JULIO CESAR HUARACHI SOTO

UM ESQUEMA PARA ANÁLISE MULTICRITÉRIO E COOPERATIVA DA PRESENÇA DE ATAQUES EUP EM REDES AD HOC DE RÁDIO COGNITIVO

Dissertação Apresentada como Requisito Parcialà Obtenção do Grau de Mestre. Programa de Pós-Graduação em Informática, Setor de Ciências Exatas, Universidade Federal do Paraná.

Orientadora: Profa. Dra. Michele Nogueira Lima

CURITIBA

2012

JULIO CESAR HUARACHI SOTO

UM ESQUEMA PARA ANÁLISE MULTICRITÉRIO E COOPERATIVA DA PRESENÇA DE ATAQUES EUP EM REDES AD HOC DE RÁDIO COGNITIVO

Dissertação Apresentada como Requisito Parcialà Obtenção do Grau de Mestre. Programa de Pós-Graduação em Informática, Setor de Ciências Exatas, Universidade Federal do Paraná.

Orientadora: Profa. Dra. Michele Nogueira Lima

CURITIBA

2012

Soto, Julio Cesar Huarachi
Um esquema para análise multicritério e cooperativa da presença de ataques EUP em redes ad hoc de rádio cognitivo / Julio Cesar Huarachi Soto. – Curitiba, 2012.
61 f.: il., tab.

Dissertação (mestrado) – Universidade Federal do Paraná, Setor de Ciências Exatas, Programa de Pós-Graduação em Informática.
Orientador: Michele Nogueira Lima

1. Sistemas de comunicação móvel. 2. Estações móveis de radio. 3. Radiofrequência. I. Lima, Michele Nogueira II. Universidade Federal do Paraná. III. Título.

CDD: 621.38456

Ministério da Educação
Universidade Federal do Paraná
Programa de Pós-Graduação em Informática

PARECER

Nós, abaixo assinados, membros da Banca Examinadora da defesa de Dissertação de Mestrado em Informática, do aluno Julio Cesar Huarachi Soto, avaliamos o trabalho intitulado, *"Um Esquema para Análise Multicritério e Cooperativa da Presença de Ataques EUP em Redes Ad Hoc de Rádio Cognitivo "*, cuja defesa foi realizada no dia 29 de agosto de 2012, às 09:30 horas, no Departamento de Informática do Setor de Ciências Exatas da Universidade Federal do Paraná. Após a avaliação, decidimos pela aprovação do candidato.

Curitiba, 29 de agosto de 2012.

Profa. Dra. Michele Nogueira Lima
DINF/UFPR – Orientadora

Prof. Dr. Ronaldo Moreira Salles
IME – Membro Externo

Prof. Dr. Aldri Luiz dos Santos
DINF/UFPR – Membro Interno

Dedico este trabajo a mis padres, Julio y Nidia, que supieron implantar en mí los valores fundamentales de la vida e inculcarme siempre ese deseo de superación.

AGRADECIMENTOS

Quero agradecer a Deus, por ser a luz em minha vida. A meus pais Julio y Nidia por sempre estar do meu lado motivando-me, apoiando-me e ensinando me ser uma melhor pessoa cada dia. A minha irmã Giuliana por ser minha inspiração de luta na vida. A minha Familia em geral pelo apoio neste caminho, só posso disser os quero muito.

Agradeço ao Dinf da UFPR por permitir realizar meus estudos. Ao CNPQ por financiar meus estudos e pesquisa. À professora Michele, pela orientação, ajuda, confiança e paciência que teve comigo. Ao professor Aldri, pela oportunidade de entrar ao grupo NR2. Ao professor Albini, pelo ensino em aulas.

Agradeço a duas pessoas importantes para mim. Urlan, por ensinar esse conceito da persistência, e de nunca desistir. Robinho, por ensinar-me o sentido de responsabilidade e ajuda constante, além de ser o moleque Mac. Não quero deixar de agradecer a cada um dos membros do grupo NR2 e não membros. A Elisa, pela ajuda e amabilidade em todo. O Fernando, o Golden Boy, pelos copos de café. O Neimar, pelo transporte aos jogos. O Marco, pelas loucuras. A Cinara, pelo grande humor. A Crystiane, por ensinar que um sábio cala e escuta. O Nuno, pela conversa em espanhol. A Angelita, pela alegria. O Ricardo, pelos conselhos e seus cantos do chaves. O Rafael, pelo metal. A Juliana, por sua alegria. O Leonardo, pela ajuda na pesquisa. Ao professor Saulo, pela grande ajuda no projeto e amizade sincera. O Rodrigo e Yuri, pelos sorrisos no laboratório. A Jenny, pela leitura, obrigado equatoriana. Não quero deixar de agradecer a João, Marcos, Luiz e demais pelos momentos de piadas.

Por outro lado, não posso deixar de agradecer a meus compatriotas. A Nadine, pelas horas de companhia e conversação que me fizeram sentir como em casa, e que depois de todo o superamos. O Christian, pelos momentos de estudo, bagunça e perdições em lugares inesperados. Também quero agradecer a todos meus amigos em Perú. A todas essas pessoas que conheci em Brasil como esses dos japoneses Juliano e Luciano, o mecânico e o pedreiro, e todas as pessoas, desculpem se esqueço de alguém, só tenho palavras de agradecimento para cada um de vocês.

Muito obrigado a todos por tudo!

Hay alguien tan inteligente que aprende de la experiencia de los demás.

Francois Marie Arouet Voltaire

RESUMO

O uso ineficiente do espectro de radiofrequências e a alta proliferação de dispositivos móveis motivaram o desenvolvimento da tecnologia de rádio cognitivo (RC). Esta permite um melhor aproveitamento do espectro de radiofrequências e tem promovido o surgimento das redes ad hoc de rádio cognitivo (CRAHNs, do inglês, *Cognitive Radio Ad Hoc Networks*). Nestas redes dois tipos de usuários compartilham o espectro: o usuário primário (UP) e o usuário secundário (US). O usuário primário possui licença para usar as bandas de frequência e tem prioridade para acessá-las; enquanto os usuários secundários não possuem licenças, mas utilizam estas bandas quando elas estiverem ociosas. Apesar das vantagens da tecnologia RC, o aproveitamento das frequências ociosas pode ser altamente comprometido por ataques de Emulação de Usuário Primário (EUP). Um ataque EUP é gerado por um usuário secundário, malicioso ou egoísta, que emula o comportamento e as características dos usuários primários legítimos a fim de ganhar prioridade no uso do espectro de radiofrequências. Os esquemas propostos na literatura para a análise, detecção ou mitigação dos ataques EUPs seguem arquiteturas de redes centralizadas ou distribuídas, além de exibir abordagens cooperativas ou não-cooperativas. Porém, esses esquemas realizam uma análise considerando um único critério para avaliar a presença de ataques na rede, resultando em altas taxas de falsos positivos. A fim de prover uma análise mais sofisticada e eficiente, este trabalho propõe IMCA, um esquema para anál**I**se **M**ulticritério e **C**ooperativa da presença de **A**taques EUP em redes ad hoc de rádio cognitivo. Este esquema segue uma abordagem descentralizada e cooperativa em que cada US realiza duas fases para determinar a probabilidade da presença de ataque EUP. A primeira fase consiste no sensoreamento e na análise dos valores de múltiplos critérios; e a segunda fase consiste na troca de informações entre vizinhos, seguida da análise das informações trocadas através do teorema de Bayes. O esquema IMCA foi implementado no simulador de rede, *Network Simulator* (NS), versão 2.31 e avaliado. Os resultados mostram que o esquema apresenta uma superioridade de até 25% comparado com um esquema monocritério não-cooperativo, quando executada apenas a primeira fase, e uma eficácia de até 77% na determinação da probabilidade da presença de ataques EUP, quando aplicadas as duas fases do esquema.

Palavras-chave: rádio cognitivo, ataque de emulação de usuário primário, redes ad hoc, análise de múltiplos critérios.

ABSTRACT

The inefficient use of the radio spectrum and the high proliferation of mobile devices have motivated the development of *Cognitive Radio (CR)* technology. The CR technology enables a better use of the spectrum and has promoted the development of *Cognitive Radio Ad Hoc Networks (CRAHNs)*. These networks handle two types of users sharing the spectrum: primary user and secondary user. A *Primary User* has license to use the frequency bands and has a higher priority to access them, whereas a *Secondary User* has no license, but use licensed bands when they are idle. However, the use of idle frequencies can be highly compromised by *Primary User Emulation Attack (PUEA)*. This attack is generated by a malicious or selfish secondary user, that emulates the behavior and the characteristics of a legitimate PU to take priority in the use of radio spectrum access. Existing proposals in the literature for analyzing, detecting or mitigating PUEA in cognitive radio networks focus on centralized or decentralized architecture, following cooperative or non-cooperative approaches. All of them apply a single criterion to evaluate the presence of attacks on the network. In order to provide a more sophisticated and efficient approach, this work proposes a *scheme for cooperat**I**ve and **M**ulticriteria analysis of the presen**C**e of PUE **A**ttacks in cognitive radio ad hoc networks*, called $IMCA$. In $IMCA$, each secondary user conducts two phases to determine the probability of the presence of PUEA. Initially, the secondary user carries a single phase sensing and analyzing the values of multiple criteria. Then, in the second phase, each secondary user exchanges information with its neighbors and analyzes it based on the Bayes' theorem in order to determine the probability of PUEA occurrence on the network. $IMCA$ has been implemented in the Network Simulator, version 2.31, and evaluated. Results show that the $IMCA$ scheme in its individual non-cooperative phase increases up to 25% of the efficiency on detecting the PUEA presence when compared with a mono-criterion non-cooperative scheme. Further, the $IMCA$ scheme applying both phases has improved in approximately 77% a mono-criterion cooperative scheme.

Keywords: cognitive radio, primary user emulation attack, ad hoc networks, multiple criteria analysis.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

3D-CTMC	Three Dimensional Continuous Time Markov Chain
ANATEL	Agência Nacional de Telecomunicações
AODV	Ad hoc On Demand distance Vector routing protocol
CRAHN	Cognitive Radio Ad Hoc Network
DoS	Denial of Service
DDT	Distance Difference Teste
DTR	Distance Ratio Test
EUP	Emulação de Usuário Primário
FCC	Federal Communications Commission
FDOA	Frequency Difference Of Arrival
IMCA	Esquema de múlt**I**plos critérios para a**N**álise **C**ooperativa da presença de **A**taques EUP
LocDef	Localization-based Defense
MCDA	Multi-Criteria Decision Analysis
NEAT	NEighbor AssisTed Spectrum Decision)
NS-2	Network Simulator 2
NWAUF	Normalized Weighted Additive Utility Function
PCA	Principal Component Analysis
QoS	Quality of Service
RC	Rádio Cognitivo
TDOA	Time Difference Of Arrival
UP	Usuário Primário
US	Usuário Secundário
WSPRT	Wald?s Sequential Probability Ratio Test

NOTAÇÃO

N_{UP}	Conjunto de usuários primários
N_S	Conjunto de usuários secundários
N_{SL}	Conjunto de usuários secundários legítimos
N_{SB}	Conjunto de usuários secundários mal intencionados
n_i	Usuário secundário
n_j	Usuário secundário vizinho de n_i
i**-ésimo**	Índice que representa um usuário secundário arbitrário
j**-ésimo**	Índice que representa um usuário secundário vizinho arbitrário
$P_{n_i}(A)$	Probabilidade preliminar calculada pelo nó n_i
$P_{n_j}(B)$	Probabilidade preliminar calculada pelo vizinho n_j
$P_{n_i}(A\|B)$	Probabilidade final calculada pelo nó n_i
$P_{n_j}(B\|A)$	Probabilidade final calculada pelo vizinho n_j
$\mathcal{S}$	Conjunto de critérios
$\mathcal{W}$	Conjunto de pesos de importância para os critérios
$\mathcal{MIN}$ **e** $\mathcal{MAX}$	Conjunto de valores mínimos e máximos
Pr	Probabilidade da presença de ataque
Pr_{pup}	Probabilidade de perda de detecção de um usuário primário
T_k	Taxa de detecção por vizinhos cooperadores
Tx_{fp}	Taxa de falsos positivos
Tx_{fn}	Taxa de falsos negativos
T_k	Taxa de detecção por vizinhos cooperadores

CAPÍTULO 1

INTRODUÇÃO

Tradicionalmente, o espectro de radiofrequências tem sido alocado por agências reguladoras, como a ANATEL (Agência Nacional de Telecomunicações) no Brasil e a FCC (*Federal Communications Commission*) nos Estados Unidos de forma estática [1, 2]. Uma parte significativa das frequências é atribuída através de licenças a empresas privadas de telecomunicação e instituições governamentais, resultando na escassez do espectro e limitando a escalabilidade necessária para suportar novos serviços e aplicações [2]. Análises recentes demonstram que esta forma de alocação subutiliza o espectro, permitindo a existência de frequências ociosas em determinados momentos (também chamadas de *"espaços em branco"* ou *"white spaces"*), como mostrado em [3, 4]. Tal comportamento tem motivado o desenvolvimento e o uso de mecanismos oportunistas e cognitivos a fim de aproveitar melhor a capacidade do espectro de radiofrequências [5, 6].

