000].

O Rádio Cognitivo (RC) é uma nova abordagem de acesso ao espectro de radiofreqüência que visa otimizar o uso deste recurso de forma oportunística. Para suportar tais capacidades, o RC possui, basicamente, quatro funcionalidades que gerenciam todas as suas atividades operacionais referentes à utilização do espectro [Akyildiz 2008]: (i) Sensoriamento do Espectro, (ii) Gerenciamento do Espectro, (iii) Mobilidade Espectral e (iv) Compartilhamento do Espectro. O Sensoriamento do Espectro é a funcionalidade responsável por monitorar o espectro e determinar quais são os canais licenciados que estão disponíveis, i.e. quais são os canais que não estão sendo utilizados pelo usuário primário. O Gerenciamento do Espectro de um RC é responsável por selecionar qual o canal licenciado livre mais apropriado para a transmissão de acordo com os seus requisitos de QoS (*Quality of Service*). A Mobilidade Espectral é responsável por desocupar o canal licenciado quando a presença do usuário primário é detectada, i.e. quando o usuário principal começar a utilizar o canal licenciado. Por fim, o Compartilhamento do Espectro é a funcionalidade que permite à rede de rádios cognitivos de utilizar os canais licenciados livres de forma cooperativa e colaborativa entre os rádios da rede.

Entre os vários desafios a serem abordados encontramos o que está relacionado ao provimento de segurança às redes de rádios cognitivos, uma vez que os equipamentos utilizados podem ser vítimas de ações que os impeçam de se comunicar efetivamente.

Entre as novas características operacionais utilizadas pela tecnologia do RC para a efetiva comunicação, encontramos a necessidade do constante monitoramento do meio para que o rádio possa: perceber as frequências licenciadas que não estão em uso; decidir qual freqüência licenciada livre utilizar; e adaptar-se às condições reais de transmissões oportunísticas nas freqüências licenciadas. Todavia, tal característica o torna vulnerável a tipos específicos e novos de ataques não observados nas redes convencionais.

De uma forma geral, o uso inadequado das freqüências licenciadas livres (FLL) pode ser configurado como um tipo de ataque [Leon 2010] às Redes de Rádios Cognitivos (RRC). Tais ações podem degradar de forma parcial ou total o funcionamento da rede cognitiva, ocasionando o não aproveitamento da capacidade oportunística de utilização das faixas licenciadas livres por parte da rede.

Este trabalho visa o desenvolvimento de um sistema de detecção de ataques para a identificação de rádios que estejam promovendo a inadequada utilização das freqüências licenciadas livres em uma RRC. Para isso, buscamos: (i) identificar os principais tipos de ataques aos quais estas redes estão sujeitas, (ii) selecionar os mecanismos de detecção mais adequados a estes tipos de ataques, e (iii) integrá-los de forma a alcançar os melhores índices possíveis de detecção.

Este artigo está organizado da seguinte forma: na Seção 2 são descritos os aspectos de segurança bem como os trabalhos relacionados; na Seção 3 a proposta do Sistema de

Detecção de Ataques é apresentada; na Seção 4 são descritos os experimentos realizados; na Seção 5 é feita uma análise dos resultados obtidos; e finalmente, na Seção 6 são tecidas as conclusões finais e as propostas de trabalhos futuros.

2. Aspectos de Segurança e Trabalhos Relacionados

Quando se fala de segurança em Rádios Cognitivos, automaticamente são associados dois novos tipos de ataques específicos: a emulação do usuário primário (*Primary User Emmulation* – PUE) e a adulteração das tabelas de Frequencia Licenciada Livre (FLL) (*Spectrum Sense False Feadback.*- SSFF).

PUE

No caso do PUE um ou mais Rádios Cognitivos modificam as suas características de transmissão, adaptando-as a forma utilizada pelo usuário primário, e induzem aos outros rádios da Rede de Rádios Cognitivos de que estas frequências livres já estejam em uso. Caso o ataque seja utilizado por pares de rádios para monopolização das freqüências livres, este é denominado de PUE-S (*Primary User Emmulation – Selfish*). Caso a finalidade seja impedir que nenhum rádio utilize as frequências livres, este é definido como PUE-M (*Primary User Emmulation – Malicious*). O mecanismo de localização dos rádios na rede possibilita a determinação do posicionamento geográfico dos rádios. Este mecanismo associado aos níveis de potência de transmissão de cada um dos rádios identifica se o rádio em análise é um usuário principal (torre de transmissão da frequência licenciada), ou um usuário secundário (rádio cognitivo componente da rede). Para a determinação da localização dos transmissores são feitas as seguintes suposições: (i) os transmissores primários são torres com uma posição conhecida e fixa, além de possuir altíssimo poder de transmissão (na escala das centenas de *KiloWatts* - kW); e (ii) o CR é um dispositivo com o poder limitado de transmissão (que varia dos *miliwatts* – mW a alguns watts - W). Diversas abordagens foram apresentadas no contexto de segurança da RRC [Clancy 2008], [Clancy 2009], [Leon 2010], que utilizam como método de detecção de ataque PUE a utilização da localização dos rádios secundários e do usuário primário. Por exemplo, [Shrestha 2010] propõe um método de detecção de PUE, baseado no cálculo Euclidiano do posicionamento dos rádios da rede, bem como da torre de transmissão. A proposta baseia-se no conhecimento prévio do posicionamento e da potência de transmissão de todos os rádios cognitivos da rede, como também do usuário primário. Porém o trabalho define sua hipótese de detecção em um cenário cooperativo, onde os rádios primários transmitem informações de controle, entre elas: posicionamento, potência de transmissão, etc.; contrariando as normas do [Fcc 2009], de que nenhuma alteração na infraestrutura e nas configurações das redes primárias deve ser feita com a finalidade de adaptar-se a nova tecnologia de rádio cognitivo. A proposta de [Park 2008] diferencia-se de sobremaneira das propostas supracitadas porque, além da análise para a decisão de detecção do ataque ser baseada também no comportamento dos rádios da rede, não há a necessidade de qualquer informação fornecida pelo usuário primário.

