UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

Joffre Gavinho Filho

SDA-COG - Sistema de Detecção de Ataques para Redes de Rádios Cognitivos

Rio de Janeiro
2012

Joffre Gavinho Filho

SDA-COG - Sistema de Detecção de Ataques para Redes de Rádios Cognitivos

PPGI
UFRJ

Joffre Gavinho Filho

SDA-COG - Sistema de Detecção de Ataques para Redes de Rádios Cognitivos

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Informática, Universidade Federal do Rio de Janeiro, como requisito parcial à obtenção do título de Mestre em Informática.

Orientador: Luiz Fernando Rust da Costa Carmo D. Inf. UPS.

Rio de Janeiro
2012

FICHA CATALOGRÁFICA

G182 Gavinho Filho, Joffre.

SDA COG – Sistemas de Detecção de Ataques para Redes de Rádios Gognitivos. / Joffre Gavinho Filho. -- 2012.
81 f.: il.

Dissertação (Mestrado em Informática) – Universidade Federal do Rio de Janeiro, Instituto de Matemática, Instituto Tércio Pacitti.

Orientador Luiz Fernando Rust da Costa Carmo.

1. Sistema de Detecção de Ataques. 2. Rádio Cognitivo. 3. Segurança - Teses I. Carmo, Luiz Fernando Rust da Costa (Orient.). II. Universidade Federal do Rio de Janeiro, Instituto de Matemática, Instituto Tércio Pacitti. III Título.

CDD

Joffre Gavinho Filho

SDA-COG - Sistema de Detecção de Ataques para Redes de Rádios Cognitivos

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Informática, Universidade Federal do Rio de Janeiro, como requisito parcial à obtenção do título de Mestre em Informática.

Aprovada em: Rio de Janeiro 31 de Agosto de 2012.

Prof. Luiz Fernando Rust da Costa Carmo – Orientador
Dr. UPS, França
UFRJ/PPGI

Profª. Luci Pirmez
D. Sc., COPPE/UFRJ, Brasil
UFRJ/PPGI

Prof. Raphael Carlos Santos Machado
D. Sc., COPPE/UFRJ, Brasil
INMETRO

Prof. Aloysio de Castro Pinto Pedroza
Dr. UPS, França
COPPE

Rio de Janeiro
2012

Dedico este trabalho a todos da minha família, especialmente à memória póstuma de meu Pai Joffre – meu grande Mestre –, à minha Mãe Lúcia e a minhas filhas Carli e Maria Luíza que, de forma inconteste, foram meu sólido alicerce para superar mais este desafio.

AGRADECIMENTOS

Aos meus pais, Joffre e Lúcia, pela formação, ensinamentos, exemplos e dedicação que, de forma única, forjaram o que de melhor há em mim.

A minhas filhas Carli e Maria Luíza, que norteiam todos os passos de minha vida.

Ao meu irmão Jorge que, de sobremaneira, sempre me apoiou em minha incansável busca do conhecimento.

A toda minha linda e impar família que, em seu caloroso aconchego, me ampararam em todos os momentos difíceis.

Aos amigos "combatentes" do laboratório de redes do NCE que "*pari passu"* buscam, como eu, suplantar mais esse degrau em nossa formação acadêmica, muito os agradeço.

Ao professor, companheiro, mestre e aluno, Claudio. Incansável no seu propósito, e que mesmo com suas 24 horas diárias repletas de atividades, conseguia, com sua mão amiga, auxiliar, não só a mim, mas todos aqueles que o cercam. Obrigado!

Aos professores do PPGI pelas orientações e ensinamentos. A ajuda dos senhores foi fundamental para o meu sucesso.

Em especial ao meu orientador, professor Luiz Fernando Rust da Costa Carmo que junto à professora Luci Pirmez e ao professor Raphael Carlos Santos Machado, mantiveram-se sempre dispostos a me orientar e ajudar, guiando-me durante todo o caminho. Professores, o sucesso deste trabalho é um reflexo de toda a vossa dedicação. Sinto-me orgulhoso de ter sido orientado pelos senhores. Muito obrigado!

"*Tra la spica e la man qual muro he messo*."

Luís Vaz de Camões

Os Lusíadas (c. IX est. 78 v. 8)

RESUMO

GAVINHO, Joffre Filho. SDA-COG - Sistema de Detecção de Ataques para Redes de Rádios Cognitivos. Rio de Janeiro, 2012. Proposta de Dissertação (Mestrado em Informática) Programa de Pós-Graduação em Informática, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2012.

Neste trabalho é proposto um Sistema de Detecção de Ataques (SDA) para redes de rádios cognitivos (RRC). A RRC é uma rede auto-organizada que combina tecnologias sem fio com processos cognitivos de aprendizagem e adaptação às características do meio de transmissão em que se encontra. Entre as diversas aplicações em que tais características poderiam ser utilizadas, citamos a sua aplicabilidade na solução da escassez espectral. Problema este ocasionado pela maciça utilização de equipamentos que fazem uso da tecnologia de transmissão sem fio nas faixas não licenciadas do espectro de freqüência. Entre as possíveis soluções para se evitar tal escassez, encontramos a utilização oportunística das faixas subutilizadas do espectro licenciado de freqüência.

Uma das características da tecnologia das RRC é a necessidade do constante monitoramento do meio para que o rádio possa: perceber, decidir e adaptar-se às condições reais de transmissões oportunísticas nas freqüências proprietárias. Todavia, tal característica a torna vulnerável a tipos específicos e novos de ataques não observados nas redes convencionais.

A proposta deste trabalho consiste no desenvolvimento e validação de um método de integração de diferentes mecanismos de detecção de ataques para as RRCs. O objetivo da utilização dos princípios destes mecanismos aplicados aos procedimentos de monitoração e percepção do meio é o da mitigação dos ataques, aumentando a eficiência e a eficácia da RRC. Para tal, o SDA proposto é formado pela combinação de dois mecanismos clássicos de detecção de ataques adaptados para esse tipo de cenário: mecanismos de Localização e de Reputação. A proposta foi avaliada por meio de experimentos para demonstrar o desempenho em conjunto dos mecanismos adaptados aplicados à detecção de dois tipos de ataques específicos às RRCs: Emulação do Usuário Primário (*Primary User Emulation* - PUE) e falso diagnóstico do sensoriamento do espectro (*Sense Spectrum False Feedback* - SSFF).

Palavras-chaves: Sistema de Detecção de Ataques. Radio Cognitivo. Segurança.

ABSTRACT

GAVINHO, Joffre Filho. SDA-COG - Sistema de Detecção de Ataques em Redes de Rádios Cognitivos. Rio de Janeiro, 2011. Proposta de Dissertação (Mestrado em Informática) Programa de Pós-Graduação em Informática, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2011.

This work proposes an Attack Detection System (ADS) for cognitive radio networks (CRN). The CRN is a self-organized network that combines wireless technologies with cognitive learning and adaptation processes with the characteristics of the transmission medium. Among the many applications in which such features could be used, we cite their applicability in spectral solution. This problem is caused by the massive use of equipment that make use of the wireless transmission technology in the unlicensed frequency spectrum bands. Among the possible solutions to prevent this shortage, we find the use of under-utilized tracks of opportunistic licensed spectrum frequency bands.

One of the features of the CRN technology is the constant need of monitoring the environment in order to make possible for the radio to: understand, decide and adapt to real conditions of opportunistic transmissions in proprietary frequencies. However, this characteristic makes it vulnerable to specific new types of attacks not seen in conventional networks.

This work's proposal consists in the development and validation of a integration method for different CRNs attack detection mechanisms. The goal of using these mechanisms principles applied to the monitoring procedures and environment perception is the mitigation of attacks, increasing the efficiency and effectiveness of the CRN. To this end, the proposed ADS is formed by the combination of two classic attack detection mechanisms adapted to this kind of scenario: location and Reputation mechanisms. The proposal was evaluated by means of experiments to demonstrate the performance of the adapted mechanisms together applied to the detection of two types of specific attacks at CRNs: Primary User Emulation (PUE) and Spectrum Sense False Feedback (SSFF).

Keywords: Attack Detection System. Cognitive Radio. Security.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AG	–	Algoritmo Genético
ARC	–	Ambiente do RC
BS	–	Base Station
CCA	–	Common Control Data Attack
CER	–	Crossover Error Rate
CIDF	–	Common Intrusion Detection Framework
CRN	–	Cognitive Radio Network
dBm	–	Decibéis Metro
DoS	–	Denial of Service
FN	–	Falso Negativo
FP	–	Falso Positivo
FCC	–	Federal Communications Commission
FF	–	False Feedback
FLL	–	Frquencia Licenciada Livre
FN	–	Falso Negativo
FP	–	Falso Positivo
FUA	–	Função Utilidade Aditiva
GHz	–	GigaHertz
IEEE	–	Institute of Eletrical and Eletronics Engineering
ISM	–	Industrial, Scientific and Medical
Km	–	Kilometro
k-NN	–	k-Nearest Neighbor
kW	–	KiloWatts
LA	–	Limiar de Aceitabilidade
LBG	–	Linde, Buzo e Gray
Mbit/s	–	MegaBits por segundo
MLBG	–	Modified Linde, Buzo e Gray
MHz	–	MegaHertz
mW	–	Miliwatts
OFA	–	Objective Function Attack
P2P	–	Peer-to-Peer
PUE	–	Primary User Emulation Attack
PUE-M	–	Primary User Emulation Attack - Malicious

PUE-S	–	Primary User Emulation Attack – Selfish
PST	–	Primary signal transmitter
QOS	–	Quality of Service
RC	–	Rádio Cognitivo
RF	–	Rádio Frequência
RRC	–	Rede de Rádios Cognitivos
RSF	–	Rede sem Fio
RSS	–	Received Signal Strengthn
RSSF	–	Rede de Sensores Sem Fio
SDA	–	Sistema de Detecção de Ataques
SDA-COG	–	Sistema de Detecção de Ataques para RRC
SSFF	–	Spectrum Sense False Feedback
SSFF-SL	–	Spectrum Sense False Feedback - Sempre-Livre
SSFF-SO	–	Spectrum Sense False Feedback - Sempre-Ocupado
SSFF-SF	–	Spectrum Sense False Feedback - Sempre-Falso
TCP	–	Transmission Control Protocol
TIC	–	Tecnologia de informação e comunicação
TV	–	Televisão
UDP	–	User Datagram Protocol
UHF	–	Ultra-High Frequency
UP	–	Usuário Primário
US	–	Usuário Secundário
VCN	–	Valore dos coeficientes de normalização
VHF	–	Very High Frequency
VN	–	Verdadeiro Negativo
VP	–	Verdadeiro Positivo
W	–	Watts
WG	–	Work Group
WGES	–	The Work Group in Efficiency of Spectrum
WRAN	–	Wireless Regional Area Network

Sumário

1 Introdução

1.1 Rádio Cognitivo

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). Esta parte do espectro pode ser uma banda inteira (nos sistemas móveis celulares) ou um canal dentro de uma banda (emissoras de rádio e televisão).

O modelo de alocação estática de bandas do espectro de freqüência no Brasil (INATEL 2009) 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. No entanto, há restrições no conteúdo que pode ser transmitido e os tipos de serviços que eles poderão oferecer (INATEL 2009). Citamos como exemplo a utilizada pelos radioamadores; e

(iii) ***Não licenciado*** - utiliza o espectro de frequência sem a necessidade de se obter uma licença. Não há um único usuário com direito de uso exclusivo e todos os usuários estão sujeitos aos limites nos termos da licença ("não licenciado" não significa sem regulamentação, os dispositivos deverão estar homologados conforme estabelecido pelo órgão regulador para poderem operar nesta parte do espectro).

Uma observação que deve ser feita é que as bandas não licenciadas de 2.4GHz a 2.5GHz e 5,8GHz são denominadas: Industrial, Cientifica e Médica (traduzido do inglês: *Industrial, Science and Medical* - ISM), frequências estas utilizadas pelas redes sem fio, controles remotos de televisão, telefones sem fio etc.

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 da Comissão Federal de Comunicações, 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 sem fio (AKYILDIZ 2006a). Em uma rede formada por RCs, os dispositivos são equipados com rádios 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), (HAYKIN 2005) e (THOMAS 2005). Com base nas informações de sensoriamento do espectro, os usuários de RC 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).

1.2 Aspectos de Segurança do RC

Se por um lado o uso da tecnologia de rádios cognitivos traz benefícios como: (i) solucionar o problema de escassez de frequências disponíveis no espectro de radiofreqüência; (ii) melhorar o potencial de desempenho das comunicações sem fio em geral; e (iii) minimizar a interferência entre dispositivos de rádio; por outro lado, origina uma série de desafios que ainda devem ser superados e que propiciam um vasto campo para pesquisa.

Entre os vários desafios a serem explorados 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, tais características o torna vulnerável a tipos específicos e novos de ataques para esse tipo de rede 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 RRCs, caso seja empregado para monopolizar egoisticamente a ocupação das FLL (*Selfish*), ou de forma a impedir que alguns RCs a utilizem (denominada de ataque de negação de serviço – *Denial of Service – DoS*). Por exemplo, em uma rede de rádios cognitivos, um atacante utilizando-se de uma transmissão "maliciosa" pode indicar aos rádios cognitivos dessa rede que as pretensas faixas licenciadas, que poderiam ser utilizadas por eles, estão em uso. 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 RRC.

1.3 Objetivos

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 as RRCs 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.

Basicamente identificou-se dois novos tipos de ataques às RRCs (LEON 2010): a emulação do usuário primário (*Primary User Emmulation* – PUE) e a adulteração das tabelas de FLL (*Spectrum Sense False Feadback.*- SSFF).

No caso do PUE (PARK 2008), um ou mais RCs modificam as suas características de transmissão, adaptando-as a forma utilizada pelo usuário primário, e induzem aos outros RCs da RRC de que estas FLLs já estão em uso. Caso o ataque seja utilizado por pares de RCs para monopolização das FLLs, este é denominado de PUE-S (*Primary User Emmulation – Selfish*). Caso a finalidade seja impedir que nenhum RC da RRC utilize as FFLs, este é definido como PUE-M (*Primary User Emmulation – Malicious*).

Nas RRCs onde ocorre o monitoramento do espectro de forma colaborativa (ZHU 2009), a ocupação das FLLs é baseada nas informações trocadas entre os RCs (tabelas de frequências livres) sobre quais frequências estão livres ou não (ZHU 2009). 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 FLLs não sejam compartilhadas, ficando o seu uso exclusivo para um único usuário, denomina-se de ataque SSFF no modo *Selfish.* Se uma FLL é declarada livre (resp. ocupada)

quando estão ocupada (resp. livre) apenas para impedir a sua utilização, configura-se um ataque SSFF de modo *DoS.*

Os principais mecanismos para detecção de ataques de PUE e de SSFF são respectivamente: os de localização (PARK 2008) e os de reputação (ZHU 2009).

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 identificará se o rádio em análise é um usuário principal (torre de transmissão da frequência licenciada), ou um usuário secundário (rádio cognitivo componente da Rede). Nas propostas de (PARK 2008) e (CLANCY 2009) usa-se uma rede de sensores secundária à RRC, onde são realizadas as análises e cálculos necessários à determinação do posicionamento geográfico dos equipamentos componentes da RRC.

O mecanismo de reputação tem por finalidade definir um grau de credibilidade às informações sobre as tabelas de freqüências livres recebidas dos RCs da RRC (ZHU 2009). Os modelos baseados em Sistemas de Reputação se fundamentam em interações prévias ocorridas entre os membros de uma rede. Segundo (SWAMYNATHAN *et al*., 2007), o conceito de reputação é definido como uma medida coletiva de confiabilidade em uma pessoa (ou coisa) baseada em indicações ou avaliações de membros de uma comunidade. Assim, o nível individual de confiança em tal pessoa pode ser obtido a partir de uma combinação das indicações recebidas e das experiências pessoais. O uso da reputação atribui um grau de aceitação a um indivíduo da rede de rádios cognitivo para desempenhar uma tarefa sem que necessariamente o RC requisitante tenha interagido com o RC alvo anteriormente. Para tanto, utiliza-se as experiências dos demais RC da Rede.

Os mecanismos de localização (PARK 2008) e o de reputação (ZHU 2009) são efetivamente empregados de forma isolada. Entretanto, 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 RRC. Quando um rádio está localizado no limite de alcance da transmissão do UP, i.e, onde a potência de recepção captada pelo RC 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 RC da RRC 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 RRC, não consiga inferir sobre algum ataque de PUE, o mecanismo de reputação o possibilitará. Visto que, o uso indevido de uma FLL por um atacante PUE induzirá aos RCs ao seu alcance de transmissão que não há canais livres e, por conseqüência, tais RCs disseminarão suas tabelas de freqüências indicando que tais canais estão ocupados pelo UP. Porém, todos os RCs que estiverem ao alcance dos RCs 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 RRC onde o atacante PUE está localizado. A retroalimentação de informações confiáveis de ataques (aferidas e validadas através dos mecanismos de reputação) indica aos RCs atacados que há uma transmissão indevida realizada por um RC localizado dentro dos seus raios de transmissão.

Ainda quanto ao mecanismo de localização (PARK 2008), outro ponto importante que deve ser observado é que este utiliza uma rede de sensores sem fio (RSSF), secundária à RRC, para a detecção de ataques de PUE. Há com isso a inserção de mais um ponto de vulnerabilidade à RRC pois, a própria RSSF pode ser alvo de ataques que modifiquem a análise realizada pelo mecanismo de localização, causando com isso a não detecção de ataques PUE e, por conseqüência, a degradação do uso oportunístico da FLL por parte dos RCs legítimos. Foi proposta também nessa dissertação, uma das formas de se evitar tal problema: a supressão da RSSF e a implementação do mecanismo nos próprios RCs autenticados da rede, eliminando com isso, esse ponto vulnerável da RRC.

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.

Uma das principais contribuições deste trabalho consiste no desenvolvimento e validação de um método de integração destes diferentes mecanismos de detecção de ataques, visando maximizar o seu desempenho.

Os dois métodos serão combinados por meio de uma função utilidade aditiva (CLEMEN 2001), onde é proposta uma utilidade para cada método e calculado o peso representativo da importância de cada um deles. Para esta atribuição de pesos ponderados a cada um dos mecanismos, faz-se uso de algoritmos genéticos (AG).

Como objetivos secundários podemos citar: (i) análise do efeito destrutivo dos ataques de PUE e de SSFF isoladamente, bem como de forma conjunta, ao desempenho da RRC; (ii) adaptação do mecanismo de localização para o ambiente urbano; (iii) calibração do mecanismo de reputação para a detecção em conjunto com o mecanismo de localização; e (iv) avaliação do uso de uma arquitetura descentralizada, onde o SDA-COG é distribuído por todos os rádios da RRC.

1.4 Organização do trabalho

O restante deste trabalho está organizado da seguinte forma. No Capítulo 2 discutem-se os conceitos básicos que descrevem em linhas gerais a base de conhecimento para este trabalho. No Capítulo 3 a proposta do Sistema de Detecção de Ataques é apresentada bem como a sua arquitetura computacional. No Capítulo 4 são apresentados os experimentos realizados. No Capítulo 5 as análises dos resultados obtidos são apresentadas. Finalmente no Capítulo 6 são tecidas as conclusões finais e as propostas de trabalhos futuros.

2 Conceitos Básicos

Nesta seção são descritos os conceitos básicos que são utilizados na seqüência deste trabalho relativos ao rádio cognitivo (RC), bem como os mecanismos de detecção de ataques, que são necessários para o entendimento do trabalho proposto. Na seção 2.1 é descrita a conceituação de um rádio cognitivo e as suas quatro funcionalidades operacionais básicas para a utilização oportunística dos canais de freqüências licenciados livres (FLL). Na seção 2.2, os aspectos de segurança são descritos, incluindo-se aí as principais formas de ataques às redes de raios cognitivos (RRCs). Na seção 2.3 conceitua-se o que é um sistema de detecção de ataque/intrusão e as suas classificações. As técnicas empregadas para a detecção de ataques às RRCs utilizadas nesse trabalho são descritas na seção 2.4: localização e reputação. A seção 2.5 introduz o conceito de função utilidade que é empregada para a combinação dos dois mecanismos. Na seção 2.6, é feita a descrição de algoritmos genéticos utilizados para atribuição de pesos ponderados à função utilidade e, por fim, na seção 2.7, são tecidas as conclusões do capítulo.

2.1 Rádios Cognitivos

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).

Portanto, o Rádio Cognitivo (RC) é uma nova abordagem de acesso ao espectro de radiofreqüência que visa otimizar o uso deste recurso de forma oportunística. O RC é baseado no acesso oportunista de usuários não-licenciados em faixas de freqüência regulamentadas. O RC é baseado em software visando dois objetivos principais: comunicação confiável e utilização eficiente do espectro de rádio.

Por suas características, o rádio cognitivo tem basicamente dois conjuntos de tarefas: o primeiro ligado ao aprendizado do meio de operação e o segundo ligado ao controle da transmissão e ao gerenciamento do espectro. No primeiro conjunto de tarefas se destaca o monitoramento do espectro e a detecção dos buracos no espectro que constituem uma oportunidade de comunicação para usuários secundários.

Para suportar tais capacidades, o RC possui 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 Qualidade de Serviço (*Quality of* Service – *QoS*). 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 (RRC) de utilizar os canais licenciados livres de forma cooperativa e colaborativa entre os rádios da rede.