A tecnologia de rádio cognitivo (RC) é um novo paradigma na comunicação sem fio que permite um melhor aproveitamento do espectro de radiofrequências [7]. A RC permite implantar em um dispositivo computacional um sistema de comunicação flexível capaz de reconfigurar e adaptar seus parâmetros de transmissão e recepção [8]. Esta adaptação é realizada provendo as funcionalidades da RC, como o gerenciamento, o sensoreamento, a decisão, o compartilhamento e a mobilidade no espectro [9, 10, 11]. Estes benefícios têm motivado a utilização da tecnologia RC para comunicação entre os dispositivos computacionais formando as redes de rádio cognitivo [12].

As redes de rádio cognitivo são compostas por dispositivos (nós) utilizando a tecnologia RC e capazes de monitorar e identificar as frequências ociosas no espectro [13]. Com base em medições e em conhecimentos adquiridos através do histórico de acontecimentos passados, cada nó pode escolher e acessar os espaços em branco do espectro de forma inteligente [14]. Uma rede de rádio cognitivo pode ser organizada seguindo uma arquitetura centralizada ou uma arquitetura descentralizada. Uma arquitetura centralizada é composta por uma estação base central que gerencia os nós da rede e o seu uso do espectro. Na arquitetura descentralizada, cada nó é responsável pelo seu próprio gerenciamento na rede e pelas decisões de como utilizar os espaços em branco do espectro. Desta forma, uma arquitetura descentralizada forma uma **rede ad hoc de rádio cognitivo** (CRAHN, do inglês, *Cognitive Radio Ad Hoc Networks*) [9, 15].

Dois tipos de usuários compartilham o espectro de radiofrequências no contexto de redes de rádio cognitivo, sendo chamados de usuários primários (UP) e usuários secundários ou cognitivos (US) [16]. Os usuários primários possuem licenças de uso das bandas e prio-

ridade para acessá-las, enquanto os usuários secundários não possuem licenças, mas podem usar as bandas quando estas estiverem ociosas. Entretanto, por determinação das agências reguladoras, os usuários secundários não devem causar interferências na comunicação dos usuários primários [17, 18]. Desta forma, os nós de uma CRAHN devem monitorar constantemente o meio a fim de detectar a presença de um usuário primário no canal utilizado. Nos casos em que um usuário primário seja detectado, o usuário secundário deve mudar rapidamente para outro canal [19], resultando em uma interrupção temporal das conexões entre os nós de uma CRAHN até que um novo canal seja selecionado para continuar a comunicação.

Além de realizar um melhor aproveitamento das frequências ociosas do espectro, as CRAHNs beneficiam diretamente os usuários finais. Estas redes utilizam melhor o espectro, podendo prover uma melhor Qualidade de Serviço (QoS, do inglês, *Quality of Service*), melhores tempos de resposta, ampla cobertura, acesso ao meio eficiente e outros [20]. Uma vantagem da CRAHN em relação a uma rede tradicional é a baixa latência que ela gera em sua transmissão [21].

1.1 Problema

As CRAHNs são vulneráveis a diversos tipos de ataques devido às características do meio de comunicação sem fio e à forma de organização deste tipo de rede [22]. Estes ataques podem ser classificados seguindo as camadas da pilha de protocolo [23]. Exemplos são os ataques de Negação de Serviço (DoS, do inglês *Denial of Service*) que podem atuar nas camadas física e enlace gerando uma interrupção na comunicação dos nós da rede, tais como os ataques *jamming*, os ataques EUP (Emulação de Usuário Primário), o OFA (*Objective Function Attack*), o CCDA (*Common Control Data Attacks*) e outros. Por outro lado, existem ataques de manipulação de dados que afetam a camada de enlace, como os ataques de *Spoofing/Sybil*, injeção de pacotes, *false feedback* e outros [24]. Ataques, como *Jellyfish* e *Lion*, atuam na camada de transporte, degradando as conexões TCP dentro de uma CRAHN [25].

O ataque de **Emulação de Usuário Primário (EUP)** é um dos mais peculiares nas CRAHNs [25, 26, 27]. Estes ataques podem ser gerados por usuários secundários mal intencionados – maliciosos ou egoístas – com o objetivo de maximizar o seu uso do espectro [28]. No ataque EUP, um usuário secundário mal intencionado manipula o seu rádio para imitar o comportamento de um usuário primário legítimo. Por exemplo, um usuário mal intencionado pode alterar a potência de transmissão, o tipo de modulação, a frequência utilizada, a largura de banda, a taxa de transmissão, entre outros. Este ataque gera uma degradação na oportunidade de acesso ao espectro dos usuários secundários legítimos [17, 29].

Desenvolver soluções para a detecção ou mitigação dos usuários secundários mal in-

tencionados gerando ataques de emulação de usuários primários é de grande importância nas CRAHNs. Estes ataques são difíceis de detectar pelo fato dos usuários secundários mal intencionados poderem modificar sua interface de rádio para imitar as características de um usuário primário e causar uma identificação errônea pelos usuários secundários legítimos [28]. Os trabalhos na literatura propõem soluções de contramedida frente aos ataques EUP seguindo abordagens não-cooperativas ou cooperativas em arquiteturas centralizadas ou descentralizadas. Inicialmente, esses trabalhos focaram em abordagens centralizadas não-cooperativas gerando uma alta latência e um ponto de falha na estação base [17, 28, 29, 30, 31]. Dessa forma, surgiram os modelos cooperativos centralizados que conseguiram diminuir a latência de decisão, mas não a existência do ponto de falhas [32, 33, 34].

Por outro lado, os esquemas não-cooperativos e descentralizados foram propostos em paralelo. Estes apresentam um maior desempenho podendo neutralizar as dificuldades das soluções que seguem uma abordagem centralizada. Nas abordagens não-cooperativas descentralizadas [22, 35], cada nó realiza individualmente a detecção do ataque EUP, podendo gerar uma alta taxa de falsos positivos e falsos negativos. Para combater esses problemas, as abordagens *cooperativas* em arquiteturas *descentralizadas* foram propostas [26]. Contudo, as soluções na literatura além de considerar abordagens cooperativas ou não-cooperativas, apresentam análises de um único critério, e esses podem levar a uma errônea identificação do ataque [17, 28, 29, 31], estes erros acontecem pelo fato de considerar este critério como o único dado para determinar a ocorrência de um ataque EUP na rede. Por tal motivo, é necessário fornecer uma solução que considere as vantagens de cada proposta apresentada na literatura conjuntamente como uma análise de múltiplos critérios para determinar a presença do ataque EUP nas redes ad hoc de rádio cognitivo.

1.2 Objetivos

Este trabalho tem como objetivo principal identificar a presença dos ataques EUPs nos canais de radiofrequências. Além disso, ele visa reduzir as altas taxas de falsos positivos e falsos negativos resultantes dos esquemas atualmente existentes na literatura. Para alcançar este objetivo propomos um esquema para anál**I**se **M**ulticritério e **C**ooperativa da presença de **A**taques EUP em redes ad hoc de rádio cognitivo, denominado de $IMCA$. O esquema segue uma abordagem cooperativa com uma arquitetura descentralizada.

O esquema $IMCA$ é composto de duas fases. A primeira fase do esquema, denominada de *individual*, realiza um sensoreamento do espectro com o objetivo de coletar dados. Estes dados formam um conjunto de valores para cada critério estabelecido pelo esquema $IMCA$. Após a coleta, o esquema realiza uma análise de múltiplos critérios (MCDM ou MCDA, do inglês, *Multiple-criteria decision-making* ou *Multiple-criteria decision analysis*). A análise baseada em múltiplos critérios pretende tornar mais eficiente

a identificação dos atacantes na rede. O esquema $IMCA$ emprega o método NWAUF (do inglês, *Normalized Weighted Additive Utility Function*), que tem como entrada as amostras coletadas no sensoreamento para os critérios, para obter um consenso entre os diferentes tipos de valores coletados. Para esse consenso, o método NWAUF realiza uma normalização dos valores dos critérios e adiciona pesos de importância a cada um dos critérios e, finalmente, determina uma probabilidade preliminar da presença do ataque. Esses pesos de importância são determinados utilizando o método de PCA (do inglês, *Principal Component Analysis*), que especifica diferentes pesos de importância seguindo o grau de correlação entre os critérios.

A segunda fase do esquema, denominada de *cooperação*, define uma abordagem cooperativa para melhorar a probabilidade da presença do ataque EUP. Para isto, a segunda fase começa com uma troca das probabilidades preliminares entre os nós vizinhos da rede. Isto é, um nó envia sua probabilidade preliminar para seus vizinhos, e da mesma forma, os vizinhos respondem com suas probabilidades preliminares. Após a troca de probabilidades preliminares, cada nó realiza um cálculo da probabilidade final da presença do ataque EUP na rede ad hoc de rádio cognitivo. O cálculo é realizado por uma técnica de fusão de informação, o teorema de Bayes.

1.3 Contribuições

As contribuições deste trabalho são:

- A aferição das vulnerabilidades de uma rede ad hoc de rádio cognitivo diante de ataques de emulação de usuário primário. Essas análises possibilitaram o entendimento das necessidades da segurança em tais redes.

- A proposta e a especificação do esquema $IMCA$, um esquema de múlt***I***plos critérios para a***N***álise ***C***ooperativa da presença de ***A***taques EUP em redes ad hoc de rádio cognitivo. Este esquema permite determinar a probabilidade do sucesso do ataque EUP.

- A comparação do esquema $IMCA$ frente a um esquema monocritério, representando os esquemas atualmente abordados na literatura. Esta avaliação mostrou que o esquema $IMCA$ apresenta resultados relevantes.

- A extensão do módulo CRAHN [36] no simulador de rede NS-2 com o desenvolvimento do esquema $IMCA$, provendo uma ferramenta para a determinação da presença de ataques EUP. Esta extensão está integrada aos demais módulos do simulador e será disponibilizada.

1.4 Estrutura da dissertação

Esta dissertação está organizada em seis capítulos. O Capítulo 2 apresenta os fundamentos da tecnologia e de redes de rádio cognitivo. Ele enfatiza o funcionamento das redes ad hoc de rádio cognitivo e relata as vulnerabilidades desse tipo de redes. O Capítulo 3 descreve os trabalhos relacionados. Nele, são descritos os esquemas para a detecção ou mitigação de ataques EUPs. Além disso, realiza-se uma classificação dos esquemas pelo modo de abordagem aplicada. O Capítulo 4 apresenta um esquema para anál**I**se **M**ulticritério e **C**ooperativa da presença de **A**taques EUP em redes ad hoc de rádio cognitivo. Esse esquema é denominado de $IMCA$, e os detalhes de seu funcionamento são descritos. O Capítulo 5 avalia o uso do esquema $IMCA$ para a análise da presença de ataques EUP e apresenta os resultados. Por fim, o Capítulo 6 descreve as considerações finais e os trabalhos futuros.