SSFF

Nas redes onde ocorre o monitoramento do espectro de forma colaborativa, a ocupação das freqüências licenciadas livres é baseada nas informações trocadas entre os rádios (tabelas de frequências livres - FLL) sobre quais frequências estão livres ou não. Através da adulteração dessas tabelas, é possível forjar que uma dada freqüência livre esteja ocupada, ou vice-versa, o que configura um ataque do tipo SSFF. Se este procedimento é empregado para que as frequências não sejam compartilhadas, ficando o seu uso exclusivo para um único usuário, denomina-se de ataque SSFF no modo egoísta *(selfish)*. Se uma frequência é declarada livre (resp. ocupada) quando estiver ocupada (resp. livre) apenas para impedir a

sua utilização, configura-se um ataque SSFF de modo *DoS (denial of service).* A generalização SSFF quanto a qualquer falsificação de informações do sensoriamento do espectro pode ainda ser especificada em três tipos distintos de ataques: (*i*) sempre-livre (SSFF-SL): sempre transmite a informação de que o canal licenciado está livre, (*ii*) sempre-ocupado (SSFF-SO): sempre transmite a informação de que o canal licenciado está ocupado, e (*iii*) sempre-falso (SSFF-SF): onde o rádio malicioso sempre transmite o inverso da realidade do canal, isto é, livre quando ocupado e ocupado quando livre. O ataque SSFF foi mencionado primeiramente em [Misha 2006] e, adicionalmente, por [Ruiliang 2008a] e [Ruiliang 2008b]. Em [Ruiliang 2008b] a detecção dos dados falsificados foi realizada utilizando-se um esquema matemático baseado na relação sequencial de probabilidade, esquema esse com bons resultados. Entretanto este método exige o conhecimento prévio da posição física de todos os elementos constituintes da rede. A proposta de [Zhu 2009] faz uso de um mecanismo de reputação para definir um grau de credibilidade às informações sobre as tabelas de freqüências livres recebidas dos rádios da rede. O uso da reputação atribui um grau de aceitação a um rádio da rede para desempenhar uma tarefa sem que necessariamente o rádio requisitante tenha interagido com o rádio alvo anteriormente. Para tanto, utiliza-se as experiências dos demais rádios da Rede.

Apesar de os mecanismos: de localização [Park 2007] e o de reputação [Zhu 2009] serem completamente independentes, há situações em que a utilização dos dois mecanismos em conjunto (de forma complementar) pode aumentar a eficiência da detecção de ataques. Por exemplo, um ataque de PUE, que normalmente é detectado pelo mecanismo de localização com base na análise das potências de transmissões captadas, pode não ser detectado dependendo do posicionamento geográfico da rede. Quando um rádio está localizado no limite de alcance da transmissão do UP, i.e. onde a potência de recepção captada pelo rádio da transmissão do UP é muito baixa, a análise do mecanismo pode ser inviabilizada, já que a distinção entre uma transmissão de um UP de uma transmissão de outro rádio da rede não é facilmente reconhecida. Porém, com a utilização dos dois mecanismos em conjunto, mesmo que o mecanismo de localização, em virtude do posicionamento geográfico da rede, não consiga inferir sobre algum ataque de PUE, o mecanismo de reputação o possibilitará. Visto que, o uso indevido de uma frequência licenciada livre (FLL) por um atacante PUE induzirá aos rádios ao seu alcance de transmissão que não há canais livres e, por conseqüência, tais rádios disseminarão suas tabelas de freqüências indicando que tais canais estão ocupados pelo Usuário Primário (UP). Porém, todos os rádios que estiverem ao alcance dos rádios atacados e fora do alcance do atacante PUE (e que evidentemente não são por estes influenciados quanto à ocupação da FLL) não detectam transmissões do UP e, por conseqüência, identificam ataques de SSFF daquela região da rede onde o atacante PUE está localizado. A retroalimentação de informações confiáveis de ataques (aferidas e validadas através dos mecanismos de reputação) indica aos rádios atacados que há uma transmissão indevida realizada por um rádio localizado dentro dos seus raios de transmissão.

Logo, esse trabalho propõe um SDA baseado no uso conjunto e adaptado de métodos de localização e de reputação. Tal escolha procura: (i) melhorar a eficiência na detecção de ataques de PUE, mesmo em situações onde o mecanismo de localização não possa inferir sobre o ataque, e (ii) agrupar em um único SDA a detecção de ataques dos tipos PUE e SSFF.

3. Proposta de SDA

O sistema de detecção de ataques descrito neste trabalho é composto, basicamente, por um mecanismo de localização integrado a um mecanismo de reputação.

3.1 Mecanismo de localização

O mecanismo de localização empregado consiste de uma variante da proposta de [Park 2008], adaptada para o ambiente urbano, uma vez que o modelo estatístico original é destinado para áreas rurais. Tal modelo foi substituído pelo proposto em [Hata 1980], para contextualizar o cenário de grandes cidades (área urbana) e com frequências acima de 400 MHz. Cenário esse onde encontrarmos as maiores concentrações de equipamentos que fazem uso das faixas de frequências não-licenciadas, causando, em virtude disso, uma maior escassez espectral, sendo então áreas propícias à utilização de redes de rádios cognitivos. O modelo [Hata 1980] para áreas urbanas é descrito como:

$$\Pr = \frac{Pt * Gr * Gt}{L} \tag{1}$$

$$L = 69{,}55 + 26{,}16\ell og(f_{MHz}) - 13{,}82\ell og(h_{Tef}) - a(h_{\mathrm{Re}f}) + [44{,}9 - 6{,}55\ell og(h_{Tef})]\ell og(d_{km}) \tag{2}$$

$$a(h_{\mathrm{Re}f}) = 3{,}2[\ell og(11{,}75h_{\mathrm{Re}f})]^2 - 4{,}97) \tag{3}$$

Na Equação 1: *Pt* e *Pr* são as potências de transmissão e recepção; *Gt* e *Gr* são os ganhos das antenas transmissoras e receptoras, respectivamente e *L* é a perda no percurso; Na Equação 2: f_{MHz} é a frequência de 150 a 1500 MHz; *d* é a distancia de 1 a 20 km; h_{Tef} é a altura efetiva da antena transmissora de 30 a 200 m; h_{Ref} é a altura efetiva da antena receptora de 1 a 10 m, e, na equação 3, $a(h_{Ref})$ é o fator de correção da altura efetiva da receptora.