Dentre as diversas pesquisas realizadas para a operacionalização do RC citamos uma em especial: a desenvolvida pelo grupo de trabalho IEEE 802.22 WG (*Work Group*) do IEEE (*Institute of Eletrical and Eletronics Engineering*), que resultou na padronização IEEE 802.22 (IEEE 2004). Tal padrão, que também é chamado de WRAN (*Wireless Regional Area Network*) é a primeira especificação do mundo que utiliza técnicas de rádios cognitivos, onde a comunicação de redes sem fio é feita na mesma banda de TV analógica e digital (IEEE 2004). Este padrão visa a comunicação ponto-multiponto, i.e, uma rede infra-estruturada formada por uma Estação Base (*Base Station* – BS) e os usuários secundários, operando nas frequências não utilizadas das bandas de transmissão de TV VHF (*Very High Frequency*) e UHF (*Ultra-High Frequency*), especificamente, entre os 54 MHz e os 862 MHz (IEEE 2004).

De acordo com o padrão IEEE 802.22, a sua utilização está voltada para um mercado de banda larga sem fios em zonas rurais, inóspitas ou economicamente desfavoráveis para a instalação de infra-estruturas. O tamanho da célula da BS deverá abranger tipicamente uma área circundante num raio de 20 a 40 km, conseguindo em casos extremos servir utilizadores a 100 km de distância. Num caso de uma cobertura num raio de 33 km poderá servir aproximadamente 1.25 pessoas por km2 (HWANG 2008), ou 5 pessoas por km2 com um raio de 17 km (COURSES 2007). A largura de canal deverá ser de 6 MHz conseguindo assim aproximadamente 18 Mbit/s de transmissão na BS (KURAN 2007), podendo mesmo chegar a 30 Mbit/s, segundo (COURSES 2007). Esta tecnologia será ainda capaz de empregar *QoS* na transmissão de dados, voz e vídeo (CORDEIRO 2005).

Em suma, O IEEE 802.22 é um padrão para redes sem fio voltado para conectividade de áreas rurais que faz uso do rádios cognitivos e pode revolucionar o modo como o espectro de frequências é compartilhado, abrindo caminho para novas formas de exploração deste meio de transmissão.

2.2 Segurança em Rádios Cognitivos

As RRCs possuem uma série de novas vulnerabilidades, quando comparadas às redes convencionais, que podem ser exploradas de forma a atingir o sistema como um todo. Neste contexto um ataque em uma RRC é definido como bem sucedido quando consegue pelo menos um dos seguintes objetivos (LEON 2010):

(i) **interferência inaceitável aos usuários primários** – uma das principais premissas para a utilização das freqüências licenciadas livres (FLLs) de modo oportunístico pela RRC é a obrigatoriedade de não haver qualquer tipo de interferência nas transmissões do usuário primário (UP). Logo, um ataque neste contexto é caracterizado quando um ou mais rádios cognitivos iniciam, ou mesmo não interrompem, as suas transmissões, em uma determinada faixa de freqüência licenciada livre (FLL), no instante que o UP a utiliza para o seu processo de comunicação, reduzindo, ou mesmo inutilizando, por conseqüência, a capacidade de recepção da rede primária:

(b) **obstrução da utilização das FLLs por parte dos rádios cognitivos** – o atacante ocupa de forma maliciosa os canais licenciados livres do espectro, impedindo que os outros rádios secundários possam ocupá-los, causando com isso a negação de serviço na RRC; e

(c) **injeção de dados falsos na rede** – as funcionalidades operacionais do RC são baseadas, além do monitoramento do meio em que se encontra, na troca de informações entre os rádios autenticados componentes da rede, entre elas: tabelas de freqüências livres, tipo de codificação utilizada nas comunicações etc. Um RC que, de forma maliciosa, informe, por meio de dados adulterados, situações que não condizem com a realidade da rede, pode provocar uma série de ações imprevisíveis por parte dos rádios, entre elas, a não utilização oportunística das freqüências livres.

Novos ataques às redes cognitivas, sumarizados e detalhados em seguida, foram escritos em (LEON 2010).

(01) ***Spectrum Sense False Feedback – SSFF.*** A detecção do espectro é a característica fundamental do Rádio Cognitivo, funcionalidade que pode ser realizada por um rádio atomicamente, ou por toda a rede de forma cooperativa. Quando a detecção for realizada

de forma cooperativa, todos os rádios autenticados pertencentes à RRC, em determinados momentos, têm a função de receber as informações da disponibilidade dos canais licenciados livres dos outros rádios (quando então são denominados de centro de fusão de dados). O centro de fusão de dados, após o processamento dos dados recebidos, tomará a decisão de ocupar ou não a FLL. Entretanto, um atacante pode emitir informações falsas sobre o espectro local, por exemplo, informando ao centro de fusão dos dados que determinada frequência está sendo utilizada/não utilizada pelo usuário principal, quando na verdade a frequência está livre/ocupada. Isso faz com que o centro de fusão de dados realize o processamento e a conseqüente tomada de decisão quanto à utilização da FLL de forma incorreta. (NHAN 2009).

(02) ***Primary User Emulation Attack*** – ***PUE.*** Do ponto de vista de (PARK 2008), é o ataque onde um rádio malicioso tenta personificar a figura do usuário primário, transmitindo nas faixas livres nos períodos em que os rádios cognitivos poderiam utilizá-las, causando com isso a negação de serviço na rede secundária. Da mesma forma, o atacante pode transmitir nas frequências livres no momento em que o usuário principal fosse utilizá-la, causando a interferência na rede primária.

(03) ***Objective Function Attack*** – ***OFA.*** Uma Rede Cognitiva possui vários parâmetros que são calculados para melhoria do desempenho da rede. Os algoritmos utilizados para esse fim modificam tais parâmetros em tempo real baseados nas observações colhidas no meio, além das informações fornecidas pelos outros rádios, com a finalidade de otimização das transmissões da rede, entre eles: frequência, largura de banda, potência de transmissão, tipo da modulação, taxa de codificação, protocolo de acesso aos canais, tipo de cifragem, tipo da autenticação, código de integridade das mensagens e tamanho dos frames (CLANCY 2008). A inserção de dados forjados influencia nas decisões tomadas pelos algoritmos de ajuste dos parâmetros de manutenção e controle, podendo provocar o colapso da rede.

(04) ***Common Control Data Attack*** – ***CCA.*** A troca de informações de controle, necessária a manutenção a rede, realizada entre a estação base e os rádios da rede, no caso de uma rede infraestruturada, ou entre os próprios rádios, em uma rede descentralizada é/pode ser realizada por meio de um canal dedicado a esse fim, denominado de canal comum de controle. Um atacante pode bloquear toda uma rede caso consiga interromper todas as comunicações que utilizem o supracitado canal. (SAFDAE 2009).

(05) ***Lion Attack - LA*** (LEON 2010) - Baseia-se no ataque de *cross-layer*, i.e., quando um atacante provoca o colapso de uma determinada camada protocolar por meio de um ataque a outra camada. Por exemplo, esse ataque pode provocar a retransmissão de pacotes TCP por

meio de um *Primary User Emulation Attack*. O atacante provoca a desconexão da comunicação do rádio por meio do *PUE*, que obrigatoriamente deverá mudar de frequência de transmissão, aumentando por isso a latência de transmissão. Em conseqüência, há a verificação das camadas protocolares superiores da não entrega dos pacotes TCP, provocando a tentativa de retransmissão dos mesmos, causando, com isso, uma redução da produção do TCP entregue. Quanto mais longa a duração na troca de frequência, mais drástica pode vir a ser a redução.

2.3 Sistema de Detecção de Ataque/Intrusão

O termo Sistema de Detecção de Ataques (SDA) é uma generalização para um enorme número de soluções propostas para identificar, reduzir e interromper atividades maliciosas definidas como ataques a uma rede de computadores (RICHARDSON 2010), (CERT 2011). Entre elas citamos: os Sistemas de Detecção de Intrusão (BARBOSA 2000), Sistema de Prevenção de Intrusos (RASH 2005), Antivírus (BEIJTLICH 2004) etc.

Os Sistemas de Detecção de Ataques (SDA) são responsáveis por identificar, relatar e combater atividades maliciosas provenientes, tanto de elementos externos quanto de elementos internos ao sistema (BARBOSA 2000; TIMOFTE 2008).

O Modelo Comum de Detecção de Intrusão (*Common Intrusion Detection Framework* – CIDF) sugere uma padronização para os Sistemas de Detecção de Intrusão. Segundo o CIDF (DEBAR *et al.* 1999; BARBOSA 2000; GARCÍA-TEODORO *et al.* 2008), os seguintes componentes são necessários: (i) gerador de eventos (E-BOX); (ii) analisador de eventos (A-BOX); (iii) banco de dados (D-BOX); e (iv) contramedidas (C-BOX), conforme ilustrado a Figura 1.

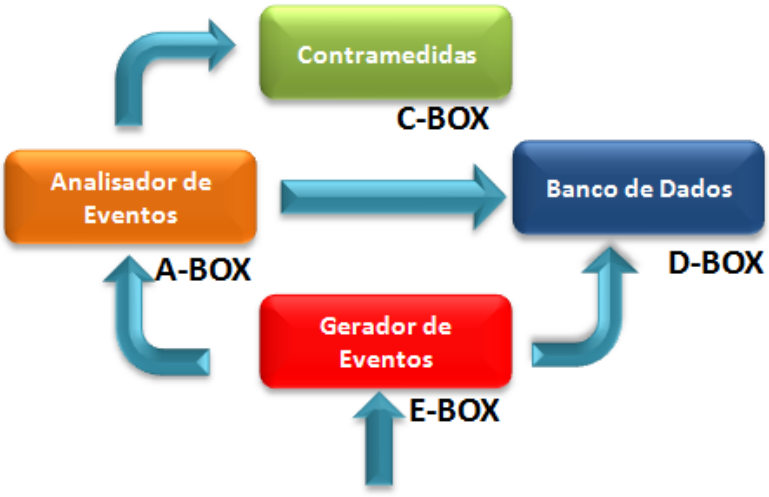


Figura 1. Interação dos componentes do modelo CIDF (BARBOSA 2000).

O componente Gerador de Eventos captura os pacotes da rede e entrega ao componente Analisador de Eventos, para o processamento das informações, e para o componente Banco de Dados, que irá armazenar estas informações para manter um histórico. O componente Analisador de Eventos é o cérebro do sistema de detecção sendo responsável por identificar se as informações que chegaram do componente Gerador de Eventos são ou não um ataque. Este componente também pode armazenar as informações de ataques identificados no componente Banco de Dados. O componente Contramedidas é responsável por receber uma informação do componente Analisador de Eventos avisando que a rede está sob ataque. Este componente pode, por exemplo, tomar diversas ações como comunicar-se com outros Sistemas, acionar alarmes e avisar ao administrador do sistema (BARBOSA 2000).

Segundo (TIMOFTE 2008), a prevenção da intrusão é definida como um processo que realiza a detecção da intrusão e a tentativa de deter possíveis incidentes detectados. Um Sistema deveria, então, ser capaz de identificar possíveis incidentes de segurança, guardar informações sobre estes incidentes, tentar realizar uma ação de forma a parar o incidente e reportá-los ao administrador da rede.

2.3.1 Classificação de um Sistema de Detecção de Ataques

A mesma classificação empregada nos Sistemas de Detecção de Intrusão (DA SILVA 2005; KAUR e SINGH 2010) pode ser empregada para o SDA de acordo com as seguintes características: (i) método de detecção; (ii) comportamento na detecção; (iii) tempo de detecção; (iv) processamento; (v) fonte de auditoria; (vi) local de processamento de dados; e (vii) local da coleta de dados. A Figura 2 ilustra essas características.

Método de detecção: tradicionalmente, é dividido em duas abordagens: a detecção por anomalias (*anomaly detection*), onde o SDA identifica intrusões como um comportamento não-usual que difere do comportamento normal esperado; e a detecção por mau uso (*misuse detection*), onde o SDA observa eventos que combinem com um padrão pré-definido de um ataque conhecido. Uma terceira abordagem, introduzida recentemente por pesquisadores da Universidade da Califórnia (DA SILVA 2005), é a baseada em especificação (*specification-based detection*). Nesta abordagem, a monitoração da execução das aplicações envolve a detecção de desvios de comportamento em relação a estas especificações. Desta forma, esta abordagem combina vantagens das duas abordagens mais antigas.

Comportamento na detecção: indica como o SDA reagirá ao detectar um ataque. Se o SDA apenas gerar alertas, ele será um SDA passivo. Caso ele também possua a capacidade de reagir, ele será considerado um SDA ativo (DA SILVA 2005).

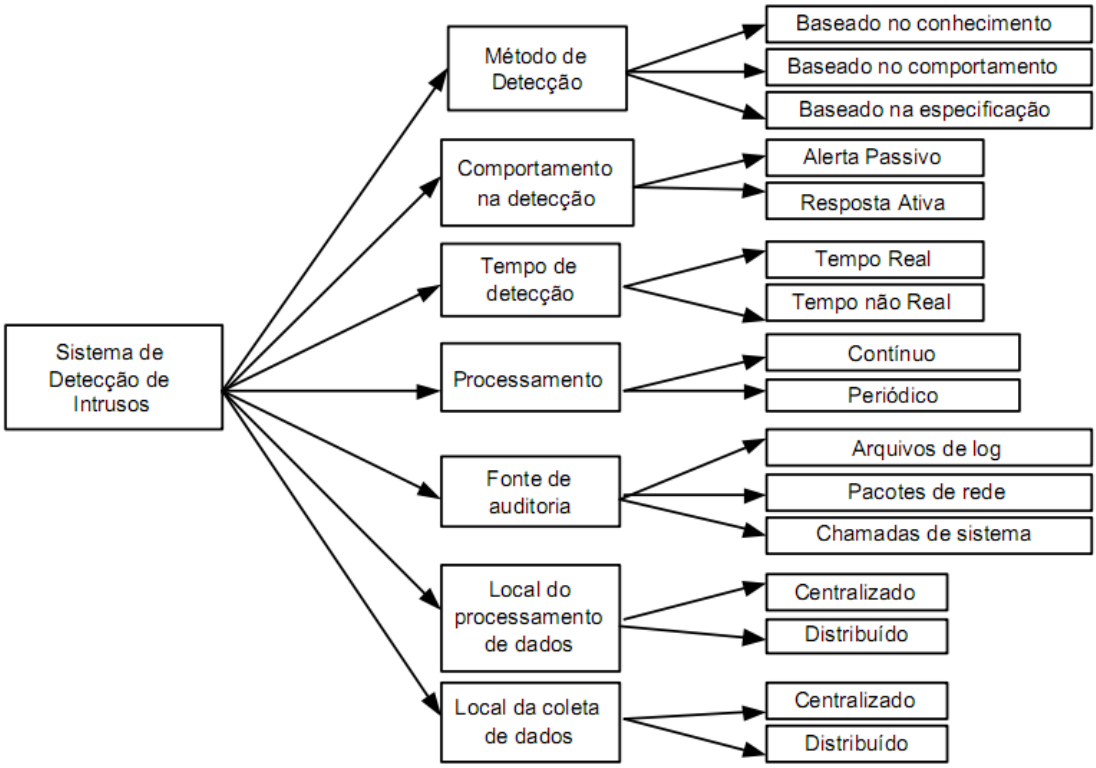


Figura 2. Classificação dos SDA/I (DA SILVA 2005).

Tempo de detecção: indica se a análise dos dados é feita em tempo real ou próximo de tempo real, ou em tempo não real, ou seja, com algum atraso. No caso das RRC é interessante que a detecção seja feita em tempo real, ou próxima do tempo real (DA SILVA 2005).

Processamento: os dados podem ser analisados de forma contínua ou por blocos de dados em um intervalo regular. Este conceito afeta diretamente o tempo de detecção do intruso.

Fonte de auditoria: indica o tipo de dados que o SDA analisa. As fontes podem ser arquivos de *log*, pacotes da rede ou chamadas de sistema.

Local de processamento: a detecção pode ser realizada em um ponto central de coleta de dados ou de forma distribuída.

Coleta de dados: os dados podem ser coletados por um ponto central ou de forma distribuída.

Eficiência dos SDA

Para possibilitar a avaliação dos Sistemas de Detecção de Ataques, são utilizadas algumas métricas que determinam a sua eficiência (SILVA 2009), i;e, falsos positivos (FP), que indicam a quantidade de alarmes falsos; falsos negativos (FN), que indicam uma condição de normalidade quando na verdade está ocorrendo um ataque; verdadeiros positivos (VP), que indicam que está ocorrendo um ataque durante um ataque; e verdadeiros negativos (VN), que indicam uma condição de normalidade quando não está ocorrendo nenhum ataque. Sendo eles:

Completude – Mede a capacidade de um SDA em não deixar de detectar um ataque (Falsos Negativos);

Acurácia – Mede a capacidade do SDA em não gerar alarmes falsos (Falsos Positivos);

Outro aspecto importante na avaliação da eficiência de um SDA está na relação entre os índices de Falsos Positivos e Negativos (Crossover Error Rate – CER). Essa relação de equilíbrio visa balancear as taxas de erros de forma a otimizar tanto a Completude quanto a Acurácia do SDA . O gráfico da Figura 3 ilustra essa relação.

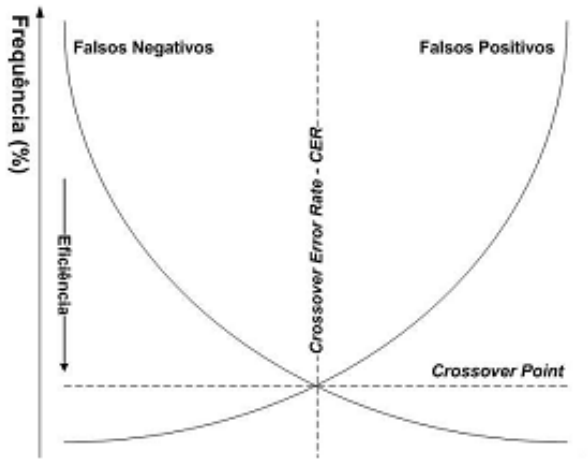


Figura 3. Gráfico representativo do Crossover Error Rate – CER.

O eixo “y” representa a frequência (taxas) em que ocorrem os Falsos Positivos e/ou Negativos. O eixo “x” indica em ordem crescente os níveis de sensibilidade de detecção configurados no SDA. O significado da sensibilidade varia com o tipo de SDA, representando, de uma forma geral, as configurações que tornam o SDA mais rigoroso em suas análises, gerando um maior número de alarmes. Observa-se que quanto mais for incrementado o nível de sensibilidade do SDA, maior será o número de intrusos detectados,

reduzindo o índice de Falsos Negativos. Em contrapartida, nesse caso, o índice de Falsos Positivos também cresce progressivamente à medida que a sensibilidade aumenta, tornando inviável a utilização do SDA. No sentido oposto, quanto menor for a sensibilidade, menor será o índice de Falsos Positivos, ao preço de uma redução brusca nos acertos, ou seja, um aumento exponencial de Falsos Negativos. O ponto ótimo está indicado no gráfico da Figura 3, e é onde há intersecção entre as curvas de Falsos Positivos e Negativos. Nesse ponto, as freqüências se igualam e quanto menor for o valor da freqüência, no ponto de intersecção (*crossover point*), mais eficiente é o SDA.

2.4 Técnicas empregadas para detecção de ataque às RRC

Dentre as diversas técnicas utilizadas na detecção de ataques, a literatura especializada tem dado ênfase a duas técnicas específicas para as RRC: de localização – na detecção de ataques de PUE, e de reputação – utilizados na identificação de ataques SSFF.

2.4.1 Localização

Segundo (HIGHTOWER 2001), as principais técnicas usadas para automatizar os mecanismos de localização são: (i) a Triangulação; (ii) a Análise de Cenários; e (iii) a Proximidade. Tais técnicas podem ser utilizadas de forma isolada ou mesmo de modo combinado.

A técnica de localização por Triangulação utiliza as propriedades geométricas dos triângulos para calcular a posição de objetos. Essa técnica pode, ainda, ser subdividida em duas categorias: Lateralização (*Lateration*), que usa medidas de distâncias (Círculos de Distâncias) e Angulação (*Angulation*), que utiliza medidas angulares (Linhas de Marcações). A Lateralização calcula a posição de um objeto pela medição de sua distância para múltiplas posições de referência. Para possibilitar os cálculos em duas dimensões (plano) é necessária a medição da distância de três pontos não co-lineares, sendo não co-planares com o objeto quando se desejar obter a posição tridimensional.

Existem três abordagens gerais para a obtenção das distâncias requeridas pela técnica da Lateralização, descritas a seguir. (i) Direta (*Direct*) – Medição direta da distância através de um instrumento físico como, por exemplo, uma haste de um robô. (ii) Tempo-de-vôo (*Time-of-flight*) – Medição da distância de um objeto para algum ponto "P", através do tempo que esse objeto leva para ir de sua posição até "P" em uma dada velocidade conhecida. Ou seja, calcula-se a diferença entre o momento da transmissão e o de chegada ao receptor. Exemplos dessa abordagem são os usos de pulso de ultra-som e de luz assim como de ondas

de rádio. (iii) Atenuação – (*Attenuation*) – A regra para o cálculo da distância por atenuação está no fato de que a intensidade de um sinal emitido decresce à medida que a distância do emissor aumenta.

Dada uma função que correlacione a atenuação, a distância por tipo de emissão e pela potência inicial da transmissão, é possível estimar a distância de um objeto até algum ponto "P" pela medição da potência do sinal no receptor, quando esse chega em "P".

A Angulação, a outra categoria da técnica de Triangulação, é similar a Lateralização, exceto que, ao invés de distâncias, são usados ângulos para a determinação da posição de um objeto. Em geral, para a determinação da posição em duas dimensões são necessárias duas medidas de ângulos e uma medida de distância entre os pontos de referência (distância previamente conhecida). A obtenção desses parâmetros, ângulo e distância, se dá com a utilização de múltiplas antenas receptoras, posicionadas a distâncias conhecidas umas das outras.