CAPÍTULO 2

FUNDAMENTOS

Este capítulo revisa os conceitos necessários para o entendimento do problema tratado neste trabalho e da solução proposta. A Seção 2.1 aborda as características da tecnologia de rádio cognitivo. Além disso, ela descreve o funcionamento das redes de rádio cognitivo, ressaltando suas arquiteturas e, em especial, as redes ad hoc de rádio cognitivo. A Seção 2.2 relata as vulnerabilidades de segurança nas redes ad hoc de rádio cognitivo e classifica os diferentes tipos de ataques, enfatizando o ataque de emulação de usuário primário (EUP). A Seção 2.3 classifica as técnicas de sensoreamento do espectro de radiofrequências. A Seção 2.4 apresenta o método utilizado para a análise de múltiplos critérios, neste trabalho também descreve o teorema de probabilidade condicional aplicado para a determinação da probabilidade da presença de ataques EUP nas redes ad hoc de rádio cognitivo.

2.1 A tecnologia de rádio cognitivo

O espectro de radiofrequências é um recurso natural e um meio de transmissão/recepção das comunicações sem fio. Estas frequências são utilizadas pelos usuários autorizados através de licenças [37]. No entanto, o crescimento e o amplo uso das tecnologias sem fio tornam o espectro um recurso escasso devido à alocação de frequências. Apesar desta escassez, estudos demonstram uma alta subutilização das frequências licenciadas. Esta subutilização do espectro é caracterizada pela ociosidade no uso do espectro em alguns períodos de tempo. Estes tempos ociosos podem ser melhor aproveitados pelos usuários secundários (US) (usuários não licenciados), como mostra a Figura 2.1 [38, 39].

A tecnologia de rádio cognitivo (RC) verifica o espectro para reconhecer a variação do meio de forma inteligente e reconfigurar seus parâmetros para a reutilização dos espaços ociosos deixados pelos usuários primários [13, 14]. Para o procedimento de verificação do espectro considera-se as funcionalidades básicas da RC, como o gerenciamento, o sensoreamento, a decisão, o compartilhamento e a mobilidade do espectro [9, 8, 10, 11]. Em seguida, cada uma destas funções é descrita, e a Figura 2.2 ilustra estas funcionalidades da RC.

- **Sensoreamento**
  O sensoreamento do espectro permite o monitoramento as bandas licenciadas disponíveis. Este realiza a detecção do início e fim das atividades licenciadas, além de identificar os espaços ociosos do espectro. O sensoreamento captura a informação

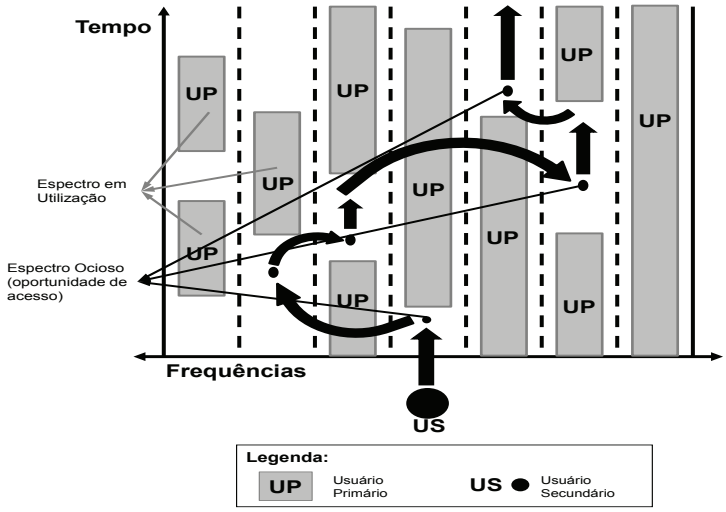


Figura 2.1: Oportunidade de acesso ao espectro

que serve como entrada para a função de decisão. Alguns das técnicas de sensoreamento são apresentadas em [40, 41, 42].

- **Decisão**

  Para realizar uma comunicação, o rádio cognitivo utiliza um canal que pode ser alterado de acordo com as condições da rede. Para isto, a decisão de ocupar um canal ocorre através da função de gerenciamento com base nas informações do sensoreamento do espectro. A função de decisão é o preâmbulo da função de compartilhamento. Alguns algoritmos para a decisão espectral são apresentados em [43, 44, 45, 46].

- **Compartilhamento**

  Devido à existência de vários rádios cognitivos querendo acessar o espectro de radiofrequências ao mesmo tempo, a RC deve coordenar os rádios cognitivos de modo que estes não colidam entre eles ou com os usuários licenciados. Esta função permite ao rádio garantir a repartição do espectro entre os usuários primários e secundários de acordo com o tipo de técnica de acesso ao espectro, podendo ser superposto (*overlay*) ou sobreposto (*underlay*). Algumas destas técnicas de compartilhamento do espectro são apresentadas em [47, 48].

- **Mobilidade**

  Todos os rádios cognitivos são catalogados como visitantes no espectro. Portanto, a mobilidade do espectro é o processo de desocupar um canal que está sendo utilizado por um visitante e levar o visitante para outro canal. Esta mudança acontece devido às malas condições do canal ou pelo início da atividade de um usuário primário em sua banda licenciada. A RC tem que garantir aos terminais de rádio operar nas

melhores bandas de frequência. Os trabalhos em [49, 50] apresentam os algoritmos para realizar a mobilidade no espectro.

- **Gerenciamento**
  O gerenciamento do espectro é a função que monitora e controla as demais funções. Esta determina quando uma das funcionalidades mencionadas anteriormente entra em ação. Além disso, ela tem que garantir e satisfazer a comunicação entre os usuários, sendo a melhor possível em termos de qualidade de serviço (QoS). Os trabalhos em [9, 51, 52, 53] apresentam uma revisão dos algoritmos empregados para o gerenciamento do espectro.

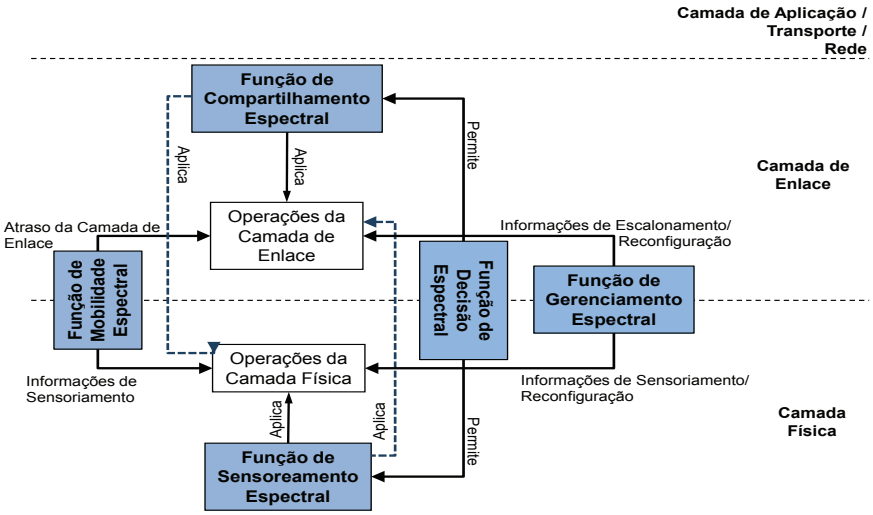


Figura 2.2: Funcionalidades da tecnologia de rádio cognitivo

2.1.1 Redes de rádio cognitivo

As redes de rádio cognitivo têm como objetivo eliminar as limitações de acesso dinâmico ao espectro das redes tradicionais, permitindo aperfeiçoar o uso do espectro e consequentemente o seu desempenho [54, 55]. Para isto, os nós de uma rede de rádio cognitivo utilizam a tecnologia RC para adaptar suas configurações de rádio às mudanças permanentes no meio de transmissão e ter um melhor aproveitamento do uso do espectro [39]. Contudo, a rede de rádio cognitivo captura as condições do espectro para depois planejar, decidir e atuar no espectro, levando em consideração os usuários (primários e secundários) compartilhando o meio[38].

A arquitetura de uma rede de rádio cognitivo apresenta dois tipos de usuário que compartilham o espectro. Um usuário autorizado para o uso prioritário das bandas licenciadas, denominado de usuário primário (UP) e o usuário secundário (US), que não

possui prioridade no uso das bandas de frequências, mas as utilizam quando estas estiveram ociosas. A rede de rádio cognitivo é composta por estes usuários que aplicam a tecnologia RC. Um US transmissor inicia o sensoreamento do espectro e depois decide qual canal licenciado ele utilizará para realizar sua transmissão. Para isto, o US transmissor comunica ao US receptor o canal que será utilizado enviando um pacote de controle por um canal de controle comum. Depois o US receptor responde com um outro pacote de controle confirmando a recepção e a configuração do canal, esta resposta é feita pelo canal estabelecido para os transmissores. Em seguida, o US transmissor acessa o canal e pode compartilha-lo com outros usuários secundários, dependendo do tipo de técnica de acesso ao meio. Os USs ao detectarem a presença de um UP no mesmo canal de transmissão devem evitar interferências e mudar para outro canal no espectro de radiofrequências, utilizando assim outras funcionalidades de uma RC [12]. Com isso, as redes de rádio cognitivo proporcionam um ótimo desempenho aos USs em termos de gestão de recursos, qualidade de serviço (QoS), segurança, controle de acesso ao meio [39].

Entretanto, o processo de comunicação entre os USs da rede dependerá diretamente do tipo de arquitetura da rede de rádio cognitivo. Nestas arquiteturas encontramos dois tipos: centralizada e descentralizada ou distribuída [9, 16, 25, 15]. Estes dois modelos de arquiteturas são descritos em seguida.

- **Arquitetura centralizada**

  Na arquitetura centralizada, uma estação base ou centro de fusão gerencia a informação coletada pelos USs. Estes USs são dispostos na rede e ficam monitorando o meio a fim de coletar informação. Esta informação é retornada à estação base com o objetivo de determinar as ações a tomar aplicando as funcionalidades da tecnologia RC.

- **Arquitetura distribuída**

  Na arquitetura distribuída, os USs não precisam de uma estação base. Cada US é independente de outro e gerencia suas próprias funcionalidade da tecnologia RC. Este tipo de arquitetura representa uma rede ad hoc de rádio cognitivo (CRAHNs, do inglês, *Cognitive Radio Ad Hoc Network*). As CRAHNs apresentam vários desafios pelo fato de cada US ser responsável pelo seu próprio gerenciamento do espectro. Estes desafios compreendem: custo de coleta de informação gerando uma latência na camada de enlace, o consumo de energia pela característica de apresentar um modo ad hoc, a taxa de mensagens de atualização para manter um correto estado da rede. Por outro lado, este modelo de arquitetura utiliza um canal de controle comum para manter a comunicação de mensagens de controle. Este canal de controle abre outro desafio, porque ele tem que ser devidamente escolhido para não sobrecarregar o canal e gerar latências na comunicação [51].

Contudo, as CRAHNs apesar de apresentar desafios, também possuem vantagens em termos de cooperação. Pela falta de suporte centralizado, a CRAHN deve confiar na observação local de cada US, para determinar suas ações. Para superar esse conhecimento limitado da topologia da rede, todas as decisões do espectro são baseadas em operações cooperativas. Os USs determinam suas ações com base em informações trocadas sobre as observações de seus vizinhos. Além disso, este modelo de arquitetura oferece uma menor complexidade em sua implementação pelo fato de só exigir informações dos USs e não de uma unidade centralizadora. O tempo de decisão de uma ação é menor do que uma arquitetura centralizada [53]. Cabe destacar que este trabalho aborda sua proposta sob este tipo de arquitetura.

A Figura 2.3 ilustra as duas diferentes arquiteturas existentes para as redes de rádio cognitivo. Observamos uma arquitetura centralizada contendo a estação base e os usuários secundários. Por outro lado, apresentamos a arquitetura descentralizada, que é composta apenas por usuários secundários autônomos.