Para compor o mecanismo de reputação deste trabalho optou-se pelo modelo clássico de fusão dos dados apresentado em [Zhu 2009]. Este modelo é formado basicamente pelo rádio definido como centro de fusão de dados, isto é, o rádio que recebe as informações de detecção do espectro, e pelos rádios que as transmitem (Figura 1). O centro de fusão pode ser qualquer um dos rádios que necessitem utilizar os canais licenciados livres em um tempo determinado (**Δ*t***). Em nosso exemplo, é representado pelo rádio ***RC*$_0$**.

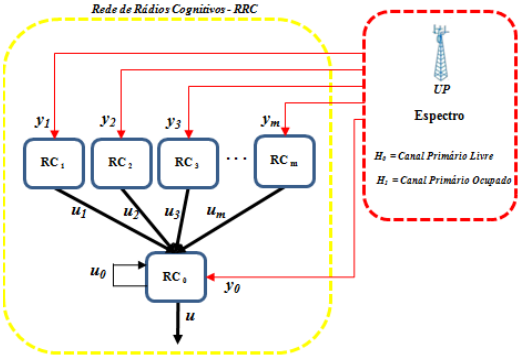

Figura 1 – Modelo Clássico de Fusão de dados

Numa rede, cada rádio mantém históricos de avaliações geradas a partir de suas experiências com outros rádios. Uma avaliação é uma nota dada pelo rádio quanto à veracidade da informação que recebeu sobre os canais licenciados livres. Estas avaliações são usualmente conhecidas por "informações de primeira mão", sendo as avaliações

recebidas de outros rádios comumente chamadas de "informações de segunda mão" [Zhu 2009].

As informações recebidas pelo centro de fusão de dados (***RC₀***) são definidas como u_i, sendo i = 0,1,2,3,...m, dos rádios cognitivos vizinhos (***RCᵢ***), quanto aos canais licenciados livres (**H₀**), e os canais licenciados ocupados pelas transmissões do usuário primário (**H₁**). Sendo u_i =0 ou u_i =1, caso a decisão do ***RCᵢ*** seja **H₀** ou **H₁** respectivamente. Tais informações tem como base a percepção que cada ***RCᵢ*** tem de seus monitoramentos do espectro, e definidas como y_i.

Cada u_i recebida por ***RC₀*** do ***RCᵢ*** é carregada no vetor de fusão $\mathbf{V}u$. Por fim, o centro de fusão, com base nas informações de monitoramento recebidas, bem como a detecção do espectro por ele realizada, extrai uma decisão global, u, onde u = 1 significa a ocupação do canal licenciado, isto é, **H₁**, e u = 0 que o canal está livre, **H₀**.

Basicamente o mecanismo faz a análise das informações u_i e a atribuição de pesos w aos ***RCᵢ***. Após a inicialização do sistema, o crédito de cada rádio ***RCᵢ*** é ajustado para **zero**, sendo que cada ***RCᵢ*** pode acumular créditos por informações u_i corretas.

Sempre que a informação de um determinado rádio for consistente com a decisão global u, isto é, a informação final processada pelo ***RC₀***, seu crédito será aumentado por um; se não diminuído por um. Denotando o crédito para o ***RCᵢ*** por C_i, o sistema de crédito é representado na Equação 4.

$$Ci = \begin{cases} Ci + 1, & if \quad u_i = u \\ \\ Ci - 1, & if \quad u_i \neq u \end{cases} \tag{4}$$

Com a finalidade de justiça ao pontuar a reputação de um rádio que, porventura, tenha classificado erroneamente a detecção do canal licenciado, o peso, antes de ser atribuído ao ***RCᵢ***, é normalizado pela média dos créditos do rádio ***RCᵢ*** . Denotando-se w_i o peso do ***RCᵢ*** , Equação 5. Onde: w_i é o peso do ***RCᵢ***, C_i é o seu crédito; ***avg*** (C_i) denota o crédito médio do ***RCᵢ*** , e g é uma constante cujo valor é de 5.51 (denominado de Valor do Coeficiente de Normalização VCN) , valor este analisado e calibrado pelo autor [Zhu 2009). O Vetor de Credibilidade W é então carregado como o valor de w_i para cada ***RCᵢ*** (Equação 6).

$$w_i = \begin{cases} 0, & if \quad Ci < -g \\ \\ \dfrac{Ci + (-g)}{avg(Ci + g)}, & if \quad Ci > -g \end{cases} \tag{5}$$

$$W = \sum_{i=0} (-1)^{ui+1} wi, \tag{6}$$

$$\begin{cases} W \geq q & \rightarrow aceita\ H_1 \\ W \leq q & \rightarrow aceita\ H_0 \\ -q < W < q & \rightarrow \text{proceder a outra análise} \end{cases}$$

O módulo de teste é inicializado com a determinação do limiar de aceitabilidade q. Este limiar é utilizado para a tomada de decisão por parte do centro de fusão quanto à ocupação, ou não, do canal licenciado. O valor q é utilizado como limite superior e $-q$ utilizado como limite inferior do módulo de teste. Após as análises realizadas, há a convergência da

credibilidade para o mínimo das credibilidades daqueles rádios cujas informações de canais livres divergiram da decisão global de cada cluster.

3.2 Integração dos mecanismos

Os dois mecanismos são combinados por meio de uma função utilidade [Clemen 2001]. Esta função propõe uma utilidade para cada método, onde é calculado o peso representativo da importância de cada um deles. Para a integração dos mecanismos descritos nas seções anteriores é usada, mais especificamente, a Função Utilidade Aditiva (FUA) [Clemen 2001] em virtude de esta proceder a analise de alternativas com atributos puramente independentes, especificamente o que ocorre quando da combinação dos dois mecanismos aqui utilizados. A metodologia utilizada como base da Função Utilidade Aditiva prevê a atribuição de pesos para cada atributo envolvido na tomada de decisão dentre as alternativas envolvidas entre dois ou mais objetivos [Lopes 2008]. Para tal, utilizamos para atribuição de pesos ponderados a cada atributo da Função Utilidade Aditiva, i.e. ao mecanismo de localização e ao mecanismo de reputação, o conceito de algoritmo genético [Lacerda 1999], pois, este consiste em uma heurística de otimização, cujo objetivo é o de achar a solução que corresponda ao ponto máximo de uma determinada função, enquadrando-se, portanto, ao objetivo deste trabalho (procedimentos detalhados na seção 5).