A segunda técnica de localização, Análises dos Cenários, utiliza as observações do cenário em torno do objeto, a fim de se determinar a sua posição. Essas observações, que podem ser feitas por imagens, por exemplo, são comparadas com uma base de dados que é constantemente atualizada. A partir desse processo de comparação e da evolução das observações pode-se determinar a posição e a direção de determinado objeto (HIGHTOWER 2001).

A terceira e última técnica, Proximidade, determina a posição de dado objeto, quando ele está próximo de uma localização conhecida. A presença do objeto é detectada através de fenômenos físicos com alcance limitado. Um exemplo de aplicação dessa técnica são os detectores de presença, identificadores por códigos de barra, etc.

2.4.2 Reputação

Segundo o dicionário Aurélio (AURÉLIO 2011), reputação é o conceito de que goza uma pessoa por parte do público, da sociedade em que vive. A reputação está intimamente relacionada ao conceito de confiança, que, segundo o mesmo dicionário, é definido como: sentimento de segurança, de certeza daquele que confia na credibilidade de alguém.

Os conceitos de confiança e reputação podem ser utilizados na concepção de mecanismos de suporte a aplicações para que estas possam acessar e fornecer serviços de forma segura.

A confiança é um conceito abrangente que engloba diversas definições (MCKNIGHT 1996). Nesta definição, a confiança é uma medida que quantifica a disposição de uma entidade em depender, em determinada situação e com relativa segurança, de algo ou alguém, assumindo que conseqüências negativas possam ocorrer.

Neste contexto, a confiança incorpora os conceitos de dependência e risco. A dependência é aquela entre pares, ou seja, de clientes em relação a provedores e vice-versa. O risco se refere à probabilidade de ocorrerem conseqüências negativas quando clientes acessam serviços nos provedores ou quando estes prestam serviços aos clientes. O risco aumenta, por exemplo, quando o valor envolvido em uma transação é alto e a probabilidade de ocorrer uma falha não pode ser desconsiderada.

Já o conceito de reputação está atrelado com a confiabilidade, uma vez que a reputação é formada por informações fornecidas por terceiros. A definição proposta em (JOSANG 2007), estabelece que a reputação é um valor resultante daquilo que é atribuído a alguém ou algo. Esta definição é especialmente talhada para ambientes de redes onde é relativamente simples disponibilizar informações fornecidas por terceiros sobre interações realizadas anteriormente por uma determinada entidade. Neste caso, o valor de reputação, computado a partir dessas interações passadas, fornece a terceiros uma avaliação preliminar sobre a confiabilidade da referida entidade em fornecer ou acessar serviços.

Com base nas definições de confiança e reputação fornecidas por este trabalho, pode-se claramente diferenciar os conceitos de reputação e confiança analisando as duas sentenças a seguir (JOSANG 2007):

1. *"Eu confio em você apesar da sua péssima reputação"*
2. *"Eu confio em você por causa da sua boa reputação"*

Assumindo que as duas sentenças compreendem o acesso ou o fornecimento de um mesmo serviço, a primeira sentença representa a utilização de uma informação privilegiada a respeito da entidade a ser avaliada, que pode ter sido obtida através da interação diretamente realizada entre os pares, por exemplo. Já a segunda sentença representa a utilização de informações fornecida por terceiros para a avaliação da entidade, podendo ou não ter sido utilizada uma informação privilegiada no cálculo da reputação.

Os sistemas de reputação (RESNICK 2000) possuem a função de coletar, distribuir e agregar os diversos valores de avaliação sobre os usos de serviços que uma entidade realizou no passado.

Baseado nestes valores de avaliação é calculado um valor de reputação da entidade em questão. Assim, os mecanismos de decisão podem se utilizar desse valor de reputação para decidirem se um novo serviço será ou não fornecido para a mesma entidade. Outra hipótese seria fornecer o serviço com restrições, estabelecendo que tipos de ações serão permitidas na execução do serviço.

Segundo (RESNICK 2000), os sistemas de reputação devem possuir três propriedades:

1. As entidades pertencentes ao sistema devem permanecer longos períodos de tempo conectados a rede;

2. As avaliações sobre as interações realizadas pelas entidades devem estar distribuídas;

3. As avaliações sobre o passado das interações realizadas devem guiar as decisões futuras de novas interações;

A razão das entidades precisarem estar longos períodos de tempo conectados advém do fato de que os sistemas de reputação são dependentes de informações históricas de avaliação do comportamento das entidades pertencentes ao sistema. Para curtos períodos de tempo de conexão, existe uma maior probabilidade de uma determinada entidade, que esteja, por exemplo, acessando um serviço, possuir nenhum histórico de avaliação, inviabilizando o cálculo de sua reputação. Nestes casos, são atribuídos empiricamente valores iniciais de reputação (muito baixos), que são menos confiáveis do que aqueles calculados a partir de valores históricos de avaliação.

A necessidade das informações estarem distribuídas reside em se evitar os problemas inerentes aos sistemas centralizados, tais como um único ponto de falha, entre outros. Uma estratégia de distribuição de informações de avaliação bastante explorada é a utilização de redes *Peer-to-Peer* (P2P) sobreposta à infra-estrutura de rede utilizada. As redes P2P fornecem as primitivas para a troca de mensagens entre os *peers* que podem ser usadas para transportar os valores de reputação. Essas mensagens podem ser distribuídas para todos os *peers* ou somente para parte deles, denominados Super-Nós.

A terceira propriedade determina o uso dos valores de reputação na decisão do fornecimento de futuros serviços para as entidades envolvidas no sistema.

Como as avaliações são vitais aos sistemas de reputação e, por conseguinte, para assegurar ou, no mínimo, aumentar o número de avaliações, mecanismos de incentivos de avaliação do uso de serviços devem ser utilizados. Em (HEOTOKIS 2002) e (FELDMAN

2004a) são identificadas três classes de mecanismo de incentivo: baseados em comércio, baseados em reciprocidade e os baseados na generosidade.

O incentivo baseado em comércio caracteriza-se por oferecer alguma vantagem ou compensação àquelas entidades que se disponham a fornecer avaliações de outras entidades. As vantagens incluem esquemas de micro-pagamento (remuneração do *peer* que fornece o recurso) assim como de troca de recursos. Um outro tipo de compensação é o fornecimento, por parte do próprio sistema de reputação, de benefícios para as entidades que forneçam avaliações, como a utilização de um recurso de uma entidade com baixa sobrecarga, por exemplo.

Nos mecanismos de incentivo baseados em reciprocidade, um usuário A fornece um recurso para um usuário B baseado nos recursos que o usuário B já forneceu para o usuário A, ou para outros usuários do sistema. Cada usuário mantém uma base de informações contendo as ações realizadas por outros usuários e usa estas informações para fornecer ou não um recurso. O conjunto de informações sobre o passado de ações de um usuário representa então a reputação deste.

Já os mecanismos de incentivo baseado em generosidade representam uma categoria onde os usuários decidem se contribuirão ou não com o sistema baseados nas contribuições fornecidas por outros usuários. Resultados a partir da utilização de um modelo em (FELDMAN 2004b) demonstram que quando a generosidade empregada pelos usuários no sistema está abaixo de certo limiar, o sistema entra em colapso por causa da grande quantidade de usuários egoístas.

Quanto aos esquemas de armazenamento e distribuição dos valores de reputação calculados, os sistemas de reputação podem ser de dois tipos: centralizado ou distribuído. Nos sistemas de reputação centralizados, existe a presença de uma entidade central que coleta os valores de avaliação sobre as transações realizadas entre as entidades e distribui os valores de reputação baseados nas requisições dos mesmos. Como exemplo, o site (EBAY 2007) utiliza um sistema de reputação centralizado de forma a fornecer valores de confiabilidade sobre as transações eletrônicas realizadas pelos usuários. Esses sistemas de reputação centralizados são mais simples de serem desenvolvidos, entretanto tais sistemas possuem severos problemas de escalabilidade e de apresentarem um ponto único de falha no sistema, que é o elemento central de armazenamento das avaliações das entidades.

De forma a contornar os problemas apresentados pelos sistemas de reputação centralizados, os distribuídos armazenam as informações de reputação nas próprias entidades (nós da rede, ou, no caso de redes P2P, os *peers*). Para determinada entidade obter o valor de reputação de uma outra entidade, aquela entidade envia requisições para diversos nós. Uma vez de posse dessas avaliações a entidade requisitante procede ao cálculo do valor de reputação.

Apesar dos sistemas de reputação distribuídos minimizarem os problemas encontrados nos sistemas de reputação centralizados, tais sistemas são mais complexos de ser construir. Por exemplo, no desenvolvimento do protocolo de comunicação para a troca de mensagens de avaliação, deve se ter o cuidado de considerar, entre outros aspectos, as confiabilidades dos nós que fornecem as avaliações.

Independente da arquitetura utilizada no sistema de reputação ser centralizada ou distribuída, a literatura apresenta diversos métodos para o cálculo da reputação final de uma entidade (JOSANG 2007). A forma mais simples de cálculo da reputação é a soma de todos os valores de avaliação obtidos dos nós da rede. Este método pode ser melhorado através do cálculo da média simples ou média ponderada dos valores de avaliação.

Além dos métodos de soma e média que podem ser utilizados, diferentes trabalhos apresentam métodos teóricos para o cálculo da reputação, como a utilização de Sistemas Bayesianos (JOSANG 2002) e (WITHBY 2000), Modelos Discretos de Cálculo da Confiança (*Discrete Trust Models*) (ABDUL-RAHMAN 2000), Lógica Nebulosa (SONG 2005), entre outros (JOSANG 2007).

2.5 Função Utilidade

Segundo (LOPES 2008), a Teoria da Utilidade com múltiplos atributos, por definição, envolve uma tomada de decisão que escolhe uma entre um número de alternativas baseadas em dois ou mais objetivos. Os dois métodos predominantes de análise de alternativas são as formas aditiva (CLEMEN 2001) e multiplicativa (KEENEY 1999). Quando os atributos do modelo são puramente independentes, utiliza-se a forma aditiva. Se a condição de independência entre os atributos não é satisfeita, faz-se necessária a utilização da forma multiplicativa para agregar as funções de utilidade de cada atributo, expurgando a dependência entre eles.

A Função de Utilidade Aditiva é composta por dois tipos diferentes de elementos: escalas individuais de atributos e pesos correspondentes a cada atributo. Existem vários

métodos para se quantificar esses elementos, um dos mais utilizados é o método *Swing Weighting*. Durante tal processo: definem-se os objetivos e a escala de atributos, classificam-se as alternativas em cada escala de atributos, acrescentam-se os pesos e avaliam-se todas as informações juntas para se obter uma comparação completa. Uma importante fase da estruturação do processo de análise é entender os objetivos. Deve ser enfatizada a importância de se identificar os objetivos fundamentais que são as razões essenciais que influenciam no contexto a decisão. Segundo (CLEMEN 2001), existem alguns critérios essenciais para se determinar os objetivos fundamentais e seus atributos:

- os objetivos representados na hierarquia de objetivos fundamentais deve incluir todos os aspectos relevantes da decisão,
- a hierarquia de objetivos deve significar uma representação útil dos objetivos que são importantes para o Decisor (elemento responsável pela tomada de decisão),
- os objetivos fundamentais não devem ser redundantes ou muito relacionados entre si, ou seja, o mesmo objetivo não deve ser repetido na hierarquia,
- de acordo com a possibilidade, os objetivos devem poder ser decompostos, para que o Decisor esteja apto a pensar sobre cada objetivo de forma fácil,
- os objetivos fundamentais devem ser distinguidos uns dos outros,
- a escala de atributos deve ser operacional. É necessário encontrar um caminho fácil de se mensurar a performance das alternativas.Segue a forma geral do modelo aditivo (CLEMEN 2001):

$$U(x_1.....x_i) = k_1U_1(x_1) + ... + k_iU_i(x_i) \quad (1)$$

Onde x_i é o valor do atributo i; U_i é o valor da utilidade do atributo i.e.; $0 \leq k \leq 1$ são as constantes de peso para os *i* atributos.

2.6. Algoritmo Genético

Segundo (LACERDA 1999), Algoritmos Genéticos (AGs) são métodos de otimização e busca, inspirados nos mecanismos de evolução de populações de seres vivos, e são implementados como uma simulação de computador em que uma população de representações abstratas de solução é selecionada em busca de soluções melhores. A evolução geralmente se inicia a partir de um conjunto de soluções criado aleatoriamente e é realizada por meio de gerações. A cada geração, a adaptação de cada solução na população é avaliada, alguns indivíduos são selecionados para a próxima geração e recombinados ou mutados para

formar uma nova população. A nova população então é utilizada como entrada para a próxima iteração do algoritmo.

Entre as várias utilizações de tais algoritmos, podemos empregá-lo para atribuição de pesos ponderados a conjuntos matemáticos, cuja otimização consiste em achar a solução que corresponda ao ponto de máximo ou de mínimo para uma determinada função.

Considerando-se, por exemplo, uma função $f_{(x)}$ composta de k elementos a serem maximizados. A cada um dos x_k elementos é atribuído um peso por meio da criação de j vetores de pesos, definidos como **cromossomos** (Equação 2).

$$f_{(x)} = j(x_1) + \ldots + j(x_k) \tag{2}$$

Cada cromossomo possuirá j posições, um para cada conjunto de elementos k. Cada posição [j,k] conterá um número real no intervalo de [0,1], escolhidos de forma randômica, que representará o conjunto de elementos chamados de genes (Tabela 1)**.**

Tabela 1 – Representação dos cromossomos

		Elemento x_k do cromossoma j			
		x_1	x_2	...	x_k
j cromossomos	1	gene j - x_1	gene j – x_2	...	gene j - x_k
	2	gene j - x_1	gene j – x_2	...	gene j - x_k
	.	.	.	.	.
	.	.	.	.	.
	.	.	.	.	.
	j	gene j - x_1	gene j – x_2		gene j - x_k

Por exemplo, observamos na Tabela 2 uma possível representação da Tabela 1 após a escolha randômica dos valores de cada **gene** j- x_k do cromossoma j, considerando-se $k = 3$ e $j = 4$.

Tabela 2 – Exemplo da representação da escolha randômica de um cromossomo

		Elemento x_k do cromossoma j			
		x_1	x_2	x_3	Σx_k
j cromossomos	1	0.32	0.44	0,24	1
	2	0,27	0.11	0.62	1
	3	0.12	0,57	0.31	1
	4	0.48	0.02	0.50	1

Os ***j*** cromossomos, definidos randomicamente no início do processo de atribuição de pesos, formam então a primeira geração da população que será utilizada nessa etapa. Cada cromossomo será processado um a um para a avaliação do seu desempenho.

O processamento é realizado da seguinte forma: o cromossomo ***j***(**gene**$_1$, **gene**$_2$,...,**gene**$_k$), é analisado por meio da fórmula de evolução do algoritmo genético (***fitness***) do cromossomo, Equação 3, (LACERDA 1999).

$$fitness = \frac{Total - FP - 2 * FN}{Total} \quad (3)$$

Onde: Total= Total de dados analisados, FP= Falsos Positivos e FN= Falsos Negativos.

Após o cálculo do *fitness* dos *j* cromossomos da primeira geração da população, inicia-se o processo evolutivo do algoritmo genético. A evolução da população e realizada por meio de seleção, cruzamento e mutação dos cromossomos.

O Método mais utilizado na fase de seleção é o Método da Roleta (*roulette wheel*) (MATHEW 2002). No método da roleta, cada cromossomo é representado proporcionalmente por seu *fitness* comparado ao somatório das aptidões, Equação 3, de todos os cromossomos da população. Um valor aleatório é gerado e o cromossomo correspondente na roleta é selecionado para gerar descendentes. O número de cromossomos selecionados é igual ao tamanho original da população.

O método é formalizado da seguinte forma: (i) o *fitness* de todos os cromossomos é somado (T*f*); (ii) é gerado um número aleatório n: 0<=n<=T*f*; (iii) seleciona-se o cromossomo cujo *fitness* somado aos *fitnesses* dos cromossomos precedentes é igual ou maior que n. Observe o exemplo na tabela 3, o *fitness* do cromossomo 01 é 8, e do cromossomo 02 é 2, logo o somatório dos T*f* é 10, e assim sucessivamente.

Tabela 3 – Método da Roleta

Cromossomo	**01**	**02**	**03**	**04**	**. . .**	**27**	**28**	**29**	**30**
Fitness	8	2	4	17	**. . .**	5	12	10	3
∑T*f*	8	10	14	31	**. . .**	100	112	122	125

Após a distribuição e cálculo do somatório dos *fitnesses* (T*f*), um número aleatório é criado e há a escolha do cromossomo.

Tabela 4 – Rodando a Roleta

Número Aleatório n	32	104	8	14	. . .	112	9	124
Cromossomo Escolhido	**04**	**27**	**01**	**03**	**. . .**	**28**	**01**	**30**

No exemplo da tabela 4, o número aleatório 32 é maior que o somatório acumulado do cromossomo 04 que é 31, tabela 3, logo o cromossomo escolhido, nesse caso é o número 04.

O método da roleta é utilizado para a seleção de dois cromossomos pais, onde então se inicia a fase de cruzamento e mutação.

Cromossomo Pai 04

0,32	0.74	0,21	0.45	**0.20**	**0.98**	**0.78**	**0.56**	0.34	0.65	0.84	0.77

Cromossomo Pai 27

0;33	0.86	0.13	0.78	**0.66**	**0.43**	**0.75**	**0.38**	0.56	0.44	0.94	0.30

Cromossomo Filho 04

0,32	0.74	0,21	0.45	**0.66**	**0.43**	**0.75**	**0.38**	0.34	0.65	0.84	0.77

Cromossomo Filho 27

0;33	0.86	0.13	0.78	**0.20**	**0.98**	**0.78**	**0.56**	0.56	0.44	0.94	0.30

Figura 4– Cruzamento em dois pontos

O cruzamento consiste basicamente em misturar o material genético de dois indivíduos (pais) da população, produzindo dois novos indivíduos (filhos) que herdam características dos pais. É utilizado o cruzamento em dois pontos (*two-point crossover*) (LACERDA 1999), isto é, são definidos aleatoriamente dois pontos de corte nos cromossomos escolhidos na fase de seleção, um dos descendentes fica com a parte central de um dos pais e as partes extremas do outro pai e, vice versa.

Os filhos então substituem as posições ocupadas pelos pais. Na figura 4 é apresentado um exemplo com cromossomos contendo 12 genes onde os pontos de corte são o gene 04 e o gene 08.

A operação de mutação evita a convergência prematura do algoritmo, introduzindo na busca novas regiões do espaço de soluções. Esta consiste em substituir aleatoriamente os valores de alguns genes dos cromossomos. É utilizada a margem de *Y*% da população para a

realização da mutação em um dos cromossomos filhos. Um número aleatório entre 1 e *Y* é calculado, caso o número esteja na faixa entre 1 e *Y/*10, o cromossomo filho sofre a mutação, isto é, um número aleatório entre 1 e *n* é escolhido. Esse número representa a posição do gene a ser substituído e em seguida, outro número real aleatório entre 0 e 1 e calculado e o gene selecionado é substituído por esse novo número. Uma observação importante nesse ponto é: caso o *fitness* do novo cromossomo criado por mutação for menor que o *fitness* do cromossomo que está sofrendo o processo, a mutação não ocorre.

O processo evolutivo do algoritmo é formado de um total de *k* gerações, onde as fases acima citadas (seleção, cruzamento e mutação) são repetidamente realizadas. Ao final de todo o processo o cromossomo (vetor de genes) com o maior *fitness*, isto é, aquele que mais está adaptado ao ambiente de classificação é escolhido como o vetor com os ***k*** valoers ponderados para cada elemento *x* da função em análise.

2.7. Conclusão do Capítulo

Com base nas definições apresentadas, pode-se delinear alguns balizadores usados na seqüência deste trabalho.

Como ataques alvos foram selecionados os ataques de PUE e os ataques de SSFF, dado o destaque encontrado na literatura.

Como os principais mecanismos para detecção de ataques de PUE e de SSFF são respectivamente: os de localização (PARK 2008) e os de reputação (ZHU 2009), tais métodos foram escolhidos como base desta dissertação. Sendo então necessário para a integração de ambos os mecanismos a escolha da **Função Utilidade Aditiva** (FUA). Tal função foi definida como método de integração em virtude desta proceder a analises 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, 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 proposto nesse trabalho.

3 Sistema de Detecção de Ataques para redes de rádios cognitivos

Neste capítulo são descritos: (i) a arquitetura lógica do SDA-COG proposto para RRCs, onde serão apresentados os seus elementos constituintes; (ii) a descrição das fases que definem o fluxo de funcionamento do SDA; e (iii) uma descrição detalhada do funcionamento do SDA proposto.

3.1 Arquitetura Lógica do SDA-COG

A arquitetura lógica do SDA-COG para a rede, mostrada na Figura 5, segue a arquitetura proposta pelo *Common Intrusion Detection Framework* (CIDF) (DEBAR *et al.* 1999; BARBOSA 2000; GARCÍA-TEODORO *et al.* 2008) e consiste dos seguintes componentes:. (i) *AmbienteRC*; (ii) *Localizacao*; (ii) *Reputacao*; (iii) *Gestor*; e (iv) *DecisaoAtaque*, bem como uma Base de Dados (BD).

Os componentes da arquitetura proposta foram agrupados em dois subsistemas: AmbienteRC e Nucleo.