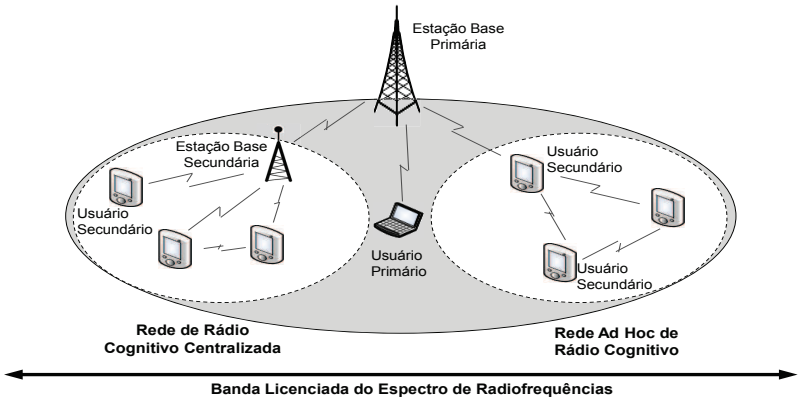


Figura 2.3: Arquiteturas das redes de rádio cognitivo

2.2 Vulnerabilidades de segurança

Apesar das vantagens das redes ad hoc de rádio cognitivo estas são vulneráveis a diversos tipos de ataques, pois o espectro de radiofrequências licenciadas utilizado pelos usuários secundários pode ser facilmente comprometido por um ou vários atacantes. Os ataques podem resultar na injeção de dados falsos no momento da troca de informação de detecção, da emulação de um usuário primário, aproveitando o espectro de forma egoísta ou maliciosa. No contexto das redes ad hoc de rádio cognitivo, realizamos nossa própria classificação dos diferentes ataques que acontecem na rede, seguindo as definições e classificações realizadas pelos autores: Clancy e Goergen, Zhang e Li, Leon et al., e Araujo et al., e considerando as camadas da pilha de protocolo [24, 25, 56, 57].

- **Camada de transporte**
  Os ataques desta camada acontecem quando um sistema criptográfico foi comprometido. Estes ataques podem afetar diretamente ao protocolo de controle de transmissão (TCP, do inglês, *Transmission Control Protocol*), resultando em uma degradação do TCP e obrigando uma mudança de canal pelo US legítimo.

- **Camada de rede**
  Nesta camada os ataques afetam à criptografia na transmissão empregada. Como em uma rede ad hoc de rádio cognitivo os nós são móveis e um desafio crucial é o consumo de energia, os nós não têm recursos suficientes para utilizar um mecanismo criptográfico poderoso e são vulneráveis a ataques. O objetivo principal destes ataques é obter a chave criptográfica da transmissão.

- **Camada de enlace**
  Os ataques nesta camada podem gerar uma decisão errônea do estado atual do espectro de radiofrequências. Isto acontece quando os USs da rede trocam informação de sensoreamento, mas esta informação trocada pode ser comprometida por ataques na camada de enlace,que podem injetar dados falsos, modificar dados ou eliminalos. A informação coletada através da troca entre vários nós pode resultar em uma decisão errônea acerca da banda de frequência que o US quer utilizar, e pode gerar interferências na comunicação de outros USs ou em um caso pior gerar uma colisão com o UP legítimo.

- **Camada física**
  Nesta camada destacam-se os ataques de negação de serviço (DoS, do inglês, *Denial of Service*). Alguns destes ataques têm por objetivo tentar imitar algumas das características de um usuário legítimo de um serviço. Outros ataques podem gerar uma alta interferência, devido ao fato dos atacantes poderem ficar ocupando os canais como USs simples, dificultando a comunicação entre os USs legítimos.

A Tabela 2.1 apresenta alguns dos ataques às redes ad hoc de rádio cognitivo. Estes são classificados de acordo com as camadas da pilha de protocolo como foi descrito anteriormente. Dentre esta classificação, focamos nas vulnerabilidades da camada de física, pelo fato de representarem um grande desafio, visto que um atacante pode comprometer a camada física e posteriormente repercutir nas camadas superiores chegando assim a tomar uma decisão errônea sobre o estado atual do espectro.

2.2.1 Ataque de emulação de usuário primário

O ataque de emulação de usuário primário (EUP) foi inicialmente apresentado por Chen e Park [28] e afeta diretamente a camada física. Este ataque é realizado por usuários

Tabela 2.1: Ataques em redes ad hoc de rádio cognitivo

Camada	Tipo de ataque
Física	Jamming
	EUP
	OFA
	CCDA
Enlace/Rede	Spoofing/Sybil
	Packet injection
	Selective forwarding
	False feedback
	Worm/Sink/Grey/Black - hole
	Flooding
	Power consumption
Transporte	Jellyfish
	Lion

secundários mal intencionados que manipulam seus rádios para terem comportamentos e características similares às transmissões de usuários primários [17, 29]. Isto se deve ao fato dos rádios cognitivos possibilitarem a reconfiguração das interfaces de rádio. Um atacante equipado com a tecnologia RC pode modificar sua interface e imitar as características do sinal do usuário primário. Esta modificação permite aos usuários secundários legítimos identificarem de forma incorreta um usuário secundário como um usuário primário, resultando em um ataque EUP [38]. As pesquisas mostram que um ataque EUP pode afetar seriamente o desempenho do espectro e reduzir significativamente a disponibilidade de canais legítimos aos usuários secundários, acontecendo uma negação de serviço [24, 25].

Um ataque EUP pode ser gerado por dois tipos de usuários secundários mal intencionados: (i) usuário malicioso, que tem como objetivo comprometer o funcionamento da rede, e (ii) usuário egoísta, que se beneficia dos privilégios que este possui para estabelecer uma comunicação exclusiva com outro usuário [28]. Estas duas ações mal intencionadas reduzem significativamente os recursos disponíveis de acesso ao meio para os usuários secundários legítimos. Além disso, elas comprometem as funcionalidades cognitivas destes usuários [29, 39].

A Figura 2.4 ilustra o espectro licenciado por usuários primários sendo acessado por um usuário secundário legítimo. O US realiza o sensoreamento do espectro e acessa as frequências ociosas no espectro. Quando um usuário primário entra em atividade em sua banda licenciada, o US muda para outra frequência ociosa do espectro. Os ataques EUPs (representados pelas caveiras na Figura 2.4) são realizados em diferentes faixas de frequências, ocupando os espaços em branco do espectro e tornando o espectro ocupado. Os USs legítimos detectam estas atividades dos atacantes como atividades de UPs legítimos, perdendo assim oportunidades de acesso ao espectro.

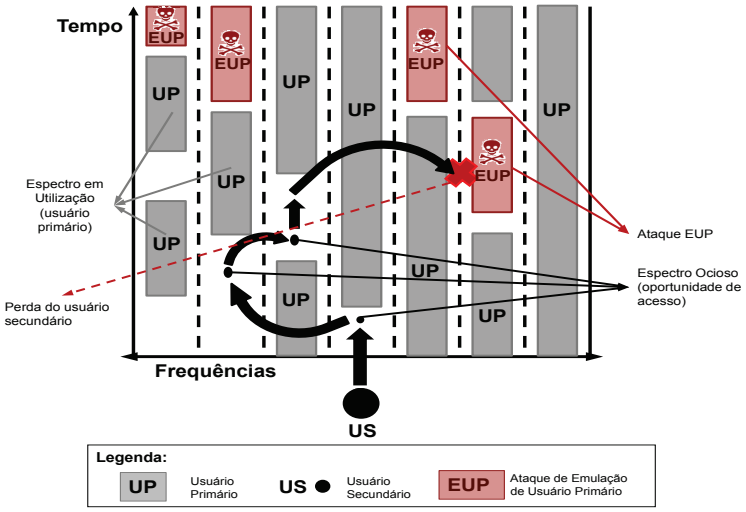


Figura 2.4: Presença do ataque EUP na rede de rádio cognitivo

2.3 Técnicas de sensoreamento do espectro

Existem diversas técnicas utilizadas para o sensoreamento do espectro de radiofrequências em redes de rádio cognitivo com o objetivo de detectar a presença de usuários primários legítimos no espectro. Em geral, estas técnicas têm como referência as características de transmissão do sinal primário. Estas características podem ser a potência de transmissão, a potência de recepção, o tipo de onda do sinal, o modulação, a amplitude, a localização do transmissor, entre outras características. As técnicas de detecção são classificadas como: não-cooperativas e cooperativas [40].

No entanto, nas técnicas de sensoreamento não-cooperativas um usuário secundário não conseguiria identificar uma transmissão primária devido ao desvanecimento do canal ou obstáculos na transmissão [38]. Consequentemente, para realizar uma detecção com obstáculos presentes, as técnicas de sensoreamento evoluíram precisando de informação sobre a detecção de usuários primários provenientes de outros usuários secundários cooperativos. A Figura 2.5 apresenta a classificação das técnicas de sensoreamento do espectro. A seguir, estas técnicas são classificadas e descritas conforme são expostas na literatura [38, 40].

2.3.1 Técnicas de sensoreamento do espectro não-cooperativas

Em uma abordagem não-cooperativa, os usuários secundários são dispostos na rede, sendo cada um destes capaz de realizar seu sensoreamento do espectro com o objetivo de detectar a presença de um UP. Este sensoreamento é realizado na banda de frequência indicada para o acesso ao espectro. Estas técnicas de detecção identificam as características da transmissão do sinal primário para decidir sobre o tipo de usuário presente na rede. Em seguida, são apresentadas as principais técnicas de sensoreamento não-cooperativas:

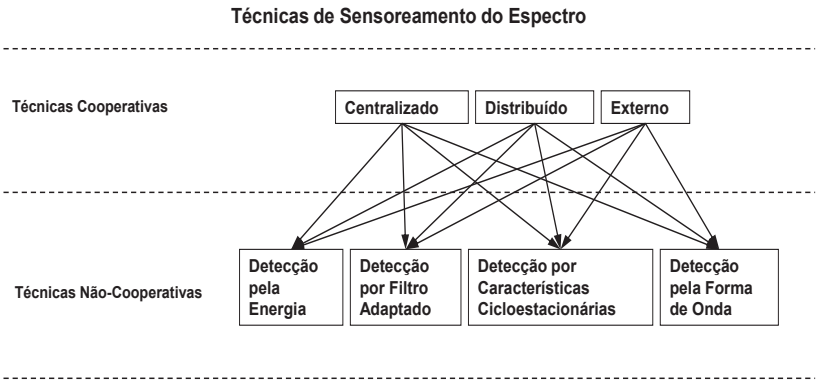


Figura 2.5: Técnicas de sensoreamento do espectro nas redes de rádio cognitivo

- **Detecção baseada na energia**

  A detecção pela energia é a técnica mais comum por seu baixo custo computacional e sua fácil implementação comparada a outras [41, 58, 59, 60, 61]. Além dessas vantagens, esta técnica é mais genérica porque não precisa de um conhecimento prévio do sinal do UP [62]. O sinal é detectado seguindo duas hipóteses como é definido na Equação 2.1 e comparado com limiares estabelecidos como é visto na Equação 2.2 [63].