4. Avaliação Experimental

Para a avaliação da proposta foi simulada uma rede sem-fio descentralizada com topologia plana e com nós fixos. Quanto à disposição física da rede, procurou-se reproduzir fielmente a utilizada em [Park 2008] para fim de estudo comparativo. A simulação foi feita em um ambiente MatLab/Simulink.

4.1 Objetivos

O objetivo da avaliação experimental teve como foco a análise comparativa dos mecanismos de detecção de forma isolada bem como os seus desempenhos em atuação conjunta, onde, neste caso, houve a calibração tanto dos limiares de aceitabilidade (LA) quanto dos valores dos coeficientes de normalização (VCN). O desempenho da rede, no que diz respeito à ocupação oportunística dos canais licenciados livres em situações normais, bem como sob regime de ataques, constituiu também um dos objetivos da avaliação. Por fim, a avaliação foi utilizada para a atribuição e calibração dos pesos de cada um dos mecanismos na função utilidade por meio do uso do algoritmo genético.

4.2 Cenário

A rede foi composta por 300 rádios cognitivos, distribuídos aleatoriamente em uma área quadrada de 2000m; cada rádio possui um raio de alcance de transmissão de 250m, com um raio de interferência de 550m, seguindo o modelo proposto em [Ross 2002] (Figura 2a). Dois usuários primários (torre de TV 1 e Torre de TV 2) são posicionas à 8000m e 5000m das bordas externas da rede (Figura 2b). As torres possuem o alcance de transmissão de 9000m e 7000m, respectivamente. As torres possuem frequência de transmissão de 617 MHz; utilizando 10 canais numerados de 1 a 10.

Foi feita a distribuição dos 300 rádios nas coordenadas cartesianas da rede de simulação de forma randômica. A distribuição utilizada para a aleatoriedade dessa inserção, como também em todos os processos da simulação, é a Distribuição Binomial [Garmeman 1993], podendo com isso cada rádio estar ao alcance: (i) das duas torres de TV; (ii) apenas da torre 1; (iii) apenas da torre 2; ou mesmo, (iv) fora do alcance das duas torres. Nessa primeira fase há então a inicialização da rede onde são formados 300 clusters com cada um dos 300 rádios constituintes, cada rádio como centro de cada cluster.

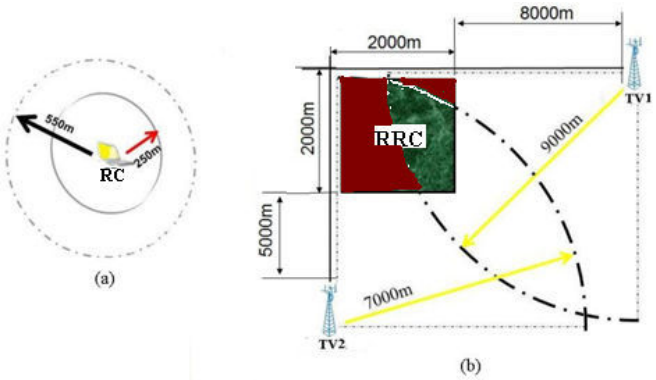

Figura 2. Cenário Utilizado: (a) Raios de Alcance do rádio (b) Rede

Cada rádio reconhece seus rádios vizinhos, isto é, os rádios que estão ao alcance do raio de transmissão do centro do cluster (250m); bem como os rádios que estão em seu raio de interferência (550m), Figura 2a.

4.3 Primeiro Experimento: Simulação das Transmissões

Nesse experimento as transmissões propriamente ditas, com e sem ataques são simuladas. Os parâmetros para a simulação [Park 2008], são modelados da seguinte forma: ambas as torres de TV possuem a altura de 100m; transmitem a frequência de 617 MHz, utilizando 10 canais de frequência, numerados de 1 a 10, cuja sensibilidade das antenas dos receptores primários é de -37.50 dBm. A potencia de transmissão da Torre de TV 1 é de 84 dBm, e da Torre de TV 2 é de 83dBm. Os rádios cognitivos possuem uma potencia de transmissão de 24 dBm, antenas de 1 m de altura, cuja sensibilidade é de -93dBm; transmitindo a frequência de 617 MHz, utilizando 10 canais de frequência, numerados de 1 a 10.

As transmissões são simuladas a cada 100ms, divididas em *slots* de 10ms cada, durante um período de uma hora. As torres de TV utilizam aleatoriamente 8, 9 ou 10 *slots* de 10 ms por transmissão, podendo ocorrer a transmissão: (i) das duas torres simultaneamente; (ii) de apenas uma delas; ou mesmo, (iii) nenhuma transmissão do usuário primário. Há a escolha randômica de 0 a 150 pares de rádios para a transmissão no espaço de 100ms, divididos em *slots* de 10ms cada. Cada rádio pode transmitir pacotes de controle (utilizando-se de 1 a 5 *slots* de 10ms) ou pacotes de dados (de 1 a 10 *slots* de 10ms). Antes de cada transmissão o rádio verifica os canais do espectro de frequência que não estão sendo utilizados: (i) pelas torres de TV; (ii) por outro(s) rádio(s) pertencente(s) ao cluster; ou mesmo, (iii) se não há interferência de alguma transmissão de um cluster vizinho.

São realizadas 30 simulações sem ataque; 30 simulações de cada um dos ataques isoladamente, variando de 1 a 30 rádios atacantes em cada uma delas; e 30 simulações com a combinação de todos os ataques, variando-se de 1 a 30 ataques de cada tipo (Tabela 1).

4.4 Segundo Experimento: Simulação da Detecção de Ataques

O mecanismo de Localização é acionado a cada intervalo de 1 segundo, analisando as potências captadas e procedendo a verificação das fontes de transmissão. Enquanto o mecanismo de reputação é disparado em intervalos de 2.5s, onde os graus de credibilidade de cada rádio são processados com base nas tabelas de frequências livres por eles disseminadas, há a simulação das transmissões das torres de TV e dos rádios, por um período de 1 hora.