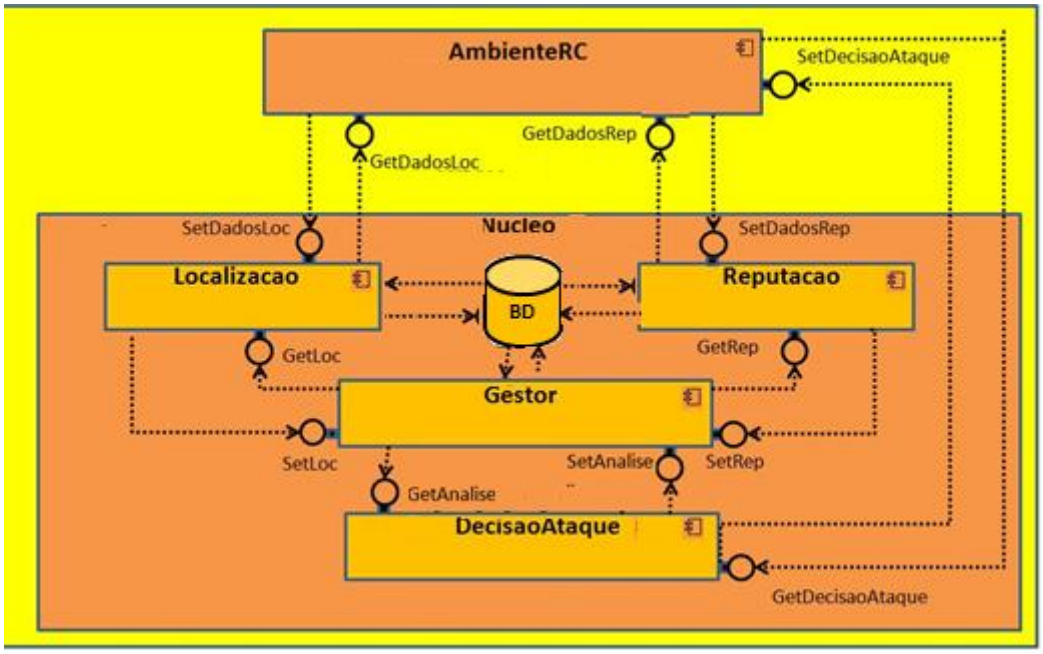


Figura 5. Arquitetura Lógica do SDA-COG.

O subsistema AmbienteRC composto, entre outros, do componente do mesmo nome, *AmbienteRC*, possui as funcionalidades operacionais do rádio, descritas na seção 2.1 Sensoriamento do Espectro, Gerenciamento do Espectro, Mobilidade Espectral e Compartilhamento do Espectro). O componente *AmbienteRC* implementa as interfaces *GetDadosLoc*, *GetDadosRep* e *SetDecisaoAtaques* provendo dados para os componentes

Localizacao, *Reputacao* e *DecisaoAtaque*, respectivamente. A interface *GetDadosLoc* fornece os seguintes parâmetros: frequências e potências captadas para o componente *Localizacao*. A tabela de frequência livre é o parâmetro fornecido pela interface *GetDadosRep* para o componente *Reputacao*. Por fim, a interface *SetDecisaoAtaques* fornece como parâmetros as tabelas recebidas dos rádios vizinhos descritas a seguir: (i) de suspeitos/atacantes de PUE; (ii) de suspeitos/atacantes de SSFF; e de reputação dos rádios. Em suma, o componente *AmbienteRC* é responsável pelo monitoramento e captura dos valores dos parâmetros que servem de insumos básicos para o subsistema Núcleo, tais como a ocupação dos canais licenciados e as informações de frequências livres, que representam as entradas do SDA proposto. Estes parâmetros são utilizados para determinar uma possível invasão.

O subsistema Núcleo é composto pelos componentes: *Localizacao*, *Reputacao*, *Gestor* e *DecisaoAtaque*. Este subsistema tem por finalidade fazer as análises e cálculos necessários para a detecção de ataques pelo SDA-COG.

O Componente *Localizacao* de um RC tem por função calcular o posicionamento dos rádios vizinhos. Para tal, o componente processa as informações sobre as potencias de transmissão dos seus RC vizinhos recebidas do *AmbienteRC* somadas às informações de localização, de modo a determinar a localização desses RCs. Os resultados do cálculo do posicionamento são então enviados ao componente *Gestor* por meio da interface *SetLoc* que prove os dados de localização dos RCs. O componente também provê as tabelas de localização do(s) rádio(s) vizinho(s)/usuário(s) primário(s) para o componente *AmbienteRC* por meio da interface *SetDadosLoc*.

O Componente *Reputacao* é o responsável em rotular, por reputação, os rádios que estão na vizinhança. Ele faz o processamento dos parâmetros e dos dados de reputação classificados pelos outros rádios – analisando determinadas tendências, as quais implicarão em uma rotulação de maior ou menor grau de reputação do rádio vizinho analisado. Este componente implementa a interface *SetRep*, fornecendo as tabelas de classificação das reputações dos rádios vizinhos, as quais são enviadas ao componente *Gestor*. O componente também provê as informações sobre a reputação dos RCs vizinhos para o componente *AmbienteRC* por meio da interface *SetDadosRep*.

O componente *Gestor* é o componente central da arquitetura. É responsável por comandar a análise e pelo disparo dos componentes: *Localizacao* e *Reputacao.* Ele processa todos os parâmetros de entrada – fornecidos pelos componentes *Localizacao* e *Reputacao* acima citados é os envia ao componente *DecisaoAtaque* por meio da interface *GetDecisao.* O

componente também retroalimenta os componentes *Localizacao* e *Reputacao* por meio das interfaces *SetLoc* e *SetRep*, cujos parâmetros são respectivamente: tabelas de localização e tabelas de reputação, armazenadas na Base de Dados (BD).

O componente *DecisaoAtaque* é responsável por analisar as informações fornecidas pelo componente *Gestor* e decidir sobre a tomada de posição do sistema quanto a detecção ou não de um ataque. Este componente implementa a interface *GetAnalise* para o componente *Gestor* e a interface *GetDecisaoAtaque* para o componente *AmbienteRC*, provendo, para ambas as interfaces, as tabelas de suspeitos/atacantes..

3.2 Fases do SDA-COG

O fluxo do funcionamento do SDA proposto é dividido em quatro fases: Inicialização; (ii) Fase de Coleta, (iii) Fase de Análise e (iv) Fase de Decisão. Os procedimentos relativos as fase estão relacionados aos componentes *AmbienteRC*, *Localizacao*, *Reputacao, Gestor* e *DecisaoAtaque* (Figura 6).

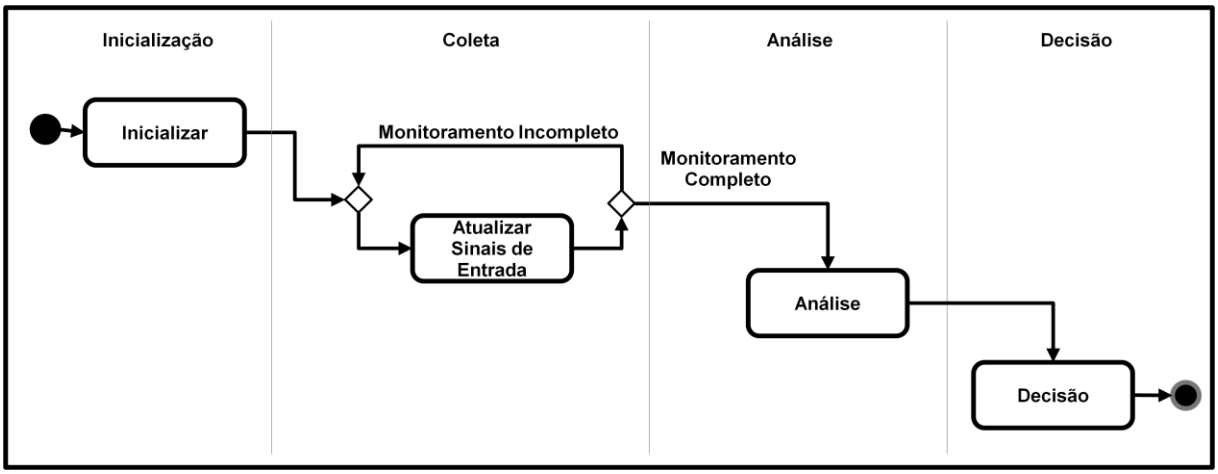


Figura 6. Diagrama de atividades da Arquitetura do SDA-COG.

Conforme ilustra a Figura 6, o SDA-COG inicia sua operação com o bloco *Inicializar*. Este bloco é responsável pela inicialização das variáveis do sistema. Na segunda fase os sinais de entrada são capturados, isto é, frequências licenciadas livres e ocupadas, bem como os mapas de frequências livres recebidas dos RCs vizinhos, conforme ilustrado nos blocos *Atualizar Sinais de Entrada*. Na terceira fase, realizada no bloco *Análise*, os sinais de entrada são analisados pelos componentes *Localizacao*, *Reputacao* e *Gestor* de forma a gerar os valores de localização e de reputação dos RCs. Na quarta e última fase o componente *Decisão* define a existência ou não de um rádio atacante.

Fase de Coleta

É na fase de Coleta que o SDA-COG inicia sua execução. Os sinais a serem usados para a detecção do ataque são coletados pelo componente *AmbienteRC* capturando as informações referentes as frequências licenciadas em uso pelo UP, as frequências licenciadas livres que estão, ou não, sendo utilizadas por algum RC vizinho, bem como os mapas de frequências livres recebidas dos RCs ao alcance de transmissão do RC que realiza a coleta. Nesta fase, os RCs coletam os sinais de entrada da rede, os quais são específicos para cada tipo de ataque. Estes sinais são representados por um conjunto de parâmetros que devem ser monitorados de forma a identificar um ataque. Após o término da Fase de Coleta de Dados, inicia-se a Fase de Análise.

Fase de Análise

A análise é baseada na avaliação dos parâmetros coletados na fase anterior. Os parâmetros referentes aos dados de transmissões captadas, como por exemplo, as potencias dos sinais de transmissões monitorados são analisadas pelo componente *Localizacao*. Enquanto as informações da utilização das frequências licenciadas, recebidas por meio dos mapas de frequências livres, são analisadas pelo componente *Reputacao.* Os cálculos e avaliações são realizados pelos dois componentes acima citados em conjunto com o componente *Gestor* dando início então à quarta e última fase.

Fase de Decisão

A fase de Decisão ocorre no RC e é executada dentro do componente *DecisaoAtaque*, exercendo a funcionalidade de identificar um ataque. Neste componente as informações coletadas e analisadas nas fases anteriores são contabilizadas e classificadas como normais ou um ataque por meio da utilização da função utilidade ponderada pelo algoritmo genético.

3.3. Descrição do SDA-COG.

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

3.3.1 Mecanismo de Localização

Diversas abordagens foram apresentadas no contexto de segurança de rede de rádios cognitivos que utilizam como método de detecção de ataques os mecanismos de localização

dos rádios secundários e do usuário primário (CLANCY 2008), (CLANCY 2009), (LEON 2010).

Foi proposto em (SHRESTHA 2010), uma técnica de localização baseada no cálculo Euclidiano do posicionamento dos rádios da rede bem como da torre de transmissão como método de detecção de PUE. As coordenadas de localização são utilizadas para a análise da localização de cada rádio. 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 (FCC 2009), de que nenhuma alteração na infraestrutura e nas configurações das redes primárias deve ser feita com a finalidade de adaptar-se à nova tecnologia de rádio cognitivo. A presente proposta diferencia-se do trabalho acima proposto, pois, além da análise para a decisão de detecção do ataque ser baseada na potencia de recepção captada dos rádios da rede, não há a necessidade de qualquer informação fornecida pelo usuário primário para a sua consecução.

É descrito em (NEWMAN 2009) uma Rede Neural associada a Mapas auto-organizáveis como método de localização dos rádios. Os classificadores são simulados no MATLAB, inclusive com a inserção de um nó malicioso que, promovendo a transmissão de dados forjados, passando-se por um usuário preliminar, ocasionando a classificação errônea por parte dos rádios cognitivos, e a consequente não transmissão naquelas faixas do espectro. O artigo propõe a minimização de tais ataques por meio da classificação matemática dos sinais detectados. Porém, também foi constatado pelos autores, que a análise de tais características é demasiadamente complexa para ser feita dentro tempo real com as ferramentas comerciais usadas atualmente pelos dispositivos sem fio. Sendo este o diferencia a nossa proposta, pois as análises são realizadas em tempo real e de forma sumária.

Entre as técnicas de localização citadas no capítulo 2, optamos pela utilização da Lateralização, mas especificamente a Atenuação. Tal escolha foi realizada com intuito de utilização das funcionalidades básicas do rádio cognitivo, isto é, o contínuo e ininterrupto processo de monitoramento dos canais de frequência, onde a análise dos sinais recebidos já é realizada pelo próprio rádio.

A proposta descrita em (PARK 2008) especifica uma forma de determinação de ataque de PUE. O trabalho propõe a detecção do nível de energia do sinal emitido, além da

localização dos transmissores. Baseia-se nas seguintes suposições: (i) os transmissores preliminares são torres da tevê com uma posição conhecida fixa e em sua alta potência de transmissão (na escala de centenas de quilowatts), e (ii) os rádios são dispositivos com o poder limitado da transmissão (que varia de miliwatts a alguns watts). Em consequência, a detecção do nível de energia pode definitivamente ser um critério robusto para validar a autenticidade de transmissões preliminares.

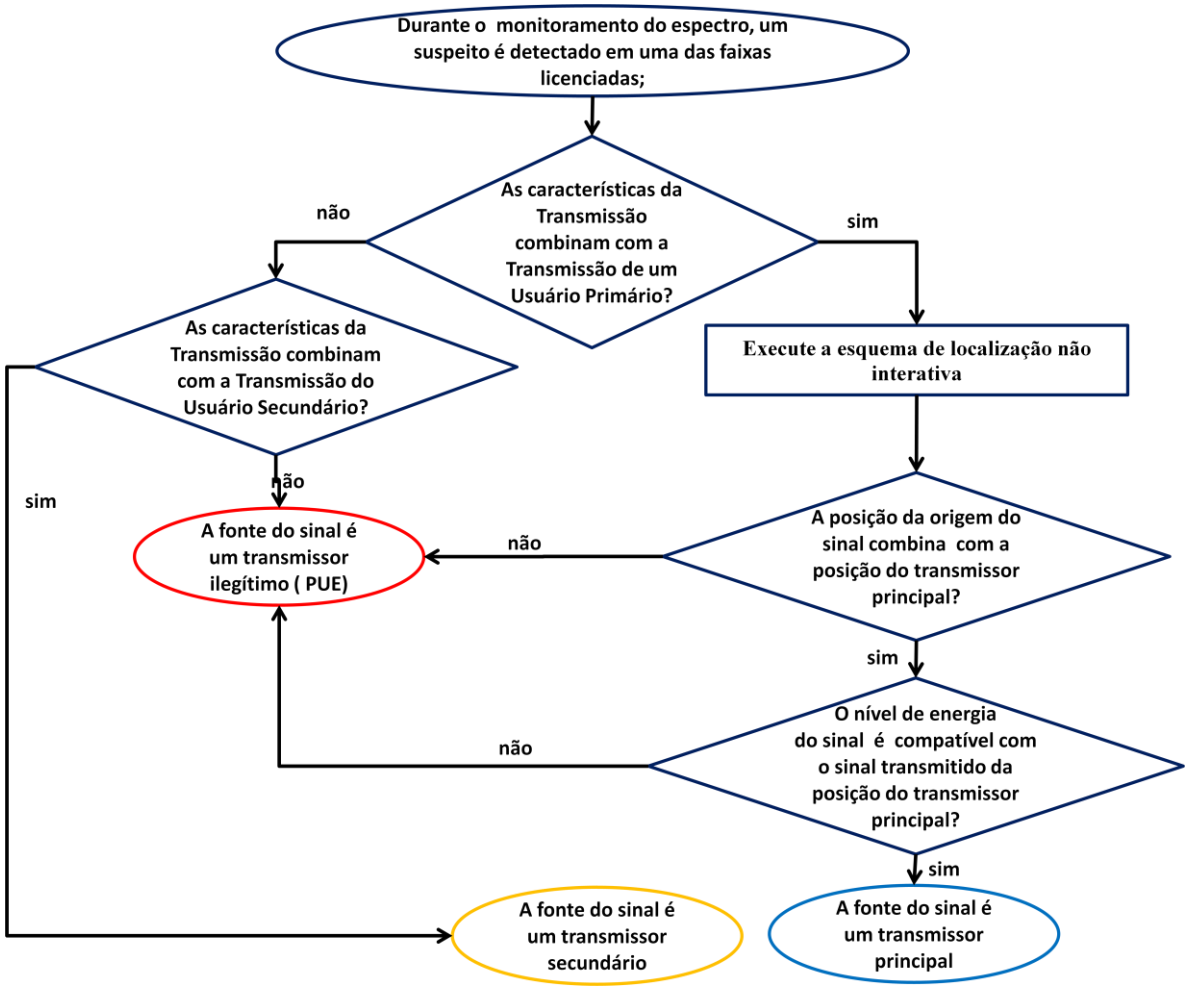


Figura 07. Fluxograma do Mecanismo de Localização (Park 2008).

O mecanismo proposto em (PARK 2008) tem como foco a identificação do ataque de PUE por meio da detecção e análise do nível de energia dos sinais monitorados com a utilização das técnicas de Atenuação por Lateralização. A figura 07 descreve a sequencia de passos utilizados para a detecção de um atacante de PUE.

Para tal é proposto um esquema de análise que verifica se um dado sinal é aquele do transmissor principal, estimando sua posição e observando as suas características de transmissão. Para estimar a posição do transmissor do sinal é empregado um esquema não interativo de localização, isto é, não há qualquer interação dos rádios secundários com o usuário primário.

A localização do Sinal do Transmissor Primário (PST - *primary signal transmitter*) foi definida como não interativa em virtude de duas exigências básicas do paradigma do rádio cognitivo: (i) nenhuma modificação deve ser feita nos usuários primários para acomodar a nova tecnologia, e, em decorrência disso; (ii) não pode haver qualquer tipo de interação entre os rádios cognitivos com os usuários primários. Devendo então ser utilizado um esquema de localização que não realize qualquer tipo de comunicação entre os dois usuários: primário e secundário.

O esquema de localização coleta em tempo real a Intensidade dos Sinais Recebidos (RSS - *Received Signal Strength*). Sendo o RSS nada mais que a medida de potência do sinal recebido. O esquema da verificação do transmissor inclui três etapas: (i) verificação de características do sinal; (ii) medida do nível de energia recebido do sinal**;** e (iii) a localização do sinal fonte.

A ideia básica do sistema de localização proposto usa o fato de que o valor de RSS diminui tipicamente com o aumento da distância entre o transmissor do sinal e o receptor (HE 2003). O modelo estatístico que foi utilizado em (PARK 2008) para modelar o comportamento da propagação do sinal pode ser encontrado em (ROOS 2002), e nesse modelo, o cálculo do RSS previsto em decibéis é dado por:

$$\mu = \rho + \beta_0 + \beta_1 \ln s \tag{4}$$

Onde: (*i*) s representa a distância entre o transmissor e o receptor; (*ii*) ρ é a potencia transmitida em decibéis, e; (*iii*) β_0 e β_1 são os parâmetros constantes que precisam ser calibrados para o ambiente a ser analisado. Enfatiza-se que esta é a calibração em ambientes externos, pois, nenhuma calibração em ambientes internos é exigida (ROOS 2002). Na calibração externa, há a necessidade do ajuste dos parâmetros relativos ao ambiente (por exemplo, rural, urbano, etc.).

Neste trabalho usaremos o modelo estatístico (PARK 2008), dado as suas boas propriedades anteriormente apresentadas, adaptado para áreas urbanas. Para isso o modelo

original foi substituído pelo proposto em (HATA 1982), que contextualiza o cenário de grandes cidades (área urbana) e 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 RRC. O modelo (HATA 1982) para áreas urbanas é descrito como:

$$\Pr = \frac{Pt * Gr * Gt}{L} \tag{5}$$

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

$$a(h_{\mathrm{Re}\,f}) = 3{,}2[\ell og(11{,}75h_{\mathrm{Re}\,f})]^2 - 4{,}97) \tag{7}$$

Onde: Na Equação 5: *Pt* e *Pr* são as potencias de transmissão e recepção; *Gt* e *Gr* são os ganhos das antenas transmissoras e receptoras, respectivamente, e; *L* é a perda no percurso, e; nas Equações 6 e 7: *f* 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; $h_{\mathrm{R}ef}$ é a altura efetiva da antena receptora de 1 a 10 m, e *a* é uma função de $h_{\mathrm{R}ef}$ que expressa o fator de correção da altura efetiva da receptora

Por fim, as funcionalidades do mecanismo de localização estão contidas no componente *Localizacao*, capítulo 3.1.

3.3.2. Mecanismo de Reputação

A detecção cooperativa do espectro (AKYILDIZ 2006) é um dos mais eficientes métodos para que um usuário secundário defina quais faixas licenciadas do espectro estão livres ou estão ocupadas pelas transmissões do usuário primário, para que então, possa fazer uso, ou não, de tais faixas.

A literatura especializada (GANESAN 2005), (MISHRA 2005), (SHANKAR 2005), (WILD 2005), utiliza como referencia, em relação à segurança dos rádios cognitivos, àqueles mecanismos que classificam a reputação baseados nas informações quanto ao sensoriamento colaborativo e cooperativo das frequências licenciadas livres.