  Na Equação 2.1, observamos H_0 e H_1 denominadas de hipóteses da detecção do sinal do UP. Sendo, H_0 a hipótese que apresenta a ausência do sinal do UP, e H_1 a hipótese que representa a presença do sinal do UP. Nas hipóteses, observa-se que $s(n)$ é o sinal a ser detectado, $w(n)$ é a adição do ruído Gaussiano, e n representa o índice de amostras. Se $s(n) = 0$, não acontecerá uma transmissão pelo usuário primário. Estas duas hipóteses (H_0 e H_1) são comparadas com um limiar denotado por μ e λ para obter o resultado da detecção denotado por D e representado na Equação 2.2.

$$\begin{aligned} H_0 &: y(n) = w(n), \\ H_1 &: y(n) = s(n) + w(n) \end{aligned} \tag{2.1}$$

$$D = \begin{cases} 1 & \mu > \lambda \\ -1 & \mu < \lambda \end{cases} \tag{2.2}$$

  A técnica de detecção pela energia pode permitir o estudo de duas probabilidades adicionais. Estas são a probabilidade de detecção P_D e a probabilidade de falso positivo P_F. P_D é a probabilidade de detectar o sinal na banda de frequência, quando realmente existe em atividade. P_F é a probabilidade de que o resultado de verificação seja incorreto porque se decide que a frequência é considerada ocupada, quando na realidade ela não está. Estas probabilidades são denotadas na Equação 2.3.

$$\begin{cases} P_D &= Pr(\mu > \lambda | H_1) \\ P_F &= Pr(\mu > \lambda | H_0) \end{cases} \tag{2.3}$$

P_F tem que ser o menor valor possível para evitar a detecção errônea de atividade no espectro. No entanto, se um ruído branco (ruído produzido pela combinação simultânea de sons de todas as frequências) está presente na transmissão, este pode ser modelado por uma variável aleatória de média-zero Gaussiana com variança σ_w^2, i.e. $w(n) = N(0, \sigma_w^2)$. Por simplicidade, pode-se modelar o sinal como uma variável de média-zero Gaussiana $s(n) = N(0, \sigma_s^2)$. Entretanto, a perda de propagação precisa ser considerada gerando uma maior complexidade. Para isto, considera-se uma distribuição Qui-Quadrado com $2N$ graus de liberdade X_{2N}^2 mostrada na Equação 2.4 [64].

$$M = \begin{cases} \frac{\sigma_w^2}{2} X_{2N}^2 & H_0, \\ \frac{\sigma_w^2 + \sigma_s^2}{2} X_{2N}^2 & H_1. \end{cases} \tag{2.4}$$

- **Detecção por filtro adaptado**
  É conhecido como um ótimo método de detecção de usuários primários quando o sinal transmitido é conhecido [65]. A principal vantagem deste método é o tempo que utiliza para obter uma probabilidade de falso-positivo ou uma probabilidade de perda de detecção ao compará-lo com outros métodos [66]. O filtro adaptado pode extrair informação do sinal primário, como o tipo de modulação, a forma do pulso e o formato do pacote para otimizar a probabilidade de detecção. No entanto, este método exige o conhecimento prévio do sinal do usuário primário, e seu desempenho é comprometido se o conhecimento não for exato. Além disso, devido às necessidades de receptores de rádio cognitivo para todos os tipos de sinais, a complexidade da implementação da unidade de detecção é muito grande. Outra desvantagem do filtro adaptado é o alto consumo de energia por parte dos algoritmos utilizados [40].

- **Detecção por características cicloestacionárias**
  É um método para detectar transmissões primárias, aproveitando as características cicloestacionárias do sinal recebido [8, 40, 67]. A técnica incorpora a periodicidade dos sinais modulados, onda sinusoidal, ciclos prefixados que possibilita a detecção do sinal principal pela análise da função da correlação espectral do sinal transmitido. Os algoritmos baseados na detecção cicloestacionária podem diferenciar melhor o ruído dos sinais dos usuários primários, sendo melhor que a detecção pela energia [67]. No entanto, a detecção cicloestacionária requer maior complexidade computacional e maior tempo de observação. Além disso, a técnica cicloestacionária é utilizada para distinguir entre diferentes tipos de transmissores e os usuários primários

[68]. O ciclo de densidade espectral (CSD) em função do sinal recebido pode ser calculado pela Equação 2.5.

$$S(f,\alpha) = \sum_{\tau=-\infty}^{\infty} R_y^{\alpha}(\tau) e^{-j2\pi f\tau}, l \tag{2.5}$$

sendo,

$$R_y^{\alpha}(\tau) = E[y(n+\tau)y*(n-\tau)e^{-j2\pi\alpha n}] \tag{2.6}$$

uma função de correlação cíclica (CAF) denotada por f, e α é a frequência cíclica. A função CSD oferece valores máximos quando a frequência cíclica é igual às frequências fundamentais do sinal transmitido. As frequências cíclicas podem ser conhecidas, ou podem ser extraídas e utilizadas como características para a identificação dos sinais transmitidos [69, 70].

- **Detecção pela forma de onda**
  Os padrões de onda são normalmente conhecidos e utilizados em sistemas sem fio para ajudar na sincronização ou para outros fins. Estes padrões incluem preâmbulos, midâmbulo, dados de controle regularmente transmitidos, sequências, etc. Um preâmbulo é uma sequência conhecida transmitida antes de cada intervalo de tempo, e um midâmbulo é transmitida no meio de um intervalo de tempo. Com a presença de um padrão conhecido, a detecção pode ser realizada através da correlação do sinal recebido comparado com uma cópia do sinal conhecido [63]. Este sistema supera o sistema de detecção pela energia [71]. Além disso, o desempenho da detecção pela forma de onda aumenta na medida em que o padrão conhecido seja maior.

  Utilizando o mesmo modelo de detecção pela energia $y(n) = s(n) + w(n)$, a métrica de detecção pela forma de onda pode ser obtida pela Equação 2.7.

$$M = Re[\sum_{n=1}^{N} y(n)s^*(n)] \tag{2.7}$$

  Onde $*$ representa a operação de junção. Na ausência do usuário primário, a métrica pode ser avaliada como a Equação 2.8.

$$M = Re[\sum_{n=1}^{N} w(n)s^*(n)] \tag{2.8}$$

  Similarmente, na presença do sinal do usuário primário, a métrica de sensoreamento é representada pela Equação 2.9

$$M = \sum_{n=1}^{N} |s(n)|^2 + Re[\sum_{n=1}^{N} w(n)s^*(n)] \tag{2.9}$$

A decisão sobre a presença do usuário primário pode ser realizada comparando o resultado da métrica M com um limiar λ. Esta detecção baseada na forma da onda do sinal é efetiva, mas a desvantagem consiste na necessidade de conhecimentos prévios dos preâmbulos e midâmbulos da onda para poder realizar a detecção. Além disso, esta técnica se mostra menos eficiente em relação à técnica de detecção pela energia por exigir um conhecimento prévio das características do sinal transmitido [40].

2.3.2 Técnicas cooperativas de sensoreamento do espectro

As técnicas cooperativas são propostas na literatura como a solução aos problemas que surgem no espectro devido ao ruído, desvanecimento do canal ou obstáculos na transmissão. A abordagem cooperativa coleta e incorpora informações do sensoreamento de vários usuários secundários, a fim de melhorar o desempenho do sensoreamento do espectro [60, 72, 73]. Esta abordagem reduz consideravelmente as probabilidades de perdas de detecção do UP e falsos positivos. Além disso, a detecção cooperativa pode diminuir o tempo de detecção [74].

As técnicas de sensoreamento cooperativas incluem o desenvolvimento de algoritmos eficientes de maior complexidade computacional [74, 75]. Nas soluções de sensoreamento cooperativa, um canal de controle pode ser usado em diferentes tipos de bandas de frequências. Dependendo dos requisitos do sistema, um canal de controle pode ser implementado. O canal de controle pode ser utilizado para o compartilhamento dos resultados do sensoreamento do espectro entre os usuários secundários. Várias soluções de canais de controle são propostas na literatura de rádio cognitivo [76], [77]. Um acesso múltiplo por divisão de tempo (TDMA) baseado em um protocolo para a troca de dados de sensoreamento é proposto em [78].

Por outro lado, o sensoreamento cooperativo é mais vantajoso pela cooperação existente entre os nós da rede. Além disso, este sensoreamento pode ser melhor aproveitado considerando a quantidade de nós cooperadores, isto é, quanto maior a quantidade de nós cooperadores melhor serão os resultados do sensoreamento [16]. Além disso, o sensoreamento cooperativo dependerá exclusivamente do tipo de arquitetura da rede de rádio cognitivo. As formas de sensoreamento cooperativo em uma rede de rádio cognitivo são descritas a seguir [16, 40].

- **Sensoreamento cooperativo centralizado**

  No sensoreamento centralizado, uma unidade central coleta a informação de detecção

dos usuários cognitivos, identifica o espectro disponível e emite esta informação para outros usuários cognitivos. Esta unidade central é conhecida como centro de fusão ou estação base. O resultado obtido no centro de fusão é calculado a partir das observações independentes de cada nó. Estas observações são transmitidas para o centro de fusão em forma binária a fim de reduzir a largura de banda. Além disso, apenas alguns dos usuários cognitivos com informação confiável são considerados pelo centro de fusão.

- **Sensoreamento cooperativo distribuído**
  O sensoreamento distribuído não precisa de um centro de fusão que coleta a informação. Esta informação de detecção é compartilhada entre os nós da rede, assim cada nó toma suas próprias decisões em relação à parte do espectro que pode ser utilizada. Este sensoreamento é mais vantajoso do que o sensoreamento centralizado no sentido de não requerer uma infraestrutura de rede de suporte e ter um custo reduzido. Como no sensoreamento centralizado, as decisões individuais são transmitidas em forma binária a fim de reduzir a largura de banda.

- **Sensoreamento cooperativo externo**
  No sensoreamento externo, os agentes realizam a detecção da atividade primária no canal licenciado, e transmitem a informação do canal monitorado aos nós da rede ou estação base, isto depende do tipo de arquitetura da rede. Estes agentes são representados por sensores. As principais vantagens dos sensores são as superações dos problemas do sombreamento. Além disso, os sensores diminuem o tempo de detecção do espectro por estar fora da rede.

2.4 Técnicas de análise de múltiplos critérios e análise condicional

Nesta seção, apresentam-se as técnicas empregadas para as análises sobre a presença do ataque EUP. Inicialmente, expomos uma técnica de análise de múltiplos critérios utilizada para determinar uma probabilidade preliminar da presença do ataque EUP. Além disso, descrevemos a técnica para determinar os pesos de importância para cada critério utilizada neste trabalho. Por fim, apresentamos a técnica de probabilidade condicional utilizada para determinar a probabilidade final da presença do ataque na rede.

2.4.1 Análise de múltiplos critérios

Uma técnica para a análise de múltiplos critérios pode seguir uma formalização da decisão do senso comum para problemas complexos que são informais [79]. A análise de múltiplos critérios (MCDM ou MCDA, do inglês, *Multiple-criteria decision-making* ou

Multiple-criteria decision analysis) é usada como um termo geral, cobrindo métodos que explicitamente procuram considerar vários critérios para ajudar os indivíduos ou grupos na avaliação holística de alternativas de decisão com objetivos diferentes e efeitos conflitantes em seus valores, auxiliando assim na tomada de decisões. A análise de múltiplos critérios utiliza vários métodos para encontrar a melhor alternativa [80].

O desenvolvimento da MCDA está intimamente relacionado com o avanço da tecnologia computacional. Por um lado, o rápido desenvolvimento da tecnologia computacional nos últimos anos tornou possível realizar uma análise sistemática dos problemas de MCDA complexo. Por outro lado, o uso generalizado de computadores e de tecnologia computacional tem gerado uma enorme quantidade de informação, o que torna o MCDA cada vez mais importante e útil no apoio à decisão [81].

O objetivo dos métodos de decisão MCDA é tomar a melhor decisão dentre diversas alternativas existentes para resolver um problema, considerando simultaneamente um conjunto de critérios de avaliação. Em particular, este trabalho emprega o método NWAUF (*Normalized Weighted Additive Utility Function*) [82], fundamentado nos estudos que mostram o seu baixo custo computacional em comparação a outros métodos MCDA, como o AHP (*Analytic Hierarchy Process*) [83] ou ELECTRE [84], e as suas respectivas variantes [82, 85].

- **Normalized Weighted Additive Utility Function**

  O processo de análise de múltiplos critérios envolve a escolha entre várias alternativas. Estas alternativas podem ser classificadas com base em vários critérios utilizando uma MCDA. Em geral, a metodologia MCDA envolve quatro etapas [82]:

  1. Identificar e avaliar valores de critérios.
  2. Identificar o conjunto de alternativas.
  3. Escolher e aplicar um método de classificação alternativa.
  4. Escolher a melhor alternativa.

  Para executar as etapas do MCDA aplicando o método NWAUF nas CRAHNs, os seguintes passos são realizados [82, 86, 87]:

  1. NWAUF define os valores mínimos e máximos para cada critério c coletados utilizando uma técnica de sensoreamento do espectro. Estes valores compõem, respectivamente, os conjuntos denotados por $\mathcal{MIN}$ e $\mathcal{MAX}$. Cada critério c contém um número de amostras. Sendo que $\mathcal{MIN}_z = c_{z,min}$ e $\mathcal{MAX}_z = c_{z,max}$, onde $z = 1, 2, 3, ...c$, por outro lado, min e max representam o valor mínimo e máximo dos conjuntos de amostras para cada critério c.

2. Cada critério c é normalizado em $c' = \frac{c_z - \mathcal{MIN}_z}{\mathcal{MAX}_z - \mathcal{MIN}_z}$. Note que os valores obtidos estão no intervalo entre 0 e 1.