A cada unidade de tempo equivalente a 10 ms (definidos como *slot*), aleatoriamente é feita a escolha se haverá ocupação (transmissão) de algum(ns) canal(is) nesse *slot*: (i) por parte das Torres de TV, (ii) de uma delas, (iii) ou de nenhuma – onde, nesse caso, configura-se o *white space*. Simultaneamente, são definidos quantos pares de rádios "irão transmitir" nesse

slot; cada rádio define se irá realizar uma transmissão de dados ou de controle. Na transmissão de controle é feita uma seleção de 1 a 5 pacotes a serem transmitidos (1 pacote equivale a 1 *slot* de tempo), enquanto que na transmissão de dados, a seleção varia de 1 a 10 pacotes. O rádio então faz o sensoriamento do meio, verificando se há a ocupação do espectro (canais) por parte: (i) dos Usuários Primários (UPs) (Torres de TV), (ii) de outro(s) rádio(s) vizinho(s), (iii) ou mesmo de alguma transmissão interferente (rádios a 550m transmitindo). Caso contrário, o rádio transmite 1 pacote, e aguarda o próximo *slot* de tempo para a transmissão de outro pacote, caso haja.

São realizadas simulações com e sem ataques. As simulações com ataques consistem, no caso de Ataques de PUE, na inserção de rádios que, em instantes aleatórios, ocupam de forma prioritária a utilização do *slot* vagos. E no caso do SSFF há a inserção de rádios que, em instantes aleatórios, emitem tabelas de frequências adulteradas.

O Mecanismo de Localização é simulado a cada 1s de forma estática, por meio de tabelas de recepção de potencias pré-configuradas. Essas tabelas são inicializadas por meio do cálculo euclidiano das distancias entre cada rádio e seus vizinhos, bem como entre os rádios e as torres de TV. As potências de recepção são então calculadas com uma taxa aleatória de erro de 10% para mais ou para menos do valor nominal encontrado.

Antes da transmissão, o rádio verifica se há ocupação do espectro de frequência licenciada. Caso as características de transmissão captada não se enquadram com a transmissão dos rádios vizinhos (os pacotes não contem os números MAC - endereço físico de 48 bits do rádio, ou, mais especificamente, da interface de rede), o rádio dispara o mecanismo de localização. A potencia do sinal é analisada, quando então é definida a existência ou não de ataque(s) PUE.

Tabela 1. Dados das Rodadas de Simulações (por *slots* de tempo)

Qtde	Tipo de Ataque	White Space	Tx TV	RCs a Transmitir	RCs que Transmitiram	Pacotes para Transmitir	Pacotes Transmitidos
0	**Sem Atqs**	1.734.167	1.865.033	2.691.394	5.267	12.107.175	89.584
1	**PUE S**	1.632.115	1.657.182	2.032.601	5.208	11.359.036	88.688
30	**PUE S**	1.687.557	1.626.369	2.695.563	1.177	12.210.425	66.265
1	**PUE M**	1.575.944	1.716.623	2.128.404	5.311	12.734.860	88.812
30	**PUE M**	1.605.428	1.774.777	2.413.363	226	12.131.096	66.358
1	**SSFF-SL**	1.655.456	1.889.362	2.572.904	5.018	12.226.692	87.432
30	**SSFF-SL**	1.784.063	1.678.762	2.768.152	5.199	12.733.963	65.327
1	**SSFF-SO**	1.551.707	1.815.660	2.732.220	5.347	12.116.144	85.163
30	**SSFF-SO**	1.764.731	1.619.580	2.442.436	0	12.738.830	63.631
1	**SSFF-SF**	1.768.732	1.801.576	2.453.715	5.289	11.181.238	87.771
30	**SSFF-SF**	1.717.718	1.885.747	2.764.480	835	12.810.070	65.580
5	**Todos**	1.660.131	1.670.717	2.254.649	5.812	12.039.828	87.904
150	**Todos**	1.648.468	1.845.401	2.013.124	0	11.970.240	32.888

O Mecanismo de Reputação é simulado a cada 2,5s, por meio da análise das tabelas de frequência recebidas dos rádios vizinhos, bem como das tabelas do próprio rádio que faz a análise. Por meio dos cálculos de atribuição de credibilidade, a reputação dos rádios então são a eles atribuídas e selecionadas como suspeitas após ultrapassarem os limiares de aceitabilidade. Os limiares de aceitabilidade (LA), superior e inferior (**q** e – **q**), foram definidos por [Zhu 2009], em 15 e -15, respectivamente. Bem com o valor do coeficiente de aceitabilidade (VCA) ***g*** em 5,51.

Foram realizadas 210 rodadas de simulações: 30 sem ataques; 30 variando-se somente o ataque de PUE Selfish de 1 a 30 pares de rádios atacantes; 30 variando-se somente o ataque

de PUE Malicioso de 1 a 30 rádios atacantes; 30 variando-se somente o ataque de SSFF-SL de 1 a 30 rádios atacantes; 30 variando-se somente o ataque de SSFF-SO de 1 a 30 rádios atacantes; 30 variando-se somente o ataque de SSFF-SF de 1 a 30 rádios atacantes, e por fim, 30 variando-se todos os ataques em conjunto de 5 a 150 rádios atacantes.

Na Tabela 1 foram representados os dados referentes as primeiras e as últimas rodadas de cada item acima mencionado. A tabela 1 é formada por 8 colunas, a saber: coluna 01 (Nr de Atacantes), quantidade de atacantes simulados naquele *slot*; coluna 02 indica o tipo de transmissão (sem ataque – Tipo de Ataque); coluna 3 (WS): a quantidade de *slots* de *white spaces*; coluna 4 (TV): a quantidade de slots ocupados pelas Torres de TV; coluna 5 (rádios Tx): quantidade de rádios a transmitir por simulação; coluna 6 (rádios N): quantidade de rádios que transmitiram; coluna 7 (Pc Tx A): número de pacotes a serem transmitidos, e; por fim, coluna 8 (Pc Tx): número de pacotes efetivamente transmitidos.

Podemos observar, por meio dos gráficos representados na Figura 3, a degradação da rede relacionada ao número de rádios que não tiveram oportunidade de transmitir quando os ataques foram inseridos nas simulações. Principalmente quando os ataques são efetuados de forma conjunta, onde, por meio de 15 atacantes, a rede perde totalmente sua capacidade de ocupação oportunística do espectro.