O mecanismo de reputação com ênfase na detecção de ataque SSFF foi mencionado em (MISHRA 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. Incluindo-se aí a posição da estação base primária, bem como posicionamento de todos os rádios - informação esta, que nem sempre é possível se ter. Em virtude disso, o método torna-se impróprio para a sua utilização em redes móveis. Em (CABRIC 2004), foi proposto um algoritmo para fusão de dados e teste para detecção de dados falsificados (inclusive para redes móveis), sem a necessidade do conhecimento prévio da localização dos elementos da rede. Porém, o esquema proposto de detecção é extremamente vulnerável a ruídos e a interferências, e não faz, na fase de detecção, a distinção entre sinais modulados, ruídos e interferências. A abordagem proposta se diferencia destes trabalhos em virtude de possuir um mecanismo de decisão baseado na análise do grau de reputação de cada rádio.

Com base no acima exposto, definimos como fonte de nosso mecanismo, o trabalho referencia proposto em (ZHU 2009), que tem como foco um esquema de identificação de ataques de SSFF (LEON 2010). Tal identificação é realizada por meio da análise e classificação ponderada da reputação e da credibilidade dos rádios da RRC com base na detecção cooperativa.

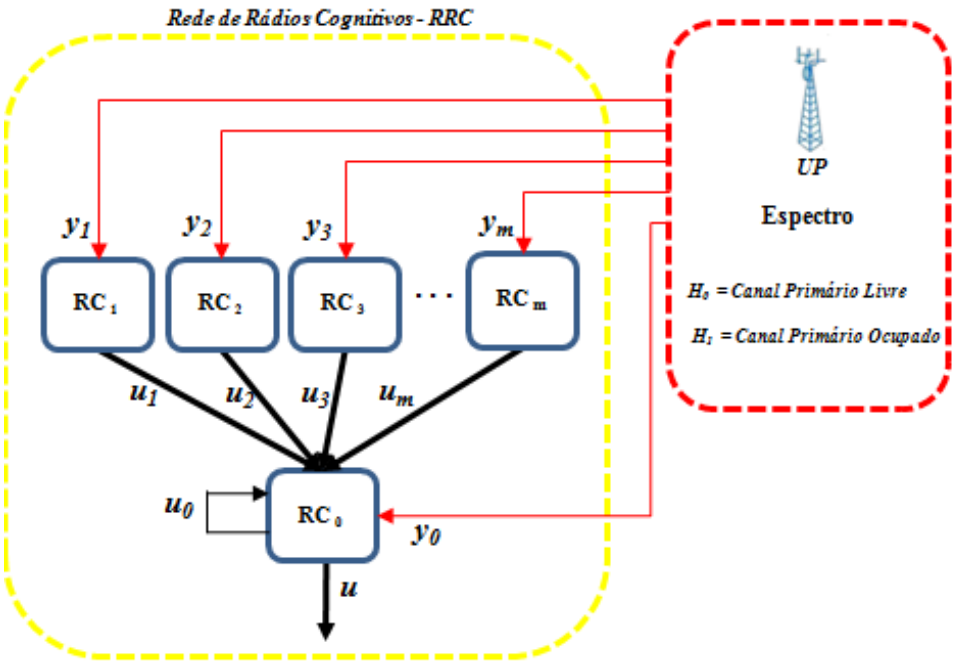


Figura 8 – Modelo Clássico de Fusão de dados

A Figura 8 demonstra um modelo clássico de fusão dos dados utilizado como base para a detecção de frequências licenciadas livres de forma cooperativa. 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. O centro de fusão poderá ser qualquer um dos RCs que necessitem utilizar os canais licenciados livres em um tempo determinado (Δt). Em nosso exemplo é representado pelo rádio RC_0. Na RRC, cada rádio da rede mantém históricos de avaliações geradas a partir de suas experiências com outros rádios. Uma avaliação é uma nota dada pelo RC 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" (SILVA 2007).

As informações recebidas pelo centro de fusão de dados (RC_0) são definidas como u_i , sendo i – 0,1,2,3,...m, dos rádios cognitivos vizinhos (RC_i), quanto aos canais licenciados livres ($\mathbf{H_0}$), e os canais licenciados ocupados pelas transmissões do usuário primário ($\mathbf{H_1}$). Sendo u_i =0 ou u_i =1, caso a decisão do RC_i seja $\mathbf{H_0}$ ou $\mathbf{H_1}$ respectivamente. Tais informações tem como base a percepção que cada RC_i tem de seus monitoramentos do espectro, e definidas como y_i.

Cada u_i recebida por RC_0 do RC_i 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, $\mathbf{H_1}$, e u = 0 que o canal está livre, $\mathbf{H_0}$.

Entretanto, caso algum rádio, ou por defeito, ou por "agir" de forma maliciosa, relate dados de detecção de forma incorreta ao centro de fusão, poderá comprometer o funcionamento da rede como um todo.

Como podemos observar na tabela 5, as informações binárias de u_i **H(0,0)** e u_i **H(1,1)**, são coincidentes quanto à ocupação do espectro. Porém u_i **H(0,1)** e u_i **H(1,0),** em caso de informações transmitidas ao centro de fusão de forma maliciosa, configuram, de uma forma geral, ataques definidos com SSFF.

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, (*ii*) sempre-ocupado e (*iii*) sempre-falso (ZHU 2009), (*i*) O ataque sempre-livre, u_i H(0,1), sempre transmite a informação de que o canal licenciado está livre, configurando

um Falso Negativo (FN) caso o canal esteja sendo ocupado pelo usuário principal. (*ii*) Ao contrário, o ataque sempre-ocupado, u_i H(1,0), sempre transmite a informação de que o canal licenciado está ocupado, ocorrendo um Falso Positivo (FP), quando o mesmo está livre. (*iii*). Por fim temos o ataque de sempre-falso, u_i H(0,1) ou u_i H(1,0), onde o rádio malicioso sempre transmite o inverso da realidade do canal, isto é, livre quando ocupado e ocupado quando livre, configurando hora o FN hora o FP.

Tabela 5 – Análise das informações u_i do RC_i quanto à ocupação do espectro

u_i	H	Informação do RC_i	Realidade do Espectro	Interpretação de u_i
0	**0**	Canal Licenciado Livre - $\boldsymbol{u_0}$	Canal Licenciado Livre - $\mathbf{H_0}$	Verdadeiro negativo – **VN**
0	**1**	Canal Licenciado Livre - $\boldsymbol{u_0}$	Canal Licenciado Ocupado - $\mathbf{H_1}$	Falso negativo – **FN**
1	**0**	Canal Licenciado Ocupado-$\boldsymbol{u_1}$	Canal Licenciado Livre - $\mathbf{H_0}$	Falso Positivo – **FP**
1	**1**	Canal Licenciado Ocupado- $\boldsymbol{u_1}$	Canal Licenciado Ocupado - $\mathbf{H_1}$	Verdadeiro Positivo – **VP**

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

Sempre que a informação de um determinado rádio for consistente com a decisão global $\boldsymbol{u}$, isto é, a informação final processada pelo $\boldsymbol{RC_0}$, seu crédito será aumentado por um; se não diminuído por um. Denotando o crédito para o $\boldsymbol{RC_i}$ por $\boldsymbol{C_i}$, o sistema de crédito pode ser representado por:

$$Ci = \begin{cases} Ci + 1, & if \quad u_i = u \\ Ci - 1, & if \quad u_i \neq u \end{cases} \tag{8}$$

C*om* 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 $\boldsymbol{RC_i}$, é normalizado pela média dos créditos do rádio $\boldsymbol{RC_i}$. Denotando-se $\boldsymbol{w_i}$ o peso do $\boldsymbol{RC_i}$, sendo calculado da seguinte forma:

$$w_i = \begin{cases} 0, & if \quad Ci < -g \\ \dfrac{Ci + (-g)}{avg(Ci + g)}, & if \quad Ci > -g \end{cases} \tag{9}$$

Onde: w_i é o peso do RC_i, C_i é o seu crédito; avg (C_i) denota o crédito médio do RC_i , 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 RC_i.

$$W = \sum_{i=0} (-1)^{ui+1} wi, \tag{10}$$

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

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.

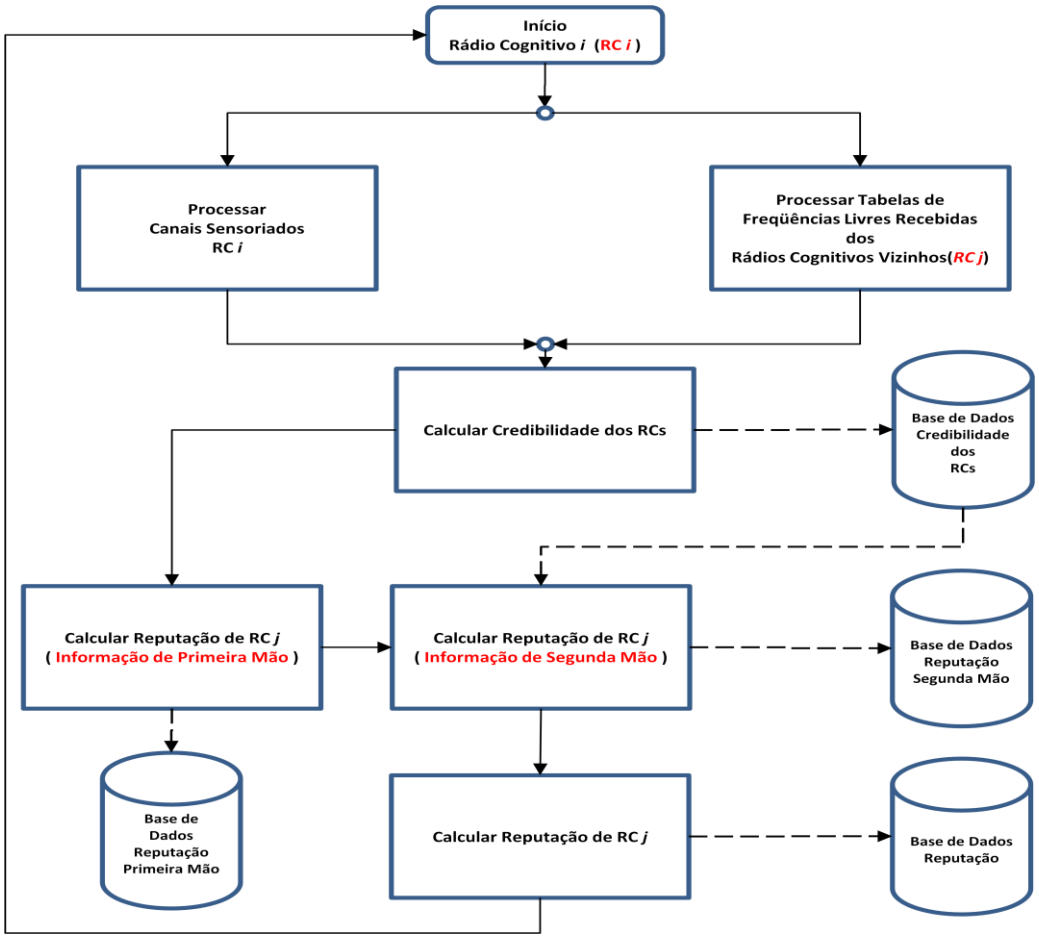


Figura 9. Fluxograma do Mecanismo de Reputação (ZHU 2009).

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. Observamos no fluxograma da figura 09 e no pseudocódigo da figura 10 a sequência de ações realizadas pelo mecanismo de reputação no cálculo e atribuição de créditos ao RCs da rede. As funcionalidades do mecanismo de reputação estão contidas no componente *Reputacao.*

```
1  Inicio
2  | var i = 0 , C_i = 0 , t=0 , m=0 ,
3  |    W = 1 , g =5.51; t_espera=20s , q=15;
4  | Para cada análise de detecção do rádio RC_0 Faça
5  |   | Receber número de RC vizinhos → m
6  |   | Para i até m faça
7  |   |   | Receber u_i do RC_i
8  |   |   | Carregar o vetor Vu[ i ] com u_i do RC_i
9  |   |   | i = i + 1
10 |   | FimPara
11 |   | i = 0;
12 |   | Se Vw [ i ] < -g
13 |   |   | w_i = 0;
14 |   | FimSe
15 |   |
16 |   | Calcular  W = Σ_{i=0}^{m} (-1)^{Vu[i]+1} Vw[i]
17 |   |
18 |   | Se – q<W< q
19 |   |   |   u = 1;
20 |   |   |   aguardar t_espera
21 |   |   | EntãoSe W ≥ q
22 |   |   |   u = 1;
23 |   |   | SeNão Se W ≤ - q
24 |   |   |   u = 0;
25 |   | FimSe
26 |   | Para cada RC_i Faça
27 |   |   | Se Vu[ i ] = u
28 |   |   |   | Vw [ i ] = Vw [ i ] + 1;
29 |   |   |   | SeNão
30 |   |   |   | Vw [ i ] = Vw [ i ] - 1;
31 |   |   | FimSe
32 |   |   | Se Vw [ i ] < -g
33 |   |   |   | Vw [ i ] = 0;
34 |   |   | FimSe
35 |   |   | Se Vw [ i ] > -g
36 |   |   |   | Vw [ i ] = Vw [ i ] + g / avg(Vw [ i ] ) + g;
37 |   |   | FimSE
38 |   | FimPara
39 | FimPara
40 Fim
```

Figura 10. Pseudocódigo do Mecanismo de Reputação (ZHU2009)

3.3.3. Integração dos mecanismos

Os dois mecanismos são combinados no componente *DecisãoAtaque* por meio de uma função utilidade aditiva onde é proposta uma utilidade para cada método além do calculo do peso representativo da importância de cada um deles. Para a integração dos mecanismos descritos nas seções anteriores é usado a Função Utilidade Aditiva (FUA) (CLEMEN 2001) em virtude desta proceder a analise de alternativas com atributos puramente independentes, especificamente o que ocorre quando da combinação dos dois mecanismos aqui utilizados. Podemos observar nas Equações 11, 12 e 13 o mapeamento da Função Utilidade (Equação11) para a Função Detecção $D_{LRC\text{-}i}$ (Equações 12 e 13). Este mapeamento tem apenas a finalidade do enquadramento da nomenclatura dos itens da FUA para o escopo deste trabalho (Tabela 6).

$$U(x_1.....x_i) = k_1U_1(x_1) + ... + k_iU_i(x_i) \quad (11)$$

$$D_{LR\text{-}i} = \gamma L + \omega R \quad (12)$$

$$D_{LR\text{-}i} = (\gamma_1 L_1 + \gamma_2 L_2) + (\omega_1 R_1 + \omega_2 R_2 + \omega_3 R_3) \quad (13)$$

Tabela 6. Mapeamento da FUA para a Função Detecção

Mapeamento	FUA (CLEMEN 2001)	Função Detecção SDA-COG
Função	U	D_{LR}
Peso	k_i Peso do Atributo $_i$	γ Peso do Mecanismo de Localização ω Peso do Mecanismo de Reputação
Pesos	k_1 k_2 k_3 k_4 k_5	γ_1 Peso Mecanismo de Localização – Ataque PUE-S γ_2 Peso Mecanismo de Localização – Ataque PUE-M ω_1 Peso Mecanismo de Reputação – Ataque SSFF-SL ω_2 Peso Mecanismo de Reputação – Ataque SSFF-SO ω_3 Peso Mecanismo de Reputação – Ataque SSFF-SF
$\sum$	$k_1 + k_2 + ... + k_5 = 1$	$\gamma_1 + \gamma_2 + \omega_1 + \omega_2 + \omega_3 = 1$
Utilidade	U_i	1
Atributos	$x_1, x_2, x_3, ..., x_i$	L Mecanismo de Localização R Mecanismo de Reputação
Atributos	x_1 x_2 x_3 x_4 x_5	L_1 Mecanismo de Localização – Ataque PUE-S L_2 Mecanismo de Localização – Ataque PUE-M R_1 Mecanismo de Reputação – Ataque SSFF-SL R_2 Mecanismo de Reputação – Ataque SSFF-SO R_3 Mecanismo de Reputação – Ataque SSFF-SF

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 Detecção, i.e, ao mecanismo de localização e ao mecanismo de reputação, o conceito de algoritmo genético (LACERDA 1999). 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.

Para tal a função DLR*i* (Equação 11) é ponderada por meio da criação de 5 cromossomos – 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.

Cada cromossomo é composto por 30 genes, formando a primeira geração. 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). Foram realizados os cruzamentos, seleções e mutações por um número total de 100 gerações com a finalidade de se calibrar a Função Detecção com a solução que corresponda ao seu ponto máximo de detecção de atques.

Tal integração está contida no componente *DexisaoAtaque*.

3.4. Conclusão do Capítulo

Neste capítulo foi apresentada a arquitetura lógica do sistema proposto com a descrição: dos dois subsistemas que a compõe, os componentes de cada subsistema, as interfaces implementadas por cada um dos componentes, bem como os parâmetros providos por cada um das interfaces.

As fases que compõem o fluxo de funcionamento do sistema foram descritas, i.e., a inicialização, a fase de coleta, a fase de análise e a fase de decisão.

Por fim, o detalhamento, as adaptações e a integração dos mecanismos de localização e de reputação – realizada por meio da função utilidade e calibrada com a utilização do algoritmo genético – foram pormenorizados.

4. Avaliação Experimental do SDA-COG

Para a Avaliação do sistema proposto foram necessárias à criação e modelagem dos elementos constitutivos do sistema da seguinte forma: (i) modelagem da RRC (rede secundária – não licenciada); (ii) modelagem das redes de usuários primários (rede licenciada); (iii) criação dos perfis de comportamento dos seguintes elementos: dos usuários primários; dos usuários secundários; e dos atacantes de: PUE-S, PUE-M, SSFF-SL, SSFF-SO e SSFF-SF; bem como a modelagem dos componentes do SDA-COG propriamente ditos: mecanismo de localização, mecanismo de reputação, mecanismo de gestão e o mecanismo de decisão de ataques. Para tal foi utilizado o MatLab/Simulink como ambiente de simulação.

4.1. Objetivos da Avaliação Experimental

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. Descrição do Cenário

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.

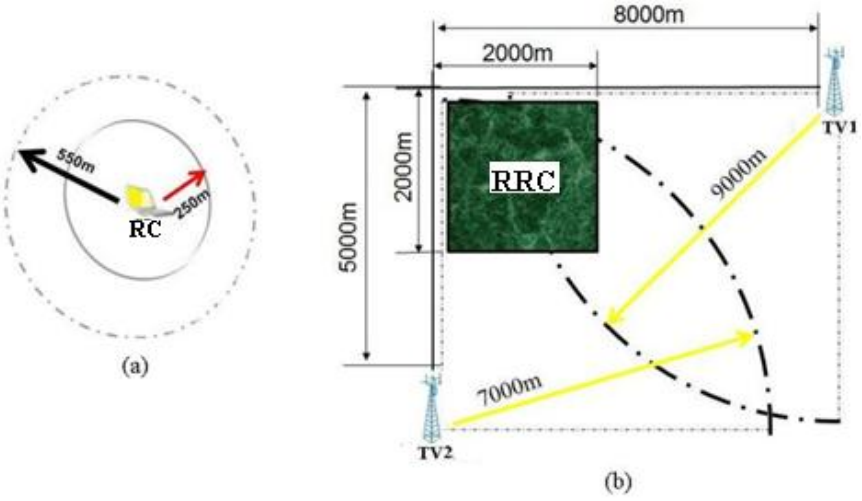


Figura 11. Cenário Utilizado: (a) Raios de Alcance do RC (b) Diagrama da RRC

A RRC foi composta por 300 rádios cognitivos, distribuídos aleatoriamente em uma área quadrada de 2000m; cada RC possui um raio de alcance de transmissão de 250m, com um raio de interferência de 550m, seguindo o modelo proposto em (ROSS 2002) (Figura 11a).

Dois usuários primários (torre de TV 1 e Torre de TV 2) são posicionas à 8000m e 5000m das bordas externas da RRC (Figura 11b). As torres possuem o alcance de transmissão de 9000m e 7000m, respectivamente.

4.3. Simulações e Resultados dos Experimentos

A simulação é dividida em duas fases (Figura 12). A primeira consiste na modelagem e geração da rede (Gerar Cenário). A segunda é constituída de três experimentos: simulação das transmissões (Gerar Transmissões); simulação da detecção de ataques (SDA-COG); e calibração do limiar de aceitabilidade (LA) e do valor do coeficiente de normalização (VCN) (Calibração).