3. Os pesos de importância para cada critério normalizado c' são adicionados e avaliados. Onde, a quantidade de pesos de importância é igual à quantidade de critérios. Além disso, cada peso w é representado em um intervalo [0,1] e a soma dos pesos precisa ser igual a 1. Isto é $\sum_{i=1}^{k} w_z = 1$, onde $w_z > 0 \; \forall \; z$.

4. Por fim, uma função de utilidade é calculada e denotada por U. O cálculo é alcançado seguindo a Equação 2.10, onde um somatório dos pesos de importância é utilizado conjuntamente com os critérios normalizados. esta utilidade calculada determina uma probabilidade, pelo fato de considerar pesos de importância sobre os valores coletados previamente.

$$U = \sum_{z=1}^{c} w_z c'_z, \; \forall \; z = 1, 2, ..., c \tag{2.10}$$

Contudo, NWAUF no passo de número 3 considera pesos de importância para cada critério. Isto é um ponto importante devido a estes pesos determinarem o grau de importância de um critério na decisão conjunta com outros. Para a obtenção destes pesos é utilizada a técnica de análise de componente principal (PCA, do inglês, *Principal-component analysis*), a qual é descrita a seguir.

- **Análise de componente principal**

PCA é uma técnica estatística usada para classificar os critérios pela soma de pesos de importância. A técnica identifica padrões nos conjuntos de critérios, e expressa esses critérios de forma que ressaltem suas similitudes e diferencias. Quando são encontrados esses padrões nos critérios, a técnica permite comprimir os critérios, reduzindo assim o número de dimensões dos critérios, sem perda de informação. [88]. A partir dessa redução da dimensionalidade, a técnica encontra as causas de variabilidades dos conjuntos de critérios, que são denominados de componentes principais, e são apresentados em um ordem decrescente de importância [89, 90]. PCA foi escolhido frente a outras técnicas pela característica de correlação entre os critérios analisados, isto pode indicar que existe alguma informação redundante [91]. Para aplicar PCA sobre um conjunto de critérios realizam-se os seguintes passos [88]:

1. PCA analisa um conjunto de critérios $\mathcal{S}$, cada critério considera um número de amostras. Onde, o objetivo é reduzir os critérios para obter um conjunto de observações e possa ser descrita com apenas, $\mathcal{L}$ variáveis, $\mathcal{L} < \mathcal{S}$.

2. Calculo da média para os conjuntos dos critérios $\mathcal{S} = \{c_1, c_2, c_3, ..., c_z\}$, denotado pela Equação 2.11, e o cálculo do desvio padrão pela Equacao 2.12.

$$u[m] = \frac{1}{N}\sum_{n=1}^{N} c[m,n] \tag{2.11}$$

$$c_m^2 = \frac{1}{N-1}\sum_{n=1}^{N}(c[m,n] - u[m])^2 \tag{2.12}$$

3. Seguidamente, é calculada a correlação e a preparação da matriz de correlação dos critérios com a Equação 2.13, com ajuda das médias e desvios de padrão encontrados no passo anterior.

$$R_{c_m} = \frac{\frac{1}{N-1}\sum_{n=1}^{N}(c[m,n] - u[m])^2}{c_m} \tag{2.13}$$

4. Estatisticamente, sobre o conjunto de critérios $\mathcal{S} = \{c_1, c_2, c_3, ..., c_z\}$, a análise da componente principal produz um novo conjunto de fatores $\mathcal{Y} = \{y_1, y_2, y_3, ..., y_z\}$, então o conjunto de componentes principais $\mathcal{Y}$ é uma combinação linear do conjunto $\mathcal{S}$, denotada pela Equação 2.14, onde a_z é chamada de carga do critério c_z no fator y_z.

$$y_z = \sum_{z=1}^{n} a_z c_z \tag{2.14}$$

5. Cada elemento do conjunto Y denota o grau de importância dos componentes principais.

2.4.2 Teorema de Bayes

Bayes introduz o conceito de probabilidade condicional em estatística elementar. Observamos que a probabilidade condicional de um evento é uma probabilidade obtida com as informações adicionais de outro evento já ocorrido. Usamos $P(A|B)$ para inferir a probabilidade condicional do evento A, uma vez que o evento B já ocorreu. A Equação 2.15 determina $P(A|B)$ [92]. Neste contexto, ao ser Bayes um método de fusão de dados de inferência probabilística e não um método de estimação, classificação, agregação, entre outras. Utilizamos Bayes para inferir uma probabilidade final de um evento que é afetado por outro evento [93].

$$P(A|B) = \frac{P(B|A)}{P(B)} \tag{2.15}$$

O fator principal para compreender a essência do teorema de Bayes é reconhecer que estamos lidando com eventos sequenciais, em que as informações adicionais são usadas para recalcular a probabilidade do evento inicial [92]. Neste contexto, os termos de probabilidade prévia e probabilidade posterior são comumente usados. A probabilidade prévia é o valor da probabilidade inicialmente obtida nas informações adicionais $P(A_i)$. A probabilidade posterior é o valor da probabilidade que foi calculada com o uso das informações adicionais $P(A_i|B)$ [94, 95]. Portanto, tendo considerando as informações adicionais e os tipos de probabilidades, a probabilidade do evento A dado o evento B, que subsequentemente aconteceu, é determinada pela Equação 2.16.

$$P(A_i|B) = \frac{P(A_i).P(B|A_i)}{\sum_{k=1}^{n} P(A_k).P(B|A_k)} \tag{2.16}$$

Uma análise pelo teorema de Bayes oferece uma maneira de lidar com a informação conceitualmente diferente de todos os outros métodos estatísticos. Bayes fornece um método no qual as observações são usadas para atualizar estimativas dos parâmetros desconhecidos de um modelo estatístico [96]. Bayes determina a probabilidade de um evento considerando valores das probabilidades das informações adicionais. Este teorema vincula o evento que irá acontecer com sua condicional, ou seja, um valor da informação adicional.

2.5 Resumo

Esse capítulo apresentou os conceitos relacionados ao funcionamento da tecnologia de rádio cognitivo, destacando seu uso nas redes ad hoc de rádio cognitivo. Além disso, foram descritas as vulnerabilidades dessas redes, sendo essas vulnerabilidades classificadas de acordo com as camadas da pilha de protocolo. Neste trabalho, focamos nas vulnerabilidades causadas na camada física, como o ataque EUP. Em seguida este foi abordado e descrito. Também foram apresentadas as técnicas de sensoreamento do espectro que têm como finalidade a coleta de informação dos canais de frequência para sua posterior análise. Além disso, descrevemos a técnica de análise de múltiplos critérios juntamente com uma técnica de análise de pesos de importância para cada um dos critérios. Por fim, apresentamos o teorema de Bayes como um método de fusão de informação e análise da probabilidade condicional.

CAPÍTULO 3

TRABALHOS RELACIONADOS

Este capítulo apresenta os principais trabalhos existentes na literatura para a detecção ou mitigação de ataques de emulação de usuários primários nas redes de rádio cognitivo. A Seção 3.1 introduz um breve resumo das soluções existentes, enfatizando os esquemas com abordagem não-cooperativa e os esquemas como abordagem cooperativa para a detecção ou mitigação dos ataques de emulação de usuários primários. A Seção 3.2 mostra uma análise crítica sobre as vantagens e desvantagens das soluções existentes.

3.1 Detecção e mitigação de ataques de emulação de usuário primário

Nesta seção, os esquemas para a detecção e mitigação de ataques de emulação de usuário primário (EUP) nas redes de rádio cognitivo são abordados. Alguns desses esquemas aplicam as técnicas de sensoreamento descritas anteriormente e outros apresentam novos algoritmos. A Tabela 3.1 ilustra um resumo dos esquemas de detecção e mitigação classificados de acordo com a abordagem utilizada: não-cooperativa ou cooperativa.

Tabela 3.1: Esquemas de detecção e mitigação de ataques EUP

Esquema / **Abordagem**	**Detecção**	**Mitigação**
Não-cooperativo	Chen e Park 2006 [28], Chen et al. 2007 [29], Jin et al. 2009 [17], Zhao et al. [97], Li e Han 2010 [30], Chen et al. 2011 [31]	Anand et al. 2008 [22], Jin et al. 2009 [35]
Cooperativo	Jin et al. [98], Huang et al. [99], Min et al. 2011 [34], Chen et al 2011 [33], Leon et al. [27]	Jin et al. 2010 [32], Jin et al. 2010 [26]

Classifica-se as soluções existentes na literatura como esquemas para detecção ou mitigação de ataques EUP. Os primeiros têm como objetivo detectar ataques no espectro e localizar os nós mal intencionados na rede. Os segundos realizam uma tarefa dupla: eles primeiro detectarão um ataque para depois, identificar os nós atacantes e realizar alguma ação na rede a fim de não utilizar essa porção do espectro que está sendo atacada. Todos estes esquemas empregam em seu desenvolvimento técnicas de sensoreamento para coletar dados para suas análises. Nas linhas da Tabela 3.1, apresenta-se as abordagens

não-cooperativas e cooperativas. Uma abordagem não-cooperativa pode ser desenvolvida em qualquer um dos tipos de arquiteturas apresentadas no Capítulo 2, cada nó da rede realiza seu próprio sensoreamento e análise do espectro a fim de tomar uma decisão sobre a presença do ataque EUP na rede. Porém, esta decisão não será influenciada por outras decisões de nós da rede. Em uma abordagem cooperativa, a decisão sobre o espectro é influenciada por outros nós cooperadores. Estes trocam informações e chegam a um consenso. A abordagem cooperativa ao igual que a abordagem não-cooperativa também pode ser implementada em qualquer tipo das arquiteturas apresentadas no Capítulo 2. Em seguida, apresentam-se os esquemas e soluções da literatura, seguindo a perspectiva da abordagem não-cooperativa e cooperativa.

3.1.1 Esquemas com abordagem não-cooperativa

Chen e Park [28] utilizam duas técnicas para a verificação do transmissor a fim de distinguir os sinais primários dos secundários mal intencionados. Uma primeira técnica é chamada de teste da relação da distância (DTR, do inglês, *Distance Ratio Test*). Esta técnica utiliza um par de verificadores que são nós dedicados para a detecção. A localização destes nós é conhecida pelo esquema. O nível da potência recebida é medido para posteriormente verificar a localização do transmissor. A segunda técnica chamada de teste da diferença da distância (DDT, do inglês, *Distance Difference Test*) verifica a diferença das distâncias entre o transmissor primário e os verificadores. Esta diferença é obtida pelo deslocamento de fase do sinal dos verificadores. Contudo, para a verificação do sinal recebido, estas técnicas utilizam uma técnica de sensoreamento baseada na detecção pela energia a fim de coletar os dados. Estes dados são analisados pelas técnicas propostas no esquema.

Chen et al. [29] propõem um esquema de verificação do transmissor chamado de LocDef (do inglês, *Localization-based Defense*). Este esquema utiliza as características do sinal e a localização do transmissor do sinal para verificar os sinais de transmissão dos UPs. O esquema de localização utiliza uma rede de sensores sem fio para coletar as informações dos sinais recebidos. Este esquema apresenta três passos: verificação das características do sinal, medição do nível de energia recebida e localização do transmissor do sinal. Inicialmente, um processo de sensoreamento é realizado, onde se detecta um sinal na banda licenciada. Se a verificação do sinal do UP é negativa, conclui-se como um sinal de US. No entanto, se a verificação é positiva, procede-se ao cálculo da localização do transmissor e compara com a localização conhecida dos transmissores primários. Se a localização não coincide com os transmissores primários conclui-se como um ataque EUP. Por outro lado, se a localização é igual aos transmissores primários, uma comparação do nível de energia é realizada a fim de obter o resultado final sob a presença do ataque EUP.

Jin et al. [17] apresentam um modelo analítico para a detecção de ataques EUPs. Uma

análise da aproximação de Fenton e o WSPRT (do inglês, *Wald's Sequential Probability Ratio Test*) são propostos. Inicialmente, considera-se aproximação de Fenton para detectar a probabilidade de sucesso do ataque EUP. Estes utilizam a desigualdade de Markov para prover um limite inferior na probabilidade de sucesso de ataque EUP. Uma função densidade de probabilidade (PDF) do sinal recebido dos usuários mal intencionados é obtida a partir da aproximação de Fenton. Esta PDF é utilizada por WSPRT para alcançar a detecção do ataque EUP.