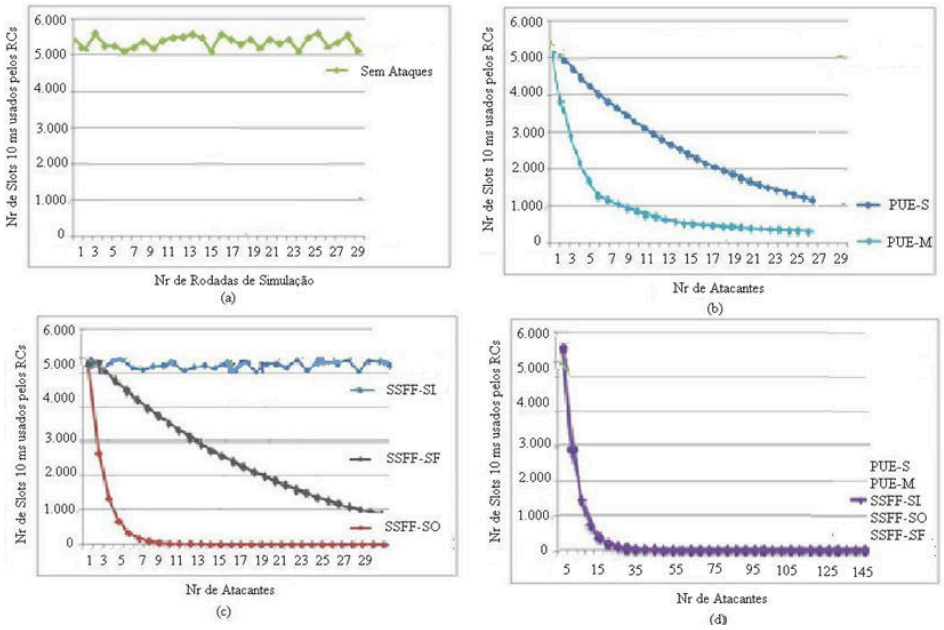

Figura 3. Degradação da RRC: (a) Sem Ataques. (b) Com Ataques de PUE. (c) Com Ataques SSFF. (d) Combinação de Todos os Ataques

Simultaneamente à simulação dos diversos tipos de transmissões, os mecanismos de localização e de reputação são disparados. Ao analisarmos cada tipo de ataque, bem como a atuação dos mecanismos de detecção de forma isolada sem qualquer tipo de calibração verificamos que na detecção do ataque de PUE-S tem-se uma taxa média de verdadeiros positivos na faixa de 42,50 %. Quanto ao ataque de PUE-M, a taxa fica em torno de 34,54%. Essa diferença pode ser justificada em virtude da maior agressividade do ataque de PUE-M, quem tem a finalidade de realmente degradar totalmente a operacionalidade da rede. Ao contrário do ataque de PUE-S, que têm por objetivo utilizar os canais livres de forma egoística.

As taxas médias de verdadeiros positivos quando o mecanismo de reputação é usado de forma isolada para a detecção de ataques de SSFF são: 44.51, 42.64 e 33. 22, para os ataques de SSFF-SL, SSFF-SF e SSFF-SO, respectivamente. Novamente foi demonstrado

que a agressividade do ataque reflete efetivamente no mecanismo de detecção. Maiores taxas para o ataque de SSFF-SL e menores para o SSFF-SO.

4.5. Terceiro Experimento: Variando o LA e o VCN

Neste experimento foram realizadas variações para o limiar de aceitabilidade (LA), bem como o valor da constante de normalização das credibilidades dos rádios (VCN) com intuito de adaptar o mecanismo de análise da reputação para o trabalho em conjunto com o mecanismo de localização. Inicialmente foram fixados o limiar de aceitabilidade e o valor da constante de normalização das credibilidades em, 15 e 5.51, respectivamente, seguindo o proposto no mecanismo original [Zhu 2009]. Em cada rodada de simulação foram realizadas 1.440 avaliações do mecanismo. Sendo realiza avaliações em intervalos regulares de 2.5 segundos. Totalizando nas 30 rodadas de simulações (combinações dos ataques): 43.300 avaliações. A Tabela 2 apresenta os resultados obtidos nesse experimento para o LA;

Tabela 2. LAs Representativos das Rodadas de Simulações

LA	10	11	12	13	14	15	16	17	18	19	20
VP	48,93	49,01	50,00	50,00	50,00	50,00	49,43	49,01	48,90	48,93	47,01
FP	3,66	3,11	2,97	0,16	0,99	1,67	2,69	3,11	3,97	3,66	4,11
FN	1,07	0,99	0,00	0,00	0,00	0,00	0,57	0,99	1,10	1,07	2,99
VN	46,34	46,89	47,03	49,84	49,01	48,33	47,31	46,89	46,03	46,34	45,89

A Tabela 3 apresenta os resultados obtidos nesse experimento para o VCN; e A Tabela 4 apresenta os resultados obtidos com a variação do LA e do VCN em conjunto. As métricas para analisar os experimentos são: (i) falsos positivos (FP), que indicam a quantidade de alarmes falsos; (ii) falsos negativos (FN), que indicam uma condição de normalidade quando na verdade está ocorrendo um ataque; (iii) verdadeiros positivos (VP), que indicam que está ocorrendo um ataque durante um ataque; e (iv) verdadeiros negativos (VN), que indicam uma condição de normalidade quando não está ocorrendo nenhum ataque.

Tabela 3. VCNs das Rodadas de Simulações

VCN	5.46	5.47	5.48	5.49	5.50	5.51	5.52	5.53	5.54	5.55	5.56
VP	48,93	49,01	50,00	50,00	50,00	49,00	48,43	47,86	46,7	45,73	44,02
FP	7,25	5,11	2,97	0,83	0,96	1,67	2,69	3,71	4,73	5,75	6,77
FN	1,07	0,99	0,00	0,00	0,00	1,00	1,57	2,14	3,3	4,27	5,98
VN	42,75	44,89	47,03	49,17	49,04	48,33	47,31	46,29	45,27	44,25	43,23

Tabela 4. LA/VCN Representativos das Rodadas de Simulações

LA	10	11	12	13	14	15	16	17	18	19	20
VCN	5.46	5.47	5.48	5.49	5.50	5.51	5.52	5.53	5.54	5.55	5.56
VP	44,65	**45,25**	45,85	46,45	**47,05**	46,42	45,59	45,56	44,98	44,97	44,07
FP	3,66	3,11	2,97	0,91	**0,16**	1,25	2,69	3,11	3,97	3,66	4,11
FN	5,35	4,75	4,15	3,55	**2,95**	3,58	4,41	4,44	5,02	5,03	5,93
VN	46,34	46,89	47,03	49,09	**49,84**	48,75	47,31	46,89	46,03	46,34	45,89

5. Avaliação dos Resultados e Calibração

Observa-se que: na simulação conjunta dos mecanismos, tanto com o aumento, quanto com a diminuição do limiar de aceitabilidade a partir do valor 13, e do valor do coeficiente de normalização, a partir do valor 5.49 ocorre aumento nos valores de FP e FN.