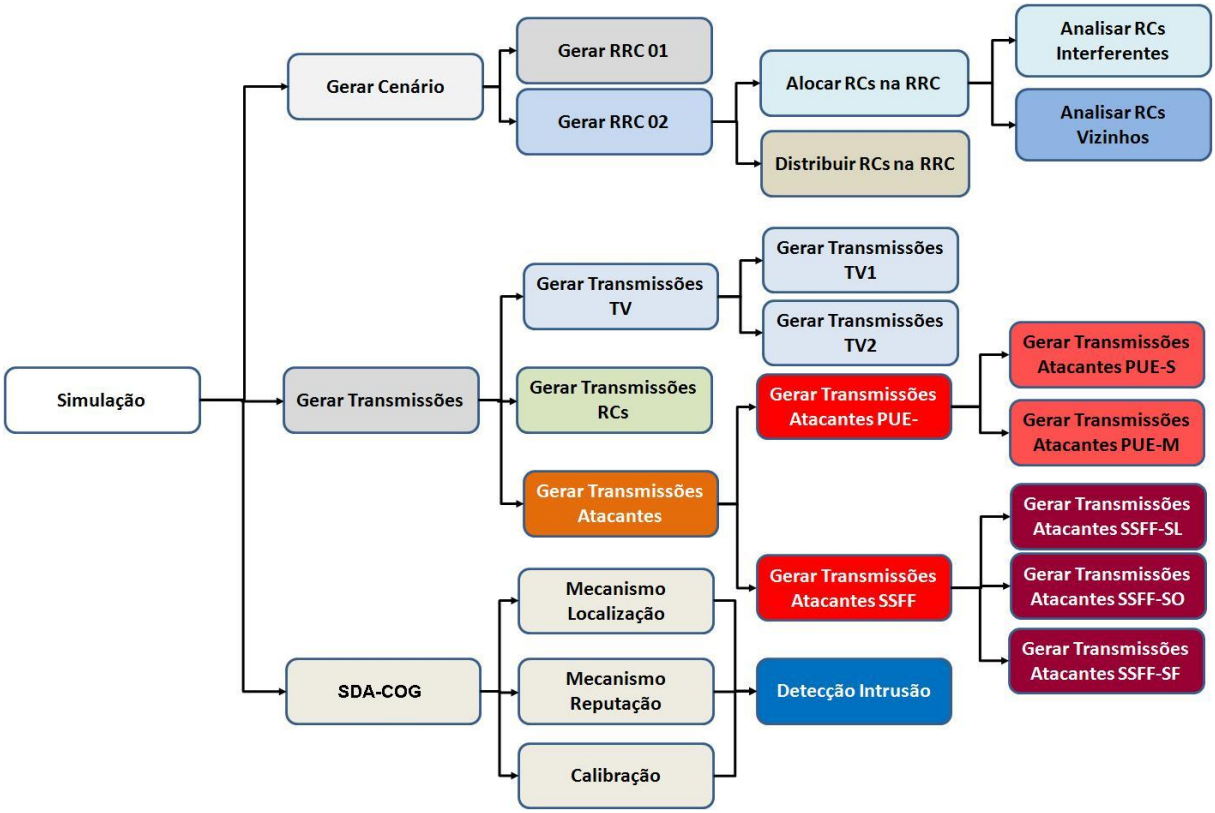


Figura 12. Diagrama de Módulos da Simulação

4.3.1. Geração do Cenário

O módulo Gerar Cenário é responsável pela criação da rede em duas etapas, Gerar RRC 01 e Gerar RRC 02. Na primeira etapa, Gerar RRC 01, a rede é dimensionada seguindo os parâmetros definidos na inicialização, isto é, são definidos os parâmetros (Tabela 7) utilizados para a criação da rede seguindo o proposto em (PARK 2008), Figura 13.

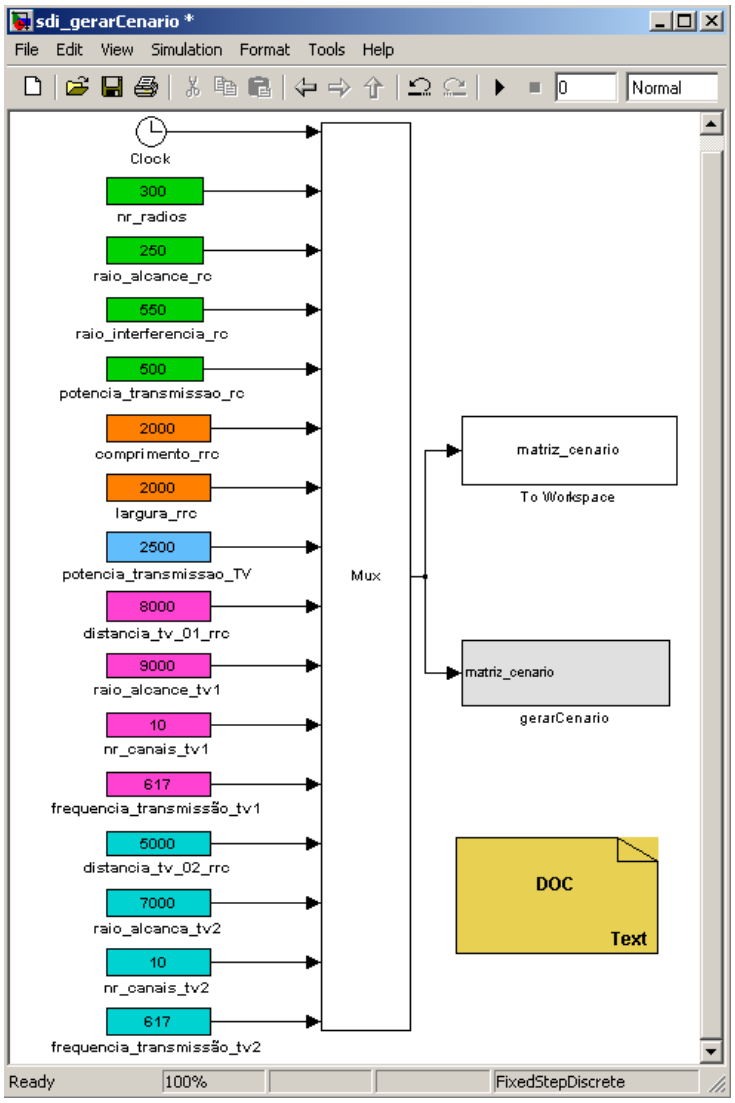


Figura 13 Modelagem do Cenário – Bloco Simulink

Podemos observar na tabela 7 a descrição das métricas e parâmetros utilizados para a geração da rede de rádios cognitivos que foram definidos no processo de inicialização da primeira fase da simulação por meio do bloco Simulink da Figura 13. Obervamos também a modelagem do mapa parcial da rede na Figura 14.

Tabela 7. Descrição dos parâmetros para geração da RRC

Nome da Variável	Descrição	Qtd
nr_radios	Quantidade de rádios Cognitivos da Rede	300 RCs
raio_alcance_rc	Raio de Alcance das transmissão dos Rádios	250 m
raio_interferencia_rc	Raio de Interferência das transmissões dos Rádios	550 m
potencia_transmissao_rc	Potencia de Transmissão dos Rádios Cognitivos	500 mW
largura_rrc	Largura da Rede de Rádios Cognitivos	2000m
comnprimento_rrc	Comprimento da Rede de Rádios Cognitivos	2000m
potencia_transmissao_TV	Potencia de Transmissão das Torres de TV	2500 KW
distancia_tv1_rrc	Distância da Torre de TV 01 à borda da RRC	8000m
raio_alcance_tv1	Raio de Alcance da Torre de TV 01	9000m
nr_canais_tv1	Número de canais da Torre de TV 01	10
frequencia_tv1	Frequencia de transmissão da Torre de TV 01	617 MHz
distancia_tv2_rrc	Distância da Torre de TV 02 à borda da RRC	5000m
raio_alcance_tv2	Raio de Alcance da Torre de TV 02	7000m
nr_canais_tv2	Número de canais da Torre de TV 02	10
frequencia_tv2	Frequencia de transmissão da Torre de TV 02	617 MHz

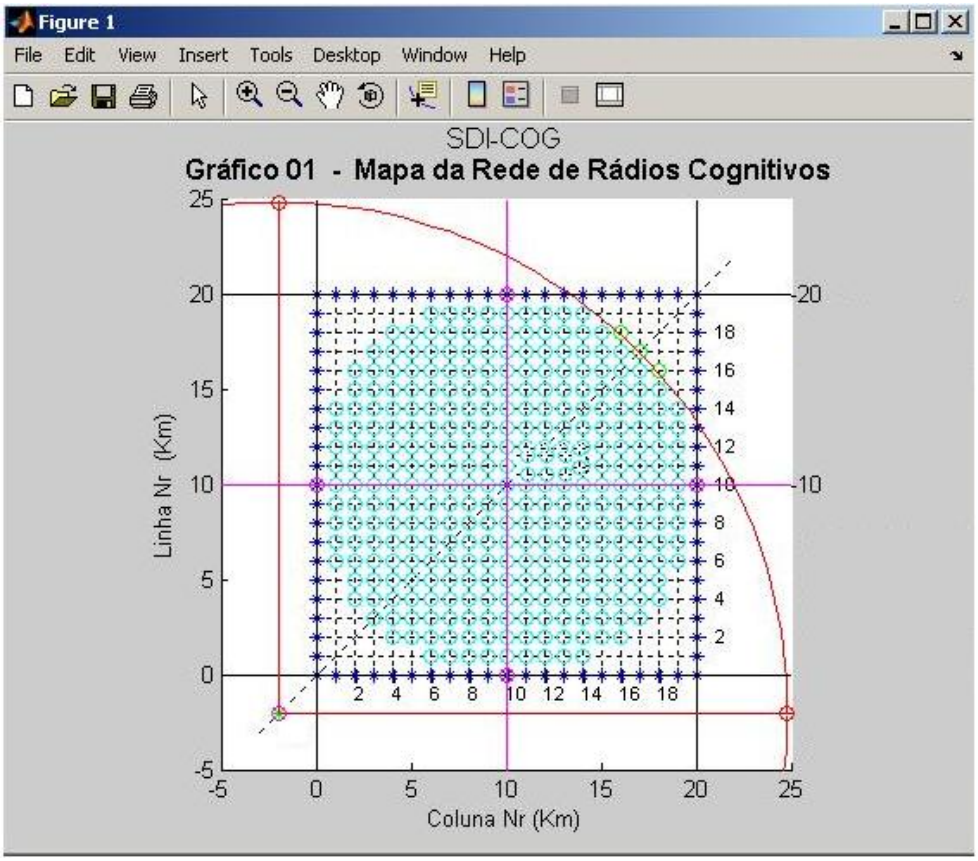


Figura 14. Modelagem da RRC 01

Na segunda etapa, gerar RRC 02, há 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 (GAMERMAN 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 etapa 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. Cada RC reconhece seus rádios vizinhos, isto é, os rádios que estão ao alcance do raio de transmissão do centro do cluster (250m); bem como os RCs que estão em seu raio de interferência (550m), Figura 15. A duas Torres de TV são posicionadas na RRC. A primeira localizada a 8.000 m da RRC com um raio de alcance de 9.000m; a segunda localizada a 5.000m da rede cognitiva possuindo um raio de alcance de 7.000 m.

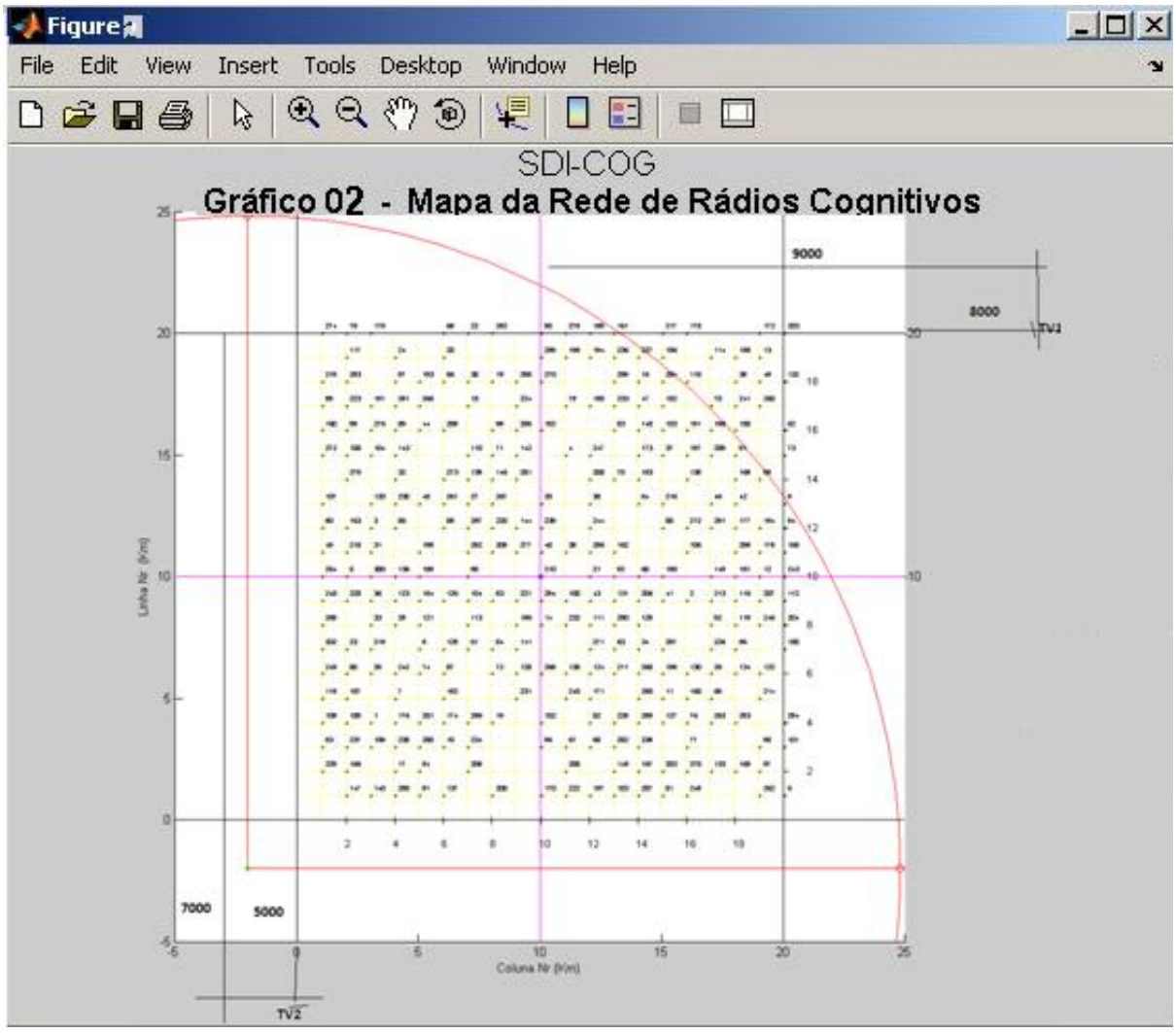


Figura 15. Modelagem da RRC 02

4.3.2. Primeiro Experimento: Simulação das Transmissões

Nesse primeiro experimento as transmissões propriamente ditas, com e sem ataques são simuladas. Como podem ser observados na figura 16, os parâmetros para a simulação (PARK 2008), são modelados. Ambas as torres de TV possuem a altura de 100m; transmitem a frequência de 617 MHz, utilizando 10 canais de frequência, 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.

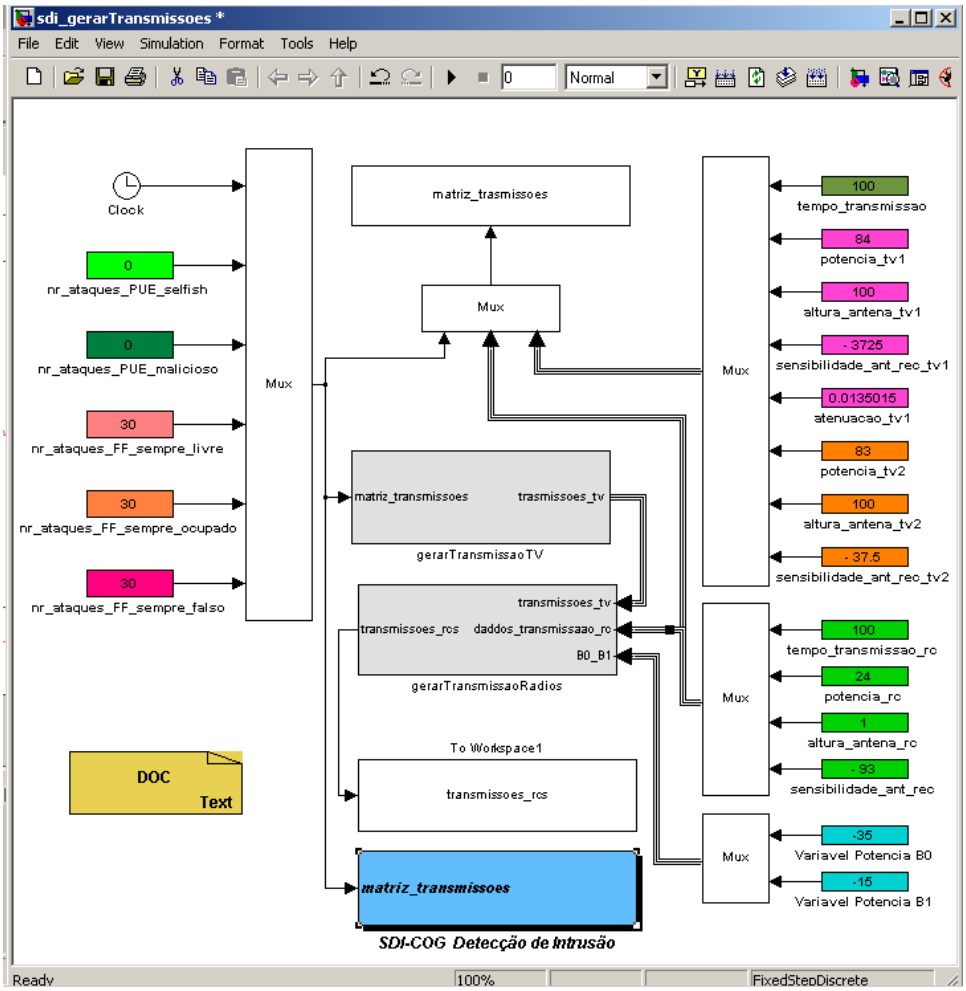


Figura 16. Modelagem das Transmissões para Análise do SDA-COG

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 das duas torres simultaneamente , de apenas uma delas, ou mesmo nenhuma transmissão do usuário primário.

Tabela 8. Descrição dos parâmetros para transmissões das Torres de TV e dos rádios

Nome da Variável	Descrição	Qtd
nr_ataques_PUE_selfish	Quantidade de rádios Cognitivos atuando como atacante de PUE-S	De 0 a 30
nr_ataques_PUE_malicioso	Quantidade de rádios Cognitivos atuando como atacante de PUE-M	De 0 a 30
nr_ataques_FF_sempre_livre	Quantidade de rádios Cognitivos atuando como atacante de SSFF-SL	De 0 a 30
nr_ataques_FF_sempre_ocupado	Quantidade de rádios Cognitivos atuando como atacante de SSFF-SO	De 0 a 30
nr_ataques_FF_sempre_falso	Quantidade de rádios Cognitivos atuando como atacante de SSFF-SF	De 0 a 30
tempo_transmissao	Intervalo de tempo destinado a cada transmissão da TV	100ms
potencia_tv1	Potencia de Transmissão da Torre de TV 01	84 dB
altura_antena_tv1	Altura da Torre de Transmissão - TV 01	100m
sensibilidade_ant_rec_tv1	Sensibilidade da Antena de recepção da transmissão da Torre – TV 01	-37,24 dB
potencia_tv2	Potencia de Transmissão da Torre de TV 02	87 dB
altura_antena_tv2	Altura da Torre de Transmissão - TV 02	100m
sensibilidade_ant_rec_tv2	Sensibilidade da Antena de recepção da transmissão da Torre – TV 02	37,5 dB
potencia_rc	Potencia de Transmissão dos rádios cognitivos	24 dB
altura_antena_rc	Altura da antena Transmissão/Recepção dos rádios cognitivos	1m
sensibilidade_ant_rec_rc	Sensibilidade da antena Transmissão/Recepção dos rádios cognitivos	-93 dB

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: pelas torres de TV, por outro(s) rádio(s) pertencente(s) ao cluster, ou mesmo, 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.

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 e processado baseado nas tabelas de frequências livres por eles disseminadas.

Em seguida, é inicializada a segunda fase, onde, simultaneamente, há a simulação das transmissões das torres de TV e dos RCs, por um período de 1 hora.

A cada unidade de tempo equivalente a 10 ms, ao qual definimos como *slot*, aleatoriamente é feita a escolha se haverá ocupação (transmissão) de algum(ns) canal(is)

nesse *slot* por parte das Torres de TV, de uma delas, ou de nenhuma – onde, nesse caso, configura-se o *white space*. Simultaneamente, são definidos quantos pares de RCs "irão transmitir" nesse *slot*; cada RC 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 RC então faz o sensoriamento do meio, verificando se há a ocupação do espectro (canais) por parte dos UPs (Torres de TV), de outro(s) RC(s) vizinho(s), ou mesmo de alguma transmissão interferente (RCs a 550m transmitindo). Caso contrário, o RC 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 RCs que, em instantes aleatórios, ocupam de forma prioritária a utilização do *slot* vagos. E no caso do SSFF há a inserção de RCs que, em instantes aleatórios, emitem tabelas de frequências adulteradas. Na Tabela 9 foram representados os dados referentes às primeiras e as últimas rodadas de cada item acima mencionados. A tabela 9 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 (RCs Tx): quantidade de RCs a transmitir por simulação; coluna 6 (RCs N): quantidade de RCs 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.

Tabela 9. 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 efetivamente Transmitidos
0	**S 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

4.3.3. Segundo Experimento: Simulação da Eficácia do SDA na Detecção de Ataques

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 RC e seus vizinhos, bem como entre os RCs 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 (Tabela 9).

A Figura 17 mostra um corte da Figura 15 onde podem ser obervados: (i) o Rádio Nr 1 (RC1); (ii) os RCs que estão ao alcance de transmissão do RC1(250 m); bem como, (iii) os RCs que podem sofrer interferência pelas transmissões do RC1 (550 m).

Na Tabela 10 estão descritas as potências captadas pelo RC1 de cada RC dentro do seu raio de alcance de transmissão, bem como as distâncias entre o RC1 às Torres de Tv e aos outros RCs. Pode ser observado que o RC1 mesmo estando à mesma distância do RC5 e do RC12 – 0,5 km, as potências captadas não são coincidentes – -82,762 (RC5) e -82,044 (RC12). Tal variação ocorre em virtude da inserção da taxa aleatória de erro.