Zhao et al. [97] apresentam um esquema de segurança contra ataques EUP. Este esquema é baseado na verificação do *fingerprint* para identificar um ataque EUP. Um *fingerprint* é definido como uma característica do sinal que se transmite no espectro. Neste esquema utiliza-se um *fingerprint* que é determinado pelo ruído do sinal. Este ruído é extraído da potência do sinal recebido para identificar ao transmissor mal intencionado no espectro.

Li e Han [30] propõem um esquema chamado de Dogfight para a detecção de ataques EUPs. Este usa um usuário secundário legítimo para monitorar o espectro em intervalos de tempo. Com isto, este esquema realiza uma detecção proativa do ataque. Um atacante e um defensor competem para o acesso ao espectro, e os autores do trabalho correlacionam essa competição com um jogo de combate aéreo. O esquema é modelado utilizando o princípio da teoria de jogos entre o atacante e o defensor. Um equilíbrio de Nash é determinado entre os dois, proporcionando uma estratégia de operação para os usuários secundários honestos.

Chen et al. [31] apresentam um método para a detecção de ataques EUP em cenários com usuários primários móveis com uma potência de transmissão baixa. Estes dispositivos móveis são representados por microfones que adicionam maiores dificuldades de detecção dos ataques, pois os métodos existentes não são aplicáveis pelo fato de que estes apresentam cenários com usuários primários fixos e com uma maior potência de transmissão. Neste esquema todos os USs legítimos estão equipados com sensores acústicos. As correlações entre o nível de energia do sinal e a informação acústica recebida pelo sensor são exploradas para verificar a autenticidade dos microfones sem fio como usuários primários.

Além das abordagens que tentam detectar ataques EUP, existem também aquelas que objetivam mitigar os efeitos desses ataques. Primeiramente os trabalhos de mitigação em cenários não-cooperativos são expostos. Anand et al..[22] propõem um modelo analítico com base na aproximação de Fenton e na desigualdade de Markov. Eles obtiveram expressões matemáticas a partir de Fenton e Markov para definir limites inferiores sobre a probabilidade de sucesso de um ataque EUP. Para isto, modelaram a potência do sinal recebida de um usuário secundário e utilizaram Fenton para determinar à média e a variância dessa potência recebida. Em seguida, utilizou-se essa média e variância para estabelecer os limites inferiores utilizando a desigualdade de Markov. Com esses limites os autores estabelecem até que ponto pode-se identificar um ataque EUP na rede.

Em Jin et al. [35] a técnica NPCHT (do inglês, *Neyman-Pearson Composite Hypothesis Test*) e a técnica WSPRT (do inglês, *Wald's Sequential Probability Ratio Test*) são propostas para mitigar os ataques EUPs. Estas duas técnicas mitigam o ataque no desvanecimento em ambientes sem fio, sem assumir as características adicionais para os nós secundários ou a presença de nós sensores. No esquema, uma aproximação de Fenton é utilizada para modelar a potência recebida pelo usuário secundário. A NPCHT permite obter uma baixa probabilidade de perda do sinal do usuário primário e minimizar a probabilidade de sucesso do ataque EUP. No entanto, aplicando a WSPRT é possível mitigar o ataque EUP.

3.1.2 Esquemas com abordagem cooperativa

Jin et al. [98] apresentam uma análise para estudar o impacto dos ataques de emulação de usuário primário nos usuários secundários legítimos em termos de perda de acesso ao espectro. Nessa análise, utilizam-se a cadeia de Markov 3D-CTMC (do inglês, *Three Dimensional Continuous Time Markov Chain*) para modelar a ocupação do canal com a presença de atacantes e usuários primários legítimos. Esta análise foi avaliada em cenários com arquiteturas centralizadas e distribuídas com abordagens cooperativas, nas quais os usuários secundários compartilhavam informações a fim de decidir sobre o espectro. Os resultados mostram que os ataques de emulação de usuário primário afetam em até 40% nas oportunidades de acesso ao canal aos usuários secundários legítimos.

Huang et al. [99] expõem as técnicas TDOA (do inglês, *Time Difference Of Arrival*) e FDOA (do inglês, *Frequency Difference Of Arrival*), empregadas para localização do transmissor. Esta localização é utilizada para diferenciar uma transmissão de usuário primário legítimo de um atacante. Esta proposta realiza a combinação das duas técnicas. Em uma primeira etapa, é aplicada a técnica TDOA para a detecção do transmissor malicioso através da potência do sinal recebido. Na segunda etapa, é aplicada a técnica FDOA com os dados calculados pelo TDOA para ter uma melhor identificação do atacante.

Min et al. [34] apresentam um framework cooperativo para a detecção de ataques EUP denominado de IRIS (do inglês, *robust cooperatIve sensing via iteRatIve State estimation*). Este usa a potência de transmissão do usuário primário e seu expoente de perda de propagação para estimar a detecção. Este esquema emprega sensores espalhados na rede para coletar a informação de sensoreamento. Posteriormente, a informação é processada em uma estação base para obter uma decisão final (cooperação centralizada).

Chen et al. [33] propõem um esquema de detecção de ataques EUP que apresenta um modelo de cooperação para maximizar a probabilidade de detecção do usuário primário. Cada usuário secundário recebe sinais do atacante e do usuário primário e envia a informação de detecção a um centro de fusão (estação base). O sinal recebido é combinado com pesos adequados para maximizar a probabilidade de detecção com a restrição da

probabilidade de falso alarme.

Em Leon et al. [27], um esquema centralizado utilizando uma abordagem cooperativa é proposto. Este esquema apresenta uma técnica para determinar a localização do atacante na rede, tendo como conhecimento prévio a localização da estação base primária. A técnica utilizada é a TDOA (do inglês, *Time Difference Of Arrival*). Esta verifica a localização do usuário mal intencionado através da diferença do tempo no sinal recebido em cada um dos receptores (usuários secundários). A técnica apresenta uma abordagem cooperativa pelo fato de que TDOA precisa do tempo de recepção do sinal de outros receptores. Além disso, o gerenciamento deste esquema é centralizado sendo realizado em uma estação base.

Nguyen et al. [100] apresentam um esquema chamado de DECLOAK. Este esquema é passivo, no qual um dispositivo fica na escuta do meio a fim de coletar dados. Estes dados coletados são *fingerprints* dos dispositivos, que não podem ser imitados facilmente. Após esta coleta, o esquema DECLOAK aplica o modelo de mistura infinita de Gauss (IGMM, do inglês, *Infinite Gaussian mixture model*) para a fusão dos *fingerprints* classificados pelo método de Gibbs a fim de determinar a presença do ataque EUP em uma rede com arquitetura distribuída e abordagem cooperativa.

Além das soluções de detecção do ataque, existem aquelas que mitigam os ataques EUPs em cenários cooperativos. Jin et al. [32] apresentam um protocolo de mitigação. Este segue uma arquitetura centralizada e divide o procedimento em duas etapas. Na primeira etapa os nós secundários legítimos monitoram o espectro, recebendo a potência de transmissão do sinal do UP, US e usuário mal intencionado. Estes três sinais são modelados para posteriormente determinar a presença do ataque pela técnica de detecção pela energia. Cada usuário secundário reporta sua decisão de detecção para uma estação base. Nesta estação, acontece a segunda etapa que levará a uma decisão final considerando as informações de detecção de outros USs. Este protocolo tenta reduzir a probabilidade de sucesso do ataque EUP.

Jin et al. [26] propõem um protocolo denominado NEAT (do inglês, *NEighbor AssisTed Spectrum Decision*). NEAT é apresentado com uma arquitetura distribuída para a mitigação de ataques EUPs. Este protocolo é um melhoramento do proposto por os mesmos autores em [32]. Na primeira etapa do esquema, os sinais do UP, US e usuário mal intencionado são modelados em termos de potência de recepção e é aplicado um mecanismo de mitigação preliminar. A segunda etapa do processo mostra o processo de detecção e mitigação cooperativo. A informação coletada é compartilhada entre os nós da rede. Para que um nó determine a presença de um ataque, este solicita informações de detecção a seus nós vizinhos, ou seja, nós a um salto de distância. Com a informação de detecção, ele toma sua decisão final do sucesso do ataque EUP.

3.2 Análise dos trabalhos relacionados

Como mencionado anteriormente, os trabalhos na literatura que apresentam esquemas para a detecção ou mitigação de ataques EUPs nas redes de rádio cognitivo são classificados seguindo abordagens não-cooperativas e cooperativas. Em seguida, realiza-se uma análise das principais vantagens e desvantagens desses esquemas.

- **Vantagens**

  Observa-se que os esquemas propostos na literatura evoluíram no tipo de abordagem empregada para cada esquema. Neste contexto cabe destacar que esquemas com uma arquitetura distribuída apresentam um melhor desempenho na detecção ou mitigação dos ataques EUPs. Além disso, a utilização de abordagens cooperativas na identificação destes ataques representam ganhos de tempo e diminuição de falsos positivos e negativos, e diminuição da perda de detecção do usuário primário legítimo, como são expostos nos seguintes trabalhos: [26, 27, 32, 33, 34, 98, 99, 100].

  Entretanto, não pode-se excluir os trabalhos que apresentam arquiteturas centralizadas ou distribuídas com abordagens não-cooperativas. Pois estes, além de considerar uma abordagem não-cooperativa, apresentam técnicas e métodos para a obtenção de características ou critérios do canal de radiofrequência. Estes critérios podem servir para realizar uma análise a fim de determinar a presença do atacante na rede. Por exemplo, Chen e park [28] e Chen et al. [29] propõem técnicas que permitem identificar a localização do transmissor, através da potência do sinal recebido no dispositivo receptor. Por outro lado, Huang et al. [99] e Leon et al. [27] proporcionam a aplicação de técnicas semelhantes para determinar a localização do atacante em abordagens cooperativas.

  No entanto, trabalhos como Zhao et al. [97] e Nguyen et al. [100] introduzem o termo *fingerprints*. Estes *fingerprints* denotam as características do canal no espectro de radiofrequências. Estes esquemas oferecem técnicas para a coleta dos valores destas características ou critérios do canal. Por outro lado, podemos aferir que um dos critérios mais relevante, amplamente estudado e utilizado entre todos os trabalhos apresentados na literatura é a potência do sinal recebido por um dispositivo. Em seguida, outros critérios considerados nestes esquemas são a localização, a distância, os tipos de modulação, o ruído, entre outras.

- **Desvantagens**

  Os esquemas centralizados ou distribuídos com abordagens não cooperativas apresentam uma alta taxa de falsos positivos e negativos. Estas desvantagens tentam ser supridas pela proposição de esquemas distribuídos cooperativos. Entretanto, apesar das vantagens dos esquemas vistos na literatura, descobrem-se que trabalhos

focando seu escopo em uma análise de múltiplos critérios ou características do canal, são quase inexistentes.

Os trabalhos apresentados neste capítulo baseiam suas análises quase que exclusivamente em um único critério ou característica. Um exemplo é o trabalho de Jin et al. [26], que propõe um esquema distribuído cooperativo tendo como referência a análise de um único critério, a potência do sinal recebido. Nguyen et al. [100] propõem o único esquema que realiza uma análise de múltiplos critérios baseada em características cicloestacionárias. O trabalho de Nguyen et al. pode representar um grande avanço na detecção ou mitigação dos ataques EUP, mas também apresenta grandes desvantagens. Ao considerar características cicloestacionárias, o esquema está obrigado a ter um conhecimento prévio das características do canal, com o objetivo de estabelecer uma autocorrelação das características obtidas e das características previamente conhecidas. Além disso, ao precisar de características cicloestacionárias este esquema necessariamente deverá utilizar uma técnica de sensoreamento cicloestacionária o que significa um maior custo computacional e robustez na implementação.

3.3 Resumo

Esse capítulo apresentou os esquemas e soluções propostos na literatura para a detecção ou mitigação de ataques EUP. Neste contexto, for realizada uma breve contextualização dos esquemas de detecção e mitigação, além das abordagens não-cooperativas e cooperativas. Também foram classificados e descritos os esquemas pelo modo de abordagem. Em seguida, uma análise das vantagens e desvantagens dos esquemas é apresentada.