Já na análise em conjuntos do LA e do VCN, com os valores 14 para o LA e o valor 5.50 para o VCN, obtemos os melhores valores de FP e FN. Como nosso estudo de caso prioriza a detecção de ataques com a utilização em conjunto dos dois mecanismos, optamos por trabalhar com o número de limiar de aceitabilidade igual a 14 e do valor do coeficiente de normalização igual a 5.50. Após as calibrações foram realizadas mais 10 rodadas de simulações utilizando-se o LN=14 e o VCN=5.50.

Houve a inserção de todos os ataques em sua configuração máxima, isto é, 30 atacantes de cada tipo. Os resultados obtidos podem ser observados na tabela 5: VP=45.14, VN=48.70, FN=4.86 e FP=1.30. Valores esses quando comparados a [Park 2008] com uma taxa média de VP=44% e a [Zhu 2009] VP=43,18%, demonstram que a combinação dos mecanismos na detecção de intrusos PUE e SSFF tem um melhor desempenho.

Tabela 5. Comparação entre as métricas de detecção do mecanismos

Nr Atacantes: 150	PARK 2008	ZHU 2009	SDA-COG
VP	44.01	43.18	**45.14**
FP	5.44	4.22	1.30
FN	5.99	6.82	4.86
VN	44.56	45.78	**48.70**

5.1. Calibração dos Pesos dos Mecanismos de Detecção

Após as fases anteriores, uma grande massa de dados foi produzida. Uma parte dessa massa então é utilizada como dados de treinamento para o algoritmo genético (AG) realizar a atribuição de pesos aos mecanismos de detecção. É calculada a Função Detecção *DLRC-i*, do rádio cognitivo *i*. Considerando que: *L-i* representa a análise realizada pelo componente *Localizacao* quanto à identificação de ataque *PUE*, onde *L-i* = 0 (o rádio *i* não é um atacante de *PUE*), ou *L-i* = 1 (o rádio *i* é um atacante de *PUE*). *R-i* representa a análise realizada pelo componente *Reputacao* quanto à identificação de ataque *SSFF*, onde *R-i* = 0 (o rádio *i* não é um atacante de *SSFF*), ou *R-i* = 1 (o rádio *i* é um atacante de *SSFF*). Para determinar a detecção de ataques *DLR-i*, combinam-se os valores *L-i* e *R-i* usando dois coeficientes de calibração γ e ω da seguinte forma:

$$DLR\text{-}i = \gamma L + \omega R \tag{7}$$

Onde: $\gamma + \omega = 1$. Para tal a função DLR*i* (Equação 7) é ponderada por meio da criação de 5 cromossomos (Equação 8) – o Mecanismo de Localização é representado por dois cromossomos: *L1*: Mecanismo de Detecção de Ataque PUE Selfish, e; *L2*: Mecanismo de Detecção do Ataque PUE Malicioso. Quanto ao Mecanismo de Reputação, este é representado por três cromossomos: *R1*: Mecanismo de Detecção de Ataque SSFF-SL; *R2*: Mecanismo de Detecção de Ataque SSFF-SO, e; *R3*: Mecanismo de Detecção de Ataque SSFF-SF.

$$DLR_i = (\gamma_1 L_1 + \gamma_2 L_2) + (\omega_1 R_1 + \omega_2 R_2 + \omega_3 R_3) \tag{8}$$

Cada cromossomo é composto por 30 genes, formando a primeira geração [Lacerda 1999]. Cada conjunto de genes (cromossomo) forma um vetor de peso. Cada gene, variando de [0-1], representa os pesos de cada mecanismo (γ para os mecanismos de Localização, e ω para os mecanismos de Reputação). São realizados os cruzamentos, seleções e mutações por um número total de 100 gerações nas 30 rodadas de simulações com todos os ataques, Tabela

1. Os valores representativos dos pesos que consistem na solução que corresponda ao ponto de máximo da função DLR*i* são (Equação 9):

$$DLR_i = (\mathbf{0{,}199}L_1 + \mathbf{0{,}321}L_2) + (\mathbf{0{,}035}R_1 + \mathbf{0{,}342}R_2 + \mathbf{0{,}103}R_3) \quad (9)$$

Podemos observar que os pesos atribuídos pelo AG condizem com a realidade da degradação da rede (Figura 3), onde o ataque mais agressivo observado é o de SSFF-SO, cujo peso de 0.342 é o de maior valor na função de detecção. Da mesma forma o peso para a detecção do ataque de SSF-SL, 0.035, reflete o ataque de menor expressão, quando comparados aos outros. Aplicando-se o mecanismo com os pesos ponderados pelo AG à massa de treinamento obtemos os valores observados na Tabela 6.

Tabela 6. Mecanismos Calibrados pelo AG e simulados com os cinco tipos de ataques

Nr Atacantes	5	25	50	75	100	125	150	Média
VP	50,00	50,00	50,00	49,31	44,87	38,45	34,29	45,65
FP	0,00	0,00	0,00	0,69	5,13	11,55	15,71	4,35
FN	0,00	0,00	0,00	0,00	1,16	3,02	5,15	1,23
VN	50,00	50,00	50,00	50,00	48,84	46,98	44,85	48,77

Finalizando, uma nova massa de dados, diferente dos dados utilizados para o treinamento do AG, é analisada com o mecanismo de detecção, agora com pesos ponderados pela função de detecção (Equação 9), cujos resultados medianos aumentaram a taxa de VP em cerca de 0.5 ponto percentual, isto é: VP=45.63, demonstrando que realmente há a necessidade de atribuição de pesos para a detecção de ataque combinados às redes, Tabela 7.