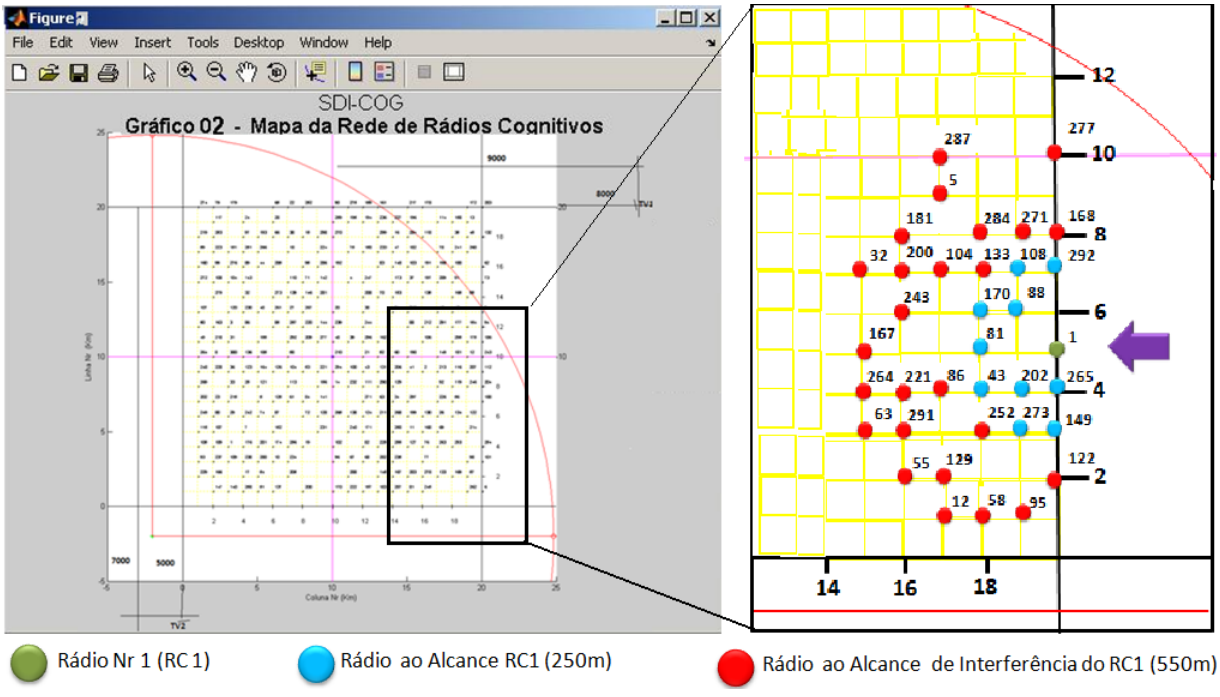


Figura 17. Corte da Figura 15 – RCs no raio de alcance do RC1

Tabela 10. Distancia/Potencia Captada do RC1 as Torres de TV e aos RCs ao Alcance

	Potência Captada pelo Rádio Nr 1 (dB)	Distância do Rádio Nr 1 (km)
Tv 1	-23,9984985	8
Tv 2	-25,8790432	6,325
Rádio Nr 5	-82,762	0,5
Rádio Nr 12	-82,044	0,5
Rádio Nr 32	-92,044	0,539
Rádio Nr 43	**-17,074**	**0,224**
Rádio Nr 55	-82,961	0,5
Rádio Nr 58	-70,148	0,447
Rádio Nr 63	-85,142	0,51
Rádio Nr 81	**-11,062**	**0,2**
Rádio Nr 86	-38,97	0,316
Rádio Nr 88	**2,68**	**0,141**
Rádio Nr 95	-61,818	0,412
Rádio Nr 104	-64,674	0,424
Rádio Nr 108	**-17,074**	**0,224**
Rádio Nr 122	-35,162	0,3
Rádio Nr 129	-64,674	0,424
Rádio Nr 133	-31,116	0,283
Rádio Nr 149	**-11,362**	**0,2**
Rádio Nr 167	-82,762	0,3
Rádio Nr 168	-35,162	0,224
Rádio Nr 170	**-17,103**	**0,224**
Rádio Nr 181	-81,33	0,5
Rádio Nr 200	-71,05	0,447
Rádio Nr 202	**2,29**	**0,141**
Rádio Nr 221	-61,818	0,412
Rádio Nr 243	-61,818	0,412
Rádio Nr 252	-31,116	0,283
Rádio Nr 264	-85,142	0,51
Rádio Nr 265	**12,438**	**0,1**
Rádio Nr 271	-38,97	0,316
Rádio Nr 273	**-17,02**	**0,224**
Rádio Nr 277	-80,761	0,5
Rádio Nr 284	-49,68	0,361
Rádio Nr 287	-92,044	0,539
Rádio Nr 291	-70,148	0,447
Rádio Nr 292	**-11,44**	**0,2**

Como é demonstrado no fluxograma da Figura 7, os RCs que necessitem transmitir, ao verificarem que há ocupação do espectro de frequência licenciada, e cujas características não se enquadram com a transmissão dos rádios vizinhos, isto é, os pacotes não contem os números MAC (endereço físico de 48 bits da estação, ou, mais especificamente, da interface de rede), disparam o mecanismo de localização. A potencia do sinal é analisada, quando então é definida a existência ou não de ataque(s) PUE.

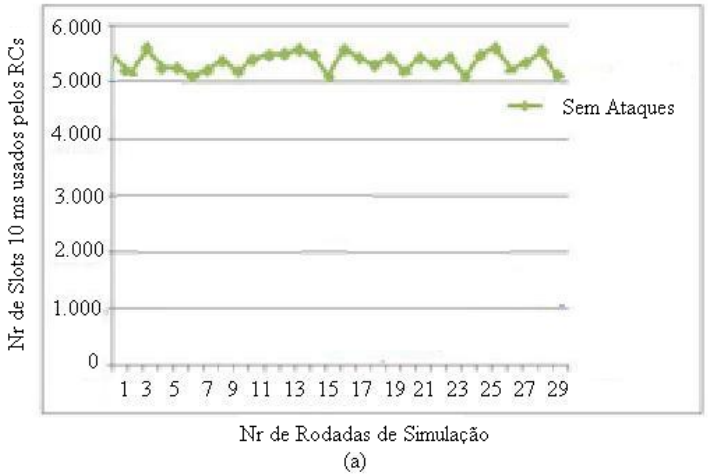
Quanto ao Mecanismo de Reputação este é simulado a cada 2,5s, por meio da análise das tabelas de frequência recebidas dos RCs vizinhos, bem como das tabelas do próprio RC que faz a análise, Figura 9. Por meio dos cálculos de atribuição de credibilidade, a reputação

dos rádios então são a eles atribuídas e selecionadas como suspeitas após ultrapassarem os limiares de aceitabilidade, como pode ser observado no pseudocódigo da Figura 10. 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.

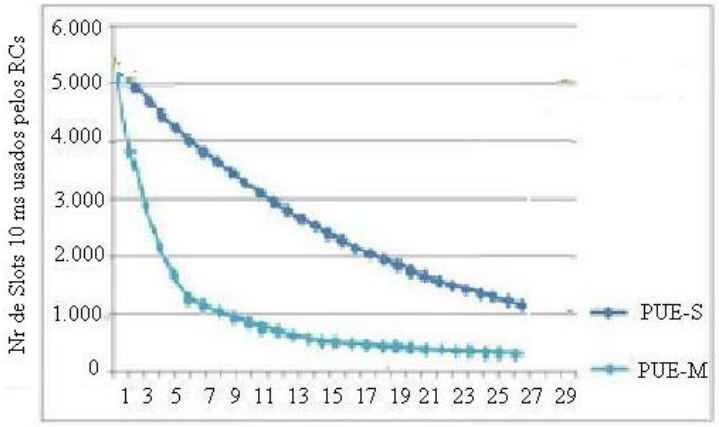
Foram realizadas 210 rodadas de simulações: 30 sem ataques; 30 variando-se somente o ataque de PUE Selfish de 1 a 30 pares de rádios atacantes; 30 variando-se somente o ataque de PUE Malicioso de 1 a 30 rádios atacantes; 30 variando-se somente o ataque de SSFF-SL de 1 a 30 rádios atacantes; 30 variando-se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

Podemos observar, por meio dos gráficos representados na Figura 18, a degradação da rede relacionada ao número de rádios que não tiveram oportunidade de transmitir quando os ataques formam inseridos nas simulações. Principalmente quando os ataques são efetuados de forma conjunta, onde, por meio de cerca de 15 atacantes, a rede perde totalmente sua capacidade de ocupação oportunística do espectro.

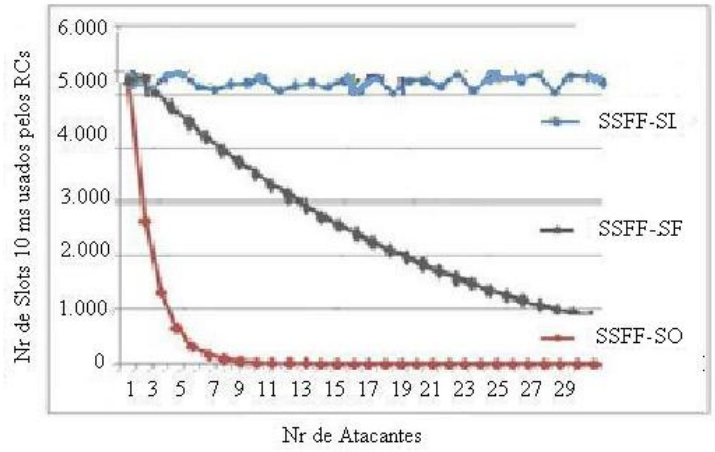
Simultaneamente à simulação dos diversos tipos de transmissões, os mecanismos de localização e de reputação são disparados. Ao analisarmos cada tipo de ataque, bem como a atuação dos mecanismos de detecção de forma isolada sem qualquer tipo de calibração, os resultados obtidos podem ser observados nas Figuras 19 e 20:



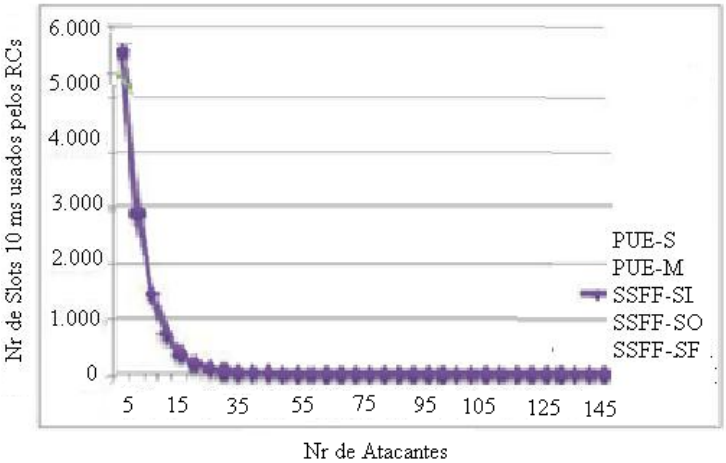
(a)



(b)



(c)



(d)

Figura 18. Simulação que apresenta as comparações dos efeitos dos ataques: (a) Sem Ataques. (b) Efeito dos Ataques de PUE. (c) Efeito dos Ataques SSFF. (d) Efeito da Combinação de Todos os Ataques.

Quanto à 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 média foi de 34,54%. Essa diferença pode ser justificada em virtude da maior agressividade o ataque de PUE-M, que 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.

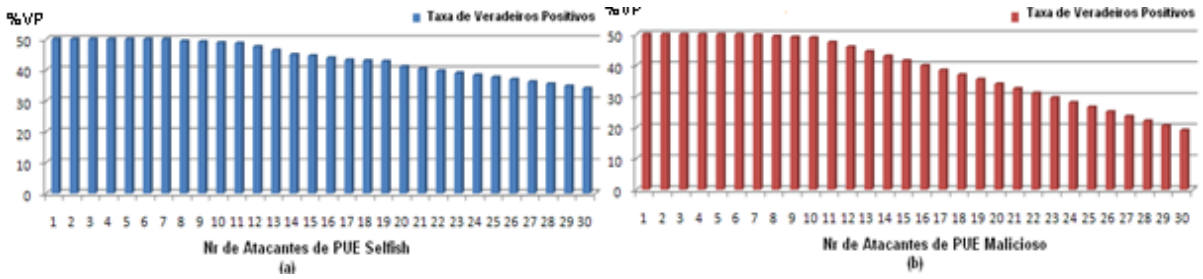


Figura 19 Simulação que apresenta as taxas de Verdadeiros Positivos utilizando-se o mecanismo de localização de forma isolada: (a) Ataques PUE S. (b) Ataques PUE M.

Nos gráficos apresentados na Figura 20, observamos as taxas de verdadeiros positivos quando o mecanismo de reputação é usado de forma isolada para a detecção de ataques de SSFF. As taxas médias foram: 44.51, 42.64 e 33.22, para os ataques de SSFF-SL, SSFF-SF e SSFF-SF, respectivamente. Novamente foi demonstrado que a agressividade do ataque reflete efetivamente no mecanismo de detecção. Maiores taxas para o ataque de SL e menores para o SO.

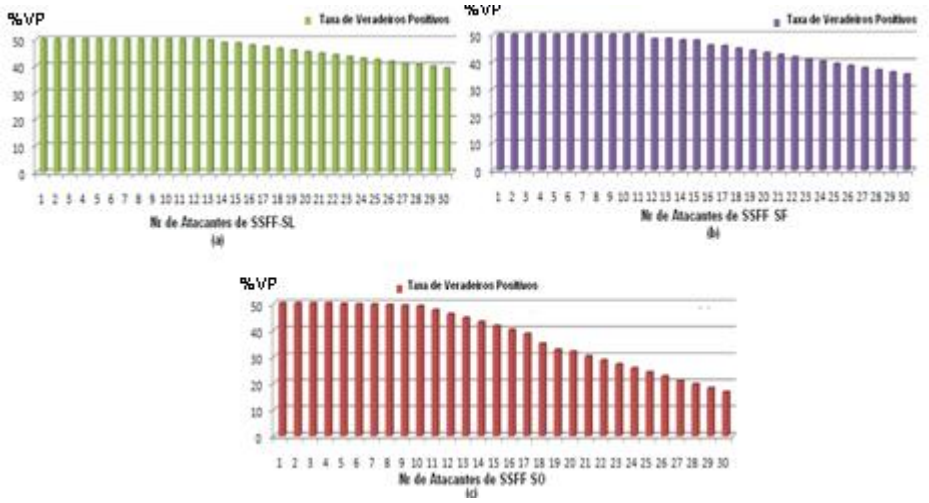


Figura 20 Simulação que apresenta as taxas de Verdadeiros Positivos utilizando-se o mecanismo de Reputação de forma isolada: (a) Ataques SSFF-SL. (b) Ataques SSFF-SF. (c) Ataques SSFF-SO

4.3.4. Terceiro Experimento: Calibração do LA e do VCN

Neste experimento foram realizadas variações para o limiar de aceitabilidade (LA) dos RCs, bem como o valor da constante de normalização das credibilidades (VCN) dos rádios com intuito de adaptar e calibrar o mecanismo de análise de reputação para o trabalho em conjunto com o mecanismo de localização.

Tabela 11. Limite de Acessibilidade 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

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 realizadas avaliações em intervalos regulares de 2.5 segundos (ZHU 2009). As simulações foram realizadas com a combinação dos cinco tipos de ataques, variando-se de 5 a 50 atacantes e calculando-se a média dos VP, FP, FN e VN para cada índice LA e VCN, seguindo (ZHU 2009)

Tabela 12. Valor do Coeficiente de Normalização 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

A Tabela 11 apresenta os resultados obtidos nesse experimento para o LA; A Tabela 12 apresenta os resultados obtidos nesse experimento para o VCN; e A Tabela 13 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 13. LA/VCN Dados 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

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 VCN igual a 5.50.

4.4. Conclusão do Capítulo

Neste capítulo foram apresentadas as simulações necessárias às avaliações experimentais do sistema de detecção. Foi simulada a geração do cenário formado pela rede de rádios cognitivos em conjunto com duas redes de transmissão de usuários primários (torre de TV 01 e torre de TV 02). Em seguida foram realizados três experimentos. O primeiro experimento apresentou o comportamento das transmissões oportunísticas dos RCs (Rádios Cognitivos) na ocupação das FLLs (Frequências Licenciadas Livres). Tal comportamento foi apresentado, tanto em um regime normal de transmissões, como na presença de ataques, demonstrado a degradação crescente da ocupação oportunística das FLLs proporcional à inserção de rádios atacantes. No segundo experimento as simulações do sistema de detecção são apresentadas com as demonstrações dos índices de detecção sob o regime de ataque. Tais simulações são executadas sem qualquer tipo de calibração e de forma isolada para cada um dos cinco tipos de ataques em análise. Por fim, a calibração do LA (Limiar de Aceitabilidade) e do VCN (Valor do Coeficiente de Normalização) é simulada. Tanto de forma isolada, como também na integração dos dois índices.

5. Avaliação dos Resultados e Calibração dos Pesos do Mecanismo de Detecção

Observou-se na Seção 4.3.4, especificamente 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 que ocorreu um 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, obtivemos os melhores valores de FP e FN. Valores esses utilizados então para as simulações e experimentos subseqüentes, i.e, optamos por trabalhar com o número de limiar de aceitabilidade igual a 14 e do VCN 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 14: VP=45.14, VN=48.70, FN=4.86 e FP=1.30. Valores esses que, 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 ataques PUE e SSFF tem um melhor desempenho.

Tabela 14. Comparação entre as métricas de detecção do SDA-COG proposto com os mecanismos de localização (PARK 2008) de reputação (ZHU 2009).

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 Utilidade (denominada nessa dissertação de Função Detecção $D_{LRC\text{-}i}$,) do rádio cognitivo *i*.

Considerando que: $L_{\text{-}i}$ representa a análise realizada pelo componente *Localizacao* quanto à identificação de ataque *PUE*, onde $L_{\text{-}i} = 0$ (o rádio *i* não é um atacante de *PUE*), ou $L_{\text{-}i} = 1$ (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 D_{LR-i}, combinam-se os valores L_{-i} e R_{-i} usando dois coeficientes de calibração γ e ω da seguinte forma:

$$DLR\text{-}i = \gamma L + \omega R \tag{14}$$

Onde: $\gamma + \omega = 1$.

Para tal a função DLR*i* (Equação 14) é ponderada por meio da criação de 5 cromossomos – 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.

$$DLR_i = (\gamma_1 L_1 + \gamma_2 L_2) + (\omega_1 R_1 + \omega_2 R_2 + \omega_3 R_3) \tag{15}$$

Cada cromossomo é composto por 30 genes, formando a primeira geração. 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, conforme descrito na Tabela 9. Os valores representativos dos pesos que consistem na solução que corresponda ao ponto de máximo da função DLR*i* são:

$$DLR_i = (\mathbf{0{,}199} L_1 + \mathbf{0{,}321} L_2) + (\mathbf{0{,}035} R_1 + \mathbf{0{,}342} R_2 + \mathbf{0{,}103} R_3) \tag{16}$$

Podemos observar que os pesos atribuídos pelo AG condizem com a realidade da degradação da RRC (Figura 18), 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 15:

Tabela 15. Mecanismos Calibrados pelo AG e simulados em conjunto com todos os ataques combinados

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 16), cujos resultados medianos aumentaram a taxa de VP em cerca de 0.5 pontos percentual, isto é: VP=45.63, demonstrando que realmente há a necessidade de atribuição de pesos para a detecção de ataque combinados às RRCs, Tabela 16.

Tabela 16. Mecanismos Calibrados pelo AG e simulados em conjunto com todos os ataques combinados

Nr Atacantes	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

5.2. Conclusão do Capítulo

O sistema foi avaliado após a calibração do limiar de aceitabilidade e do valor do coeficiente de normalização para o trabalho em conjunto dos dois mecanismos de detecção.

Foi demonstrado o aumento nos índices de detecção conjunta quando comparados aos mecanismos utilizados de forma isolada.

Por fim, o sistema foi calibrado, de forma única para a utilização da função utilidade, por meio da utilização de algoritmos genéticos, cujo resultado demonstrou maior eficiência na detecção dos ataques.

6. Conclusões

Este trabalho teve como objetivos apresentar um estudo sobre a detecção de ataques e o desenvolvimento de um sistema de detecção para a identificação de rádios que promovem a inadequada utilização das freqüências licenciadas livres em uma rede de rádios cognitivos (RRCs). Para isso: (i) identificamos os principais tipos de ataques aos quais as RRCs estão sujeitas: a emulação do usuário primário (*Primary User Emmulation* – PUE) e a adulteração das tabelas de frequências licenciadas livres (*Spectrum Sense False Feadback.*- SSFF); (ii) selecionamos os dois mecanismos de detecção mais adequados a estes tipos de ataques: o mecanismo de localização e o de reputação; e integramos as técnicas de localização e classificação de reputação de forma a alcançar os melhores índices possíveis de detecção. Tal integração foi operacionalizada por meio da utilização de uma função utilidade aditiva (função detecção), cujos pesos dos atributos componentes foram calculados com a utilização da heurística de algoritmos genéticos. O sistema foi validado por meio de simulações e comparado, em suas métricas de detecção, aos dois mecanismos utilizados como base deste trabalho.