Tabela 7. Mecanismos Calibrados pelo AG e simulados com os cinco tipos de ataques

Nr	5	25	50	75	100	125	150	Média
VP	50.00	50.00	50.00	49.44	44.91	38.54	34.33	45.63
FP	0,00	0,00	0,00	0,56	5,09	11,46	15,67	4,37
FN	0,00	0,00	0,00	0,00	1,26	3,12	5,34	1,24
VN	50,00	50,00	50,00	50,00	48,74	46,88	44,66	48,76

6. Conclusão

Este trabalho teve como objetivos apresentar um estudo sobre a detecção de ataques e propor um SDA baseado em técnicas de localização e classificação de reputação para redes de rádios cognitivos. Foi simulada uma rede com a criação dos diversos perfis de comportamento dos rádios cognitivos necessários à análise do desempenho da rede sob condições de ataques. Tal SDA foi programado de forma a atender, então, às demandas e restrições deste tipo de rede. Nos experimentos realizados, observou-se a degradação da capacidade de utilização oportunística de ocupação dos canais licenciados livres por parte dos rádios, proporcionalmente ao aumento do número de atacantes. O SDA mostrou-se eficaz na detecção, tanto de ataques isolados, como também aqueles realizados de forma conjunta. Com o uso do mecanismo de reputação, associado ao de localização, houve uma convergência eficiente da rede como um todo na identificação de ataques sofridos pela rede. Principalmente após a calibração, em uma primeira fase, do mecanismo de reputação, e em seguida, da calibração do SDA com um todo. Em trabalhos futuros serão investigadas outras opções de cálculo do limiar de aceitabilidade, bem como o do valor do coeficiente de normalização, com o intuito de analisar uma melhor forma de detecção do intruso. Pretende-se também realizar outros tipos de testes para a atribuição de pesos a cada mecanismo utilizado, com a finalidade de aumentar a eficiência e a eficácia do SDA.

Referências

Akyildiz, Ian F.; VURAN, Mehmet C.; LEE, Won-Yeol; MOHANTY, Shantidev, (2006a). "NeXt generation/dynamic spectrum access/cognitive radio wireless networks:A survey**".** Computer Networks, n. 50.

Akyildiz Ian F, J. Laskar, and Y. Li, (2006b), "OCRA: OFDM-based cognitive radio networks," Broadband Wireless Networking Laboratory Technical Report, March.

Akyildiz, Ian, F., LEE, WON-YEOL, VURAN, M. C., & MOHANTY S, (2008). "A Survey on Spectrum Management in Cognitive Radio Networks**".** IEEE Communications Magazine,

Clancy,T, Goergen N , (2008). "Security in cognitive radio networks: threats and mitigation". Third International (CrownCom),; 1–8. DOI: 10.1109 / CROWNCOM .2008.4562534.

Clancy, T, A. Khawar, (2009)."Security Threats to Signal Classifiers Using Self-Organizing Maps", Fourth International CrownCom)

Clemen, R. T.; REILLY, T. (2001) Making Hard Decisions: An Introduction to Decision Analisys. Pacific Grove: Duxbury, 2001.

Fcc (2003), Federal Communication Commission Home Page. http://www. fcc.gov -

Garmeman D. e Migon, H.S., (1993). Inferência estatística: uma abordagem integrada. Textos de Métodos Matemáticos do Instituto de Matematica, UFRJ

Hata, M. Empirical formula for propagation loss in land mobile radio services. IEEETrans. On Vehicular Technology, v. VT-29, n. 3, p. 317-325, aug. 1980.

Inatel (2009) Instituto Nacional de Telecomunicações– "Projeto Sendora", Curso de Mestrado em Telecomunicações - http://www.inatel.br/

Lacerda, E.G.M e Carvalho, A.C.P.L. (1999) "Introdução aos algoritmos genéticos", In: Sistemas inteligentes: aplicações a recursos hídricos e ciências ambientais. Editado por Galvão, C.O., Valença, M.J.S. Ed. Universidade/UFRGS: Ass Bras de Recursos Hídricos.

Leon, Olga, Juan Hernandez-Serrano, Miguel Soriano (2010). "Securing cognitive radio networks".International Journal of Communication Systems, vol 23,. ISSN/ISBN 1074-

Lopes C. L. (2008) A escolha de um custodiante para uma administradora financeira: Análise multiatributo por medições conjuntas e trocas justas. Mestrado em adm, Ibmec – RJ,

McHenry, M. (2003). Frequency agile spectrum access technologies, FCC Workshop CR.

Mitola, J (2000). "Cognitive radio: An integrated agent architecture for software defined radio". Ph.D. Dissertation, KTH Royal Institute of Technology, Stockholm, Sweden.

Mitola III and G. Q. Maguire, Jr. (2009), "Cognitive Radio: Making Software Radios More Personal," IEEE Personal Communications, Vol. 6, No. 4, pp. 13-18, Aug.

Misha ,S., M Sahai, A., Brodersen, R.W., (2006). Cooperative Sensing among Cognitive Radios. In: IEEE International Conference on Communications, ICC 2006, 1658–1663

Park, J., M. R. Chen, , and J. H. Reed**,** (2008). **"**Defense against primary user emulation attacks in cognitive radio networks**,"** IEEE Journal on Selected Areas in CSICRTA Vol. 26, No. 1,

Ross T., P. Myllymaki, and H. Tirri, (2002). "A statistical modeling approach to location estimation," IEEE Trans. Mobile Computing, Vol. 1, Jan.-March, p 59–69.

Ruiliang, C., Jung-Min, P., Hou, Y.T., Reed, J.H. (2008a): Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks. IEEE Communications Magazine 46,50–

Ruiliang, C, Jung-Min, P., Kaigui, B. (2008b).: Robust Distributed Spectrum Sensing inCognitive Radio Networks. In: IEEE The 27th, INFOCOM 2008, pp. 1876–1884

Shrestha , J., Sunkara, A. , Thirunavukkarasu, B., (2010). Security in Cognitive Radio. San Jose: San Jose State University.

Thomas R. W., L. A. Da Silva, and A. B. MacKenzie, (2005) "Cognitive Networks," *IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN 2005.*,

Zhu, Feng and Seung-Woo Seo, (2009). "'Enhanced Robust Cooperative Spectrum Sensing in Cognitive Radio", JCN, Special Issue on Cognitive Radio: A Path in the Evol of Public