O mecanismo de localização (PARKER 2008) foi adaptado para o ambiente urbano, visto que, em sua forma original, tal mecanismo foi utilizado para a detecção de ataques de PUE em áreas rurais. Essa adaptação teve por finalidade atender a cenários onde encontrarmos as maiores concentrações de equipamentos que fazem uso das faixas de frequências não licenciadas (cenário urbano). Causando, em virtude disso, uma maior escassez espectral, sendo então áreas propícias à utilização de RRC.

Outra modificação no mecanismo de localização original foi promovida: a implementação do mecanismo nos próprios rádio cognitivos (RCs) autenticados da rede, pois, o mecanismo de (PARKER 2008) utiliza uma rede de sensores sem fio (RSSF), secundária à RRC, para a detecção de ataques de PUE. Suprimindo-se, com essa alteração, este ponto de vulnerabilidade à RRC.

Quanto ao mecanismo de reputação, houve a necessidade da calibração do limiar de aceitabilidade (LA) e do valor do coeficiente de normalização (VCN) na integração com o mecanismo de localização. A finalidade foi a de maximizar os índices de verdadeiros positivos (VP) na detecção de ataques. Os valores definidos na proposta original do mecanismo (ZHU 2009) são: LA=15(-15) e VCN=5.51. Após as calibrações realizadas, encontramos para os maiores índices de VP os seguintes valores: LA= 14 e VCN=5.40, valores estes então utilizados em todas as simulações realizadas nesse trabalho.

Foi simulada uma RRC com a criação dos diversos perfis de comportamento dos rádios cognitivos necessários à análise do desempenho da RRC sob condições de ataques. Tal SDA foi programado de forma a atender, então, às demandas e restrições deste tipo de rede.

As simulações foram realizadas, em uma primeira fase, na geração do cenário da RRC seguindo o modelo proposto em (PARK 2008) que teve por finalidade a análise comparativa entre os mecanismos. Em seguida foram realizados três experimentos para a validação do SDA. No primeiro, houve a simulação das transmissões, tanto das torres de Tv (usuários primários - UP), quando dos rádios cognitivos (rádios legítimos/rádios atacantes). Neste experimento realizado, observou-se a degradação da capacidade de utilização oportunística de ocupação dos canais licenciados livres por parte dos RCs, proporcionalmente ao aumento do número de atacantes. A identificação dos ataques realizada pelo sistema de detecção foi o foco do segundo experimento. Os mecanismos foram utilizados de forma independentes e sem qualquer tipo de calibração. Quanto ao mecanismo de localização na detecção de ataques de PUE-S registrou uma taxa média de verdadeiros positivos na faixa de 42,50 % e de 34,54% para o ataque de PUE-M. As taxas médias de verdadeiros positivos do mecanismo de reputação foram: 44.51, 42.64 e 33.22, para os ataques de SSFF-SL, SSFF-SO e SSFF-SO, respectivamente. O terceiro experimento consistiu na calibração do LA e do VNC.

A simulação integrada dos dois mecanismos foi realizada após a calibração do LA e do VCN. Os resultados obtidos foram VP=45.14, VN=48.70, FN=4.86 e FP=1.30. Valores esses que, quando comparados a (PARK 2008), com uma taxa média de VP=44% e a (ZHU 2009) de VP=43,18%, demonstram que a combinação dos mecanismos na detecção de ataques de PUE e de SSFF tem um melhor desempenho.

Por fim, é utilizado o algoritmo genético para realizar a atribuição de pesos aos mecanismos de detecção na Função Utilidade, encontrando-se os seguintes pesos: PUE-S=0.199**,** PUE-M= 0.321, SSFF-SL=0.035, SSFF-SO=0.342 e SSFF-SF= 0.103. A análise do sistema de detecção com pesos ponderados aumentaram a taxa de verdadeiros positivos de VP=45.14 para VP=45.63, demonstrando que a atribuição de pesos para a detecção de ataque combinados às RRCs tem uma melhor performance.

Em suma, o SDA-COG 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 RRC. Principalmente após a calibração, em uma primeira fase, do mecanismo de reputação, e em seguida, da calibração do SDA com um todo.

6.1. Trabalhos Futuros

Quanto aos trabalhos futuros, podem ser investigadas outras formas de se melhorar os resultados obtidos como, por exemplo, a utilização de diferentes mecanismos de localização e de reputação, de forma a melhorar a detecção isolada de atacantes. Ou seja, os valores obtidos para verdadeiros positivos (VP), verdadeiros negativos (VN), falso positivos (FP) e falsos negativos (FN). Outra forma de se tentar uma melhora nestas métricas seria a verificação de outros métodos de se calibrar o limiar de aceitabilidade, bem como o valor do coeficiente de normalização do mecanismo de reputação, como por exemplo: lógica *fuzzy*, redes neurais etc.

A análise e validações do sistema proposto foram concebidas com base em simulações de uma rede descentralizada, plana e com nós fixos. O sistema poderia ser avaliado com outras topologias, como por exemplo, uma rede centralizada, ou mesmo, descentralizada, porém, com rádios móveis.

Outra linha de pesquisa seria a utilização de uma diferente heurística na atribuição de pesos ponderados à função utilidade. Por exemplo, ao invés do algoritmo genético, utilizar-se a lógica nebulosa para tal atribuição. Ou mesmo, a total substituição da função utilidade por outro método de integração dos mecanismos. Como por exemplo, a própria lógica *fuzzy* ou redes neurais.

Em suma, em trabalhos futuros, com o objetivo de maximizar os índices de verdadeiros positivos na detecção de ataques, serão investigadas outras combinações de mecanismos de detecção; 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 de ataques. 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-COG.

Referências

ABDUL-RAHMAN (2000), A., HAILES, S., Supporting Trust in Virtual Communities. Em: Proceedings of the Hawaii International Conference on System Sciences, 2000.

AURÉLIO (2011), Dicionário Aurélio On Line – Dicionário de Lingua Portuguesa: http://74.86.137.64-static.reverse.softlayer. com/

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

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

AKYILDIZ, Ian, (2008). F., LEE, WON-YEOL, VURAN, M. C., & MOHANTY S., "A Survey on Spectrum Management in Cognitive Radio Networks**".** IEEE Communications Magazine, Vol. 46, Issue 4, pp. 40-48

ALMEIDA, E. P. L. (2010). "Desenvolvimento de Técnica de Sensoriamento do Espectro Embasada em Detecção de Energia para Aplicações em Sistemas Rádio-Cognitivos." Dissertação de Mestrado em Engenharia Elétrica, Publicação PPGENE.DM - 412/2010, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 103p.

BARBOSA, A. (2000) "Sistemas de Detecção de Intrusão – Seminários Ravel – CPS760", http://www.lockabit.coppe.ufrj.br/downloads/academicos/IDS.pdf.

BARCELLOS (2006), M. P. ; GASPARY, L. P., Segurança em Redes P2P: Princípios, Tecnologias e Desafios. Em: XXIV Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, p. 211-260, 2006.

BARFORD, P (2002).. et al. A signal analysis of network traffic anomalies. In: IMW '02: Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurement. New York, NY, USA: ACM,

BEIJTLICH (2004), Richard, The Tao of Network Security Monitoring: Beyond Intrusion Detection, Addison-Wesley, 2004.

BRUTLAG, J (2000). D. Aberrant behavior detection in time series for network monitoring. In: LISA '00: Proceedings of the 14th USENIX conference on System administration. Berkeley, CA, USA: USENIX Association,.

CABRIC, D. (2004), Mishra, S.M., Brodersen, R.W.: "Implementation Issues in Spectrum Sensing for Cognitive radios". In: Conf. Record of the 38th Asilomar Conf. on Signals, Systems and Computers, vol. 1, pp. 772–776

CARLSON, A .B., (1981) "Sistemas de Comunicação: uma introdução aos sinais e ruídos em comunicação elétrica", São Paulo: McGraw-Hill do Brasil,.

CERT, 2011 – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. (2011) Estatísticas do CERT.br. http://www.cert.br/stats/incidentes/

CHHABRA, P. et al (2008). "Distributed spatial anomaly detection". INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, pp. 1705-1713, abril.

CLANCY T, (2008) Goergen N. "Security in cognitive radio networks: threats and mitigation". Third International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom),; 1–8. DOI: 10.1109 / CROWNCOM .2008.4562534.

CLANCY T, (2009), A. Khawar, "Security Threats to Signal Classifiers Using Self-Organizing Maps", Fourth International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom)

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

CORDEIRO (2005) Cordeiro, C, Challapali, K, Birru, D 2005 "IEEE 802.22: the first worldwide wireless standard based on cognitive radios". Proceedings of *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005*, Baltimore, USA. pp. 328-337, 8 a 11 de Novembro de 2005

COURSES (2007) Courses, E, Surveys, T 2007 "Dynamic spectrum access in the IEEE 802.22 wireless regional area network". Proceedings of *Second International Conference on Access Networks & Workshops; AccessNets' 07*, Ottawa, Ontario. pp. 1- 6, 22 a 24 de Agosto de 2007

DA SILVA, A. (2005) "Detecção de Intrusos Descentralizada em Redes de Sensores Sem Fio", Dissertação de Mestrado, UFMG.

DA SILVA, A. *et al.* (2006) "Detecção de Intrusos Decentralizada em Redes de Sensores Sem Fio", 24º Simpósio Brasileiro de Redes de Computadores, Curitiba, Brasil.

DEBAR, H. *et al.* (1999) "Towards a Taxonomy of Intrusion-Detection Systems", Computer Networks, v. 31, páginas 805-822.

DEWAELE, G. et al (2007). "Extracting hidden anomalies using sketch and non Gaussian multiresolution statistical detection procedures". In: LSAD '07: Proceedings of the 2007 workshop on Large scale attack defense. New York, NY, USA: ACM,. pp. 145-152.

EBAY (2007). *eBay* Partner Network Site Ebay, http://www.ebay.com, Último acesso: Agosto de 2007.

FCC, Federal Communication Commission (2009) Home Page. http://www. fcc.gov - último acesso em 13/10/2009.

FELDMAN (2004a), M., LAI, K., STOICA, I., CHUANG, J., Robust Incentives Techniques for Peer-to-Peer Networks. Em: Proceedings of the 5th ACM conference on Eletronic Commerce, pages 102-111, 2004.

FELDMAN (2004b), M., PAPADIMITRIOU, C., STOICA, I., CHUANG, J., Free- Riding and Whitewashing in Peer-to-Peer Systems. Em: Proceedings SIGCOMM workshop on Practice and Theory of Incentives and Game Theory in Networked Systems, 2004.

GANESAN G. (2005) and Y. Li, "Cooperative spectrum sensing in cognitive radio networks," *Proc. DySPAN*, Nov. , pp. 137–143.

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

GARCÍA-TEODORO, P. *et al.* (2008) "Anomaly-based network intrusion detection: Techniques, systems and challenges", Computers & Security, v. 28, páginas 18-28.

GOMES (2007) Alexandre Lages. Um Sistema para o Aumento da Confiabilidade da utilização de Serviços através de Sistemas de Reputação. 2007. 0 f. Dissertação (Mestrado em Informática) – Universidade Federal do Rio de Janeiro,

HARTIGAN, J. A (1979).; Wong, M. A. "Algorithm AS 136: A K-Means Clustering Algorithm". *Journal of the Royal Statistical Society, Series C (Applied Statistics)* **28** (1): 100–108. JSTOR 2346830.

HE T., (2003) C. Huang, B. M. Blum, J. A. Stankovic, and T. F. Abdelzaher, “Range-free localization schemes in large scale sensor networks,” Proc.ACM MobiCom, Sept., pp. 81–94.

HIGHTOWER, J. (2001), Gaetano Borriello, “Location Systems for Ubiquitous Computing” IEEE Computer, 57-66,

HWANG (2008) Hwang, SH, Um, JS, Song, MS, Kim, CJ, Park, HR, Kim, YH 2008 "Design and Verification of IEEE 802.22 WRAN Physical Layer". Proceedings of *3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, Singapure. pp. 1-6, 15 a 17 de Maio de 2008

IANCULESCU, Cristian (2005); MUDRA, Andy. Cognitive Radio and Dynamic Spectrum Sharing. Proceeding of the SDR 05 Technical Conference and Product Exposition.

IEEE (2004) Starts Standard to Tap Open Regions in the TV Spectrum for Wireless Broadband Services". *News release* (IEEE Standards Association). October 12, 2004. Archived from the original on February 7,2009. http://web.archive.org/ web/20090207 021748/ http:// standards.ieee.org/announcements/pr_80222.html. Retrieved August 19, 2011.

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

INMETRO (2011), Instituto Nacional de Metrologia, Normalização e Qualidade Industrial Projeto de Normalização do Rádio cognitivo: “PlatCog - Plataforma de rádio cognitivo – abril, 2011”, http://www.dco.ct.ufrn.br/news/news_workshop_cpqd.html

JOSANG (2002), A., ISMAIL, R., The Beta Reputation System. Em: Proceedings of the 15th Bled Eletronic Commerce Conference, 2002.

JOSANG (2007), A., ISMAIL, R., BOYD, C. A Survey of Trust and Reputation Systems for Online Service Provision. Em: Decision Support Systems, 43(2), pages 618-644,2007.

KAUR, K. e SINGH, B. (2010) “Wireless Sensor Network based: Design Principles & measuring performance of IDS”, International Journal of COmputer Applications, volume 1, número 28, páginas 81-85.

KEENEY, R. L.(1999); RAIFFA, H. Decisions with multiple objectives: preferences and value tradeoffs. Cambridge: Cambridge University Press, 1999.

KRISHNAMURTHY, B. et al (2003). Sketch-based change detection: methods, evaluation, and applications. In: IMC '03: Proceedings of the 3rd ACM SIGCOMM conference on Internet measurement. New York, NY, USA: ACM,. pp. 234-247.

KURAN (2007) A survey on emerging broadband wireless access technologiesKuran, MS, Tugcu, T A survey on emerging broadband wireless access technologies. *Computer Networks: The International Journal of Computer and Telecommunications Networking* 51, 3013-3046.2007a

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: Associação Brasileira de Recursos Hídricos. p. 99-150. (Coleção ABRH de Recursos Hídricos; 7.). Porto Alegre.

LAKHINA, A (2004a)..; CROVELLA, M.; DIOT, C. Characterization of network-wide anomalies in traffic flows. In: IMC '04: Proceedings of the 4th ACM SIGCOMM conference on Internet measurement. New York, NY, USA: ACM, pp. 201-206.

LAKHINA, A. (2004b); CROVELLA, M.; DIOT, C. Diagnosing network-wide traffic anomalies. In: SIGCOMM '04: Proceedings of the conference on Applications,

technologies, architectures, and protocols for computer communications. New York, NY, USA: ACM, 2004. pp. 219-230

LEON, Olga (2010), Juan Hernandez-Serrano, Miguel Soriano. "Securing cognitive radio networks".International Journal of Communication Systems, vol 23,. ISSN/ISBN 1074-5351

LI, X. et al (2006). Detection and identification of network anomalies using sketch subspaces. In: IMC '06: Proceedings of the 6th ACM SIGCOMM conference on Internet measurement. New York, NY, USA: ACM,. pp. 147-152.

LINDE Y (1980), Buzo A, Gray R. An algorithm for vector quantizer design. IEEE Transactions on Communications ;28(1):84–94.

LOPES, C. L. (2008) A escolha de um custodiante para uma administradora financeira: Análise multiatributo por medições conjuntas e trocas justas. Dissertação de mestrado em administração, Ibmec – RJ, Fev./ 2008.

MCHENRY,M. (2003). Frequency agile spectrum access technologies, FCC Workshop on Cognitive Radio.

MATLAB (2012) Wikipédia – a Enciclopédia Livre: http://pt.wikipedia.org/wiki/MATLAB

MATHEW Tom V. (2002) Genetic Algorithm Department of Civil Engineering, Indian Institute of Technology Bombay, Mumbai-400076.

MING-YANG Su (2011), "A Using clustering to improve the KNN-based classifiers for online anomaly network traffic identification", Journal of Network and Computer Applications Volume 34, Issue 2, March, Pages 722-730

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

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 (2009) and G. Q. Maguire, Jr., "Cognitive Radio: Making Software Radios More Personal," IEEE Personal Communications, Vol. 6, No. 4, pp. 13-18, Aug. 1999.

MCKNIGHT (1996), D. H., CHERVANY, N. L., The meanings of Trust. Technical Report MISRC Working Paper Series, 96-04, 1996.

NHAN Nguyen-Thanh (2009), Insoo Koo, "A secure distributed spectrum sensing scheme in cognitive radio**"**, Proceedings of the Intelligent computing 5th international conference on Emerging intelligent computing technology and applications, September 16-19, , Ulsan, South Korea

NAVSTAR (2004), Navstar Global Positioning System, "Interface Specification IS-GPS-200" Navstar GPS Space Segment/Navigation User Interfaces Revision D.

NEWMAN T. (2009) and T. Clancy, "Security threats to cognitive radio signal classifiers", in Virginia Tech Wireless Personal Communications Symposium, June.

NIST (2010), National Institute of Standards and Technology "NIST Framework and Roadmap for Smart Grid Interoperability Standards", NIST Special Publication 1108.

OSSIE (2007) Open Source Software Communications Architecture (SCA) Implementation Embedded, Home Page. - http://ossie.wireless.vt.edu/trac/

PARK J (2008).-M. R. Chen, , and J. H. Reed**,** "Defense against primary user emulation attacks in cognitive radio networks**,**" IEEE Journal on Selected Areas in Communcations Special Issue on Cognitive Radio Theory and Applications**,** Vol. 26, No. 1, Jan.

PIRES, P. F. (2007), DELICATO, F. C., LAGES, A. G., PIRMEZ, L., SATYA: "A Reputation-based Approach for Service Discovery and Selection in Service Oriented Architectures". Em 9th ACM International Workshop on Web Information and Data Management, Lisboa, Portugal,.

RASH (2005), Michael et al, Intrusion Prevention and Active Response: Deployment Network and Host IPS, Syngress, 2005.

RESNICK (2000), P., ZECKHAUSER, R., FRIEDMAN, E., KUWABARA, K., Reputation Systems. Em: Communications of the ACM, Vol. 43, Dezembro, 2000.

RICHARDSON, R. (2010) CSI/FBI Computer Crime Survey. Em 15th Annual 2010/2011 Computer Crime and Security, 44 páginas.

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

ROSENVERGER C (2000), Chehdi K. Unsupervised clustering method with optimal estimation of the number of cluster: application to image segmentation. In: Proceedings of the IEEE international conference on pattern recognition, , p. 656–9.

RUILIANG, C. (2008a), Jung-Min, P., Hou, Y.T., Reed, J.H.: Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks. IEEE Communications Magazine 46,50–55

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

RUOHORNAA Ruohomaa , S., (2007) Kutvonen, L., and Koutrouli, E., "Reputation Management Survey", 2nd International Conference on Availability, Reliability and Security.

SAFDAE, G.A (2009), & M.O'Neill, "Common Control Channel Security Framework for Cognitive Radio Networks", 69th IEEE Vehicular Technology Conference, p.1-5.

SCHERRER, A. et al. (2007) Non-gaussian and long memory statistical characterizations for internet traffic with anomalies. IEEE Trans. Dependable Secur. Comput., IEEE Computer Society Press, Los Alamitos, CA, USA, v. 4, n. 1, pp. 56-70,.

SHANKAR, S. N (2005); C. Cordeiro, K. Challapali, "Spectrum agile radios: utilization and sensing architectures," *Proc. DySPAN*, Nov., pp. 160–169.

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

SIMULINK (2012) Wikipédia – a Enciclopédia Livre: http://pt.wikipedia.org/wiki/Simulink

SILVA (2007), F. M. and de Rezende, J. F. - "Avaliação de Métodos Matemáticos usados nos Modelos de Reputação de Incentivo à Cooperação" - in XXV Simpósio Brasileiro de Redes de Computadores - SBRC'2007, pp. 999-1012, Belém, PA, May 2007.

SIMONOFF J. S (1996)., Smoothing Methods in Statistics, Springer-Verlag,

SONG (2005), S., HWANG, k., KWOK, Y. and ZHOU, R., Trusted P2P Transactions with Fuzzy Reputation Aggregation. Em: Security in P2P Systems, IEEE Internet Computing, Novembro-Dezembro, 2005.

SWETS (1986), J. A. “Form of Empirical ROCs in Discrimination and Diagnostic Tasks,” *Psycological Bulletin*, *99* (2):181–198 (1986).

THEOTOKIS (2002), S. A., SPINELLIS, D., A Survey of Peer-to-Peer File Sharing Technologies. White paper, Electronic Trading Research Unit (ELTRUN), Athens University,2002.

THOMAS (2005) R. W., L. A. DaSilva, and A. B. MacKenzie, “Cognitive Networks,” *IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN 2005)*, Baltimore, MD, November 2005, pp. 352-360.

TIMOFTE, J. (2008) “Wireless Intrusion Prevention Systems”, Revista Informática Economica, número 3, páginas 129-132.

VIRGINIA TECH (1896)Virginia Polytechnic Institute and State University Home Page: http://www.vt.edu/

WILD B., K. (2005) Ramchandran, “Detecting primary receivers for cognitive radio applications,” *Proc. DySPAN*, Nov., pp. 124–130.

WITHBY (2000), A., JOSANG, A. INDULSKA, J., Filtering out Unfair Ratings in Bayesian Reputation Systems. Em: Proceedings of the 7th International Workshop onCooperative Information Agents, 2000.

ZHU,Feng (2009) and Seung-Woo Seo, "'Enhanced Robust Cooperative Spectrum Sensing in Cognitive Radio", JCN, Special Issue on Cognitive Radio: A Path in the Evolution of Public Wireless Networks, Volume 11, Pages 122-132, Apr.