CAPÍTULO 4

ESQUEMA IMCA

Este capítulo apresenta $IMCA$, um esquema de múltiplos critérios para análise cooperativa da presença de ataques EUP (Emulação de Usuário Primário) em redes ad hoc de rádio cognitivo. O esquema compreende duas fases. A primeira fase tem como base as técnicas de sensoreamento e as técnicas de análise de múltiplos critérios, e a segunda fase utiliza um método de fusão de dados para determinar a presença de ataques EUP. A Seção 4.1 apresenta uma visão geral do esquema $IMCA$. A Seção 4.2 descreve a fase individual do esquema, enquanto a Seção 4.3 detalha a fase cooperativa. Por fim, a Seção 4.4 resume o conteúdo deste capítulo.

4.1 Visão geral do esquema $IMCA$

O esquema para anál**I**se **M**ulticritério e **C**ooperativa da presença de **A**taques EUP ($IMCA$) tem como objetivo determinar a probabilidade da presença de ataques emulação de usuário primário (EUP) em redes ad hoc de rádio cognitivo. O esquema $IMCA$ é composto de duas fases principais: a **individual** e de **cooperação** que executa em cada nó da rede. A Figura 4.1 ilustra as fases do esquema $IMCA$.

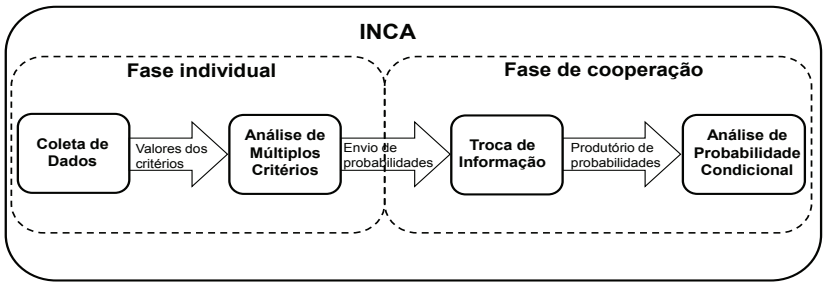


Figura 4.1: Esquema $IMCA$

A fase individual é responsável por calcular de forma probabilística as hipóteses preliminares por cada usuário secundário (US) da rede. Ela é composta pelas operações de, *coleta de dados* e da *análise de múltiplos critérios*. A operação de coleta de dados realiza um sensoreamento do espectro a fim de obter os valores para os critérios utilizados pelo esquema. O sensoreamento do espectro emprega a técnica de detecção pela energia para coletar dados nos diferentes canais de frequências. Em seguida, a operação de análise de múltiplos critérios emprega o método NWAUF e determina a probabilidade preliminar da presença do ataque EUP a partir de valores dos critérios obtidos na coleta de dados.

Após cada US obter sua hipótese preliminar, a fase de cooperação determina a probabilidade final da presença do ataque EUP. Nesta fase, cada nó envia a probabilidade preliminar calculada por ele mesmo para seus nós vizinhos. Sendo denominados de vizinhança, os nós que estão no mesmo canal de frequência e a um salto de distância de um nó. Por sua vez, cada nó vizinho também compartilhará sua respectiva probabilidade preliminar. Após essa troca de informações, cada nó emprega uma análise de fusão de dados utilizando o teorema de Bayes para calcular sua probabilidade final sobre a presença de um ataque EUP.

4.1.1 Modelo do sistema

Nesta subseção descrevemos o modelo de rede e o modelo de ataque considerados neste trabalho. Utiliza-se a notação definida na Tabela 4.1 para explicar os modelos de rede e de ataque.

Tabela 4.1: Notação do esquema IMCA

Notação	**Definição**
N_{UP}	Conjunto de usuários primários
N_S	Conjunto de usuários secundários
N_{SL}	Conjunto de usuários secundários legítimos
N_{SB}	Conjunto de usuários secundários mal intencionados
i-ésimo	índice que representa um usuário secundário arbitrário
j-ésimo	índice que representa um usuário secundário vizinho arbitrário
n_i	Usuário secundário
n_j	Usuário secundário vizinho de n_i
$P_{n_i}(A)$	Probabilidade preliminar calculada pelo nó n_i
$P_{n_j}(B)$	Probabilidade preliminar calculada pelo vizinho n_j
$P_{n_i}(A\|B)$	Probabilidade final calculada pelo nó n_i
$P_{n_j}(B\|A)$	Probabilidade final calculada pelo vizinho n_j
$\mathcal{S}$	Conjunto de critérios
$\mathcal{W}$	Conjunto de pesos de importância para os critérios
$\mathcal{MIN}$ e $\mathcal{MAX}$	Conjunto de valores mínimos e máximos
M	Conjunto de canais de frequências
m	canal de frequência

Modelo de rede - A rede ad hoc de rádio cognitivo é formada por um conjunto de usuários secundários estáticos (nós sem movimentação) representado por N_S. Cada elemento em N_S é representado por n_i, sendo $N_S = N_{SL} \cup N_{SB}$, em que N_{SL} é o subconjunto de USs legítimos e N_{SB} é o subconjunto de US mal intencionados (malicioso e ou egoísta). Cada US arbitrário n_i possui um mecanismo de sensoreamento do espectro. Os nós da rede se comunicam utilizando um canal de frequência, denotado por m e, consequentemente, compõe um conjunto de canais M. Cada n_i desejando transmitir realiza o processo de sensoreamento com o objetivo de verificar quais canais do espectro de frequência estão livres, para então determinar o canal a ser utilizado. A escolha do canal ocorre de três formas: aleatória, sequencial, e considerando a alta oportunidade de transmissão no canal como é definido no modelo de rede CRAHN.

Após o sensoreamento, cada n_i calcula uma probabilidade preliminar da presença do ataque EUP, denotada por $P_{n_i}(A)$. Posteriormente, cada n_i calcula a probabilidade final da presença do ataque EUP, denotada por $P_{n_i}(A|B)$, considerando as probabilidades preliminares vizinhas $P_{n_j}(B)$, onde n_j representa um nó vizinho do nó n_i. Por outro lado, assumimos que a rede ad hoc de rádio cognitivo opera paralelamente a uma rede primária formada pelo conjunto de usuários primários denotado por N_{UP}. Cada usuário primário $UP \in N_{UP}$ realiza suas transmissões em sua respectiva banda licenciada. Estas comunicações primárias iniciam no transmissor primário e finalizam no receptor primário.

Modelo do ataque - Os nós pertencentes ao conjunto de usuários mal intencionados $N_{SB} \in N_S$, denominados atacantes, emulam as características de um usuário primário ao adaptar e modificar os parâmetros de seu dispositivo de rádio. Por exemplo, alterando a potência de transmissão, o tipo de modulação, a largura de banda, a taxa de transmissão, entre outros). Esta emulação permite aos usuários secundários mal intencionados aproveitarem os espaços vazios do espectro e deixarem os usuários secundários legítimos $N_{SL} \in N_S$ sem oportunidades de acesso. Os atacantes agem considerando as características dos usuários primários em termos de prioridade de acesso aos canais do espectro. Assume-se que um atacante, assim como um usuário secundário legítimo, está equipado com um mecanismo de sensoreamento do espectro que permite a detecção da presença de um usuário primário. Este equipamento possibilita ao atacante o acesso a um canal a ser atacado. Assim, o atacante emulará as características de um usuário primário legítimo nesse canal a fim de se aproveitar do uso prioritário do espectro, com o objetivo de que um US legítimo detecte a presença de um UP legítimo, e deixe outros USs legítimos sem oportunidades de acesso ao espectro.

A Figura 4.2 ilustra o funcionamento de uma rede ad hoc de rádio cognitivo (CRAHNs, do inglês, *Cognitive Radio Ad Hoc Networks*) sob ação dos atacantes. Nesta rede, observa-se diferentes nós legítimos, representados por círculos brancos, e nós mal intencionados representados por círculos cinza. Todos os nós possuem uma lista de canais disponíveis. Cada nó mal intencionado apresenta as mesmas características que um US legítimo. Por outro lado, um usuário mal intencionado (ex. n_{10}) pode comprometer a comunicação entre dois nós legítimos transmitindo (ex. n_7 e n_9) por ter o mesmo canal de frequência para transmitir (ex. canal 4).

4.2 Fase individual

A fase individual determina de forma probabilística a hipótese preliminar da presença de ataques EUP na rede e é composta de duas operações: a *coleta de dados* e a *análise de múltiplos critérios*. Na primeira operação, o $IMCA$ realiza um sensoreamento do espectro, monitorando cada um dos M canais que compõem a rede primária. Neste sensoreamento,

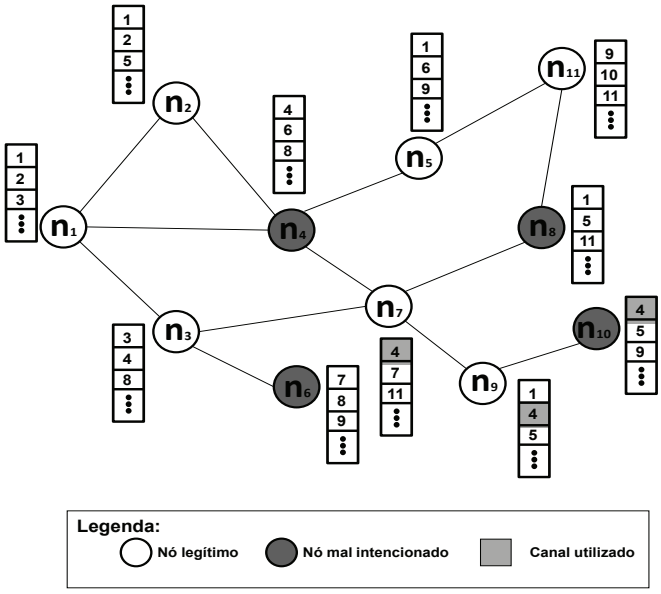


Figura 4.2: Modelo de rede com usuários secundários legítimos e mal intencionados

os valores são obtidos utilizando a técnica de detecção pela energia, descrita no Capítulo 2, devido a sua simplicidade de implementação e por dispensar um conhecimento prévio do sinal, como provado em [41, 101]. Estes valores representam os dados para cada critério estabelecido pelo $IMCA$. Estes critérios definem as características do sinal em uma transmissão nos canais de frequências. A Figura 4.3 ilustra o sensoreamento do espectro para a coleta de dados na fase individual do esquema $IMCA$. Observamos o nó n_{11} monitorando o canal M_3 do espectro de radiofrequências; da mesma forma, os nós n_9 e n_{10} monitoram o canal M_1 onde poderá estabelecer uma comunicação entre estes dois usuários secundários. Em seguida, cada nó secundário n_i obtém os valores de cada um dos critérios. Após a coleta, estes dados são agrupados em um conjunto de amostras $\mathcal{S}$ para cada critério c.

Em seguida, os conjuntos $\mathcal{W}$, $\mathcal{MIN}$ e $\mathcal{MAX}$ são definidos para o cálculo da probabilidade preliminar da presença do ataque EUP, denotada por $P_{n_i}(A)$. Os conjuntos $\mathcal{MIN}$ e $\mathcal{MAX}$ são compostos pelos valores mínimos e máximos para cada um dos critérios. O conjunto $\mathcal{W}$ é determinado pelos pesos de importância para cada critério. O cálculo da probabilidade preliminar é realizado pelo método de análise de múltiplos critérios NWAUF (do inglês, *Normalized Weighted Additive Utility Function*) [82]. Estudos mostram o baixo custo computacional deste método em comparação a outros para análise de múltiplos critérios, como o AHP (*Analytic Hierarchy Process*) [83] ou ELECTRE [84], e as suas respectivas variantes [82, 85]. Os passos gerais do método NWAUF são apresentados no Algoritmo 1. Os conjuntos $\mathcal{S}$, $\mathcal{W}$, $\mathcal{MIN}$ e $\mathcal{MAX}$ são usados pelo algoritmo NWAUF. Este método utiliza os conjuntos $\mathcal{MIN}$ e $\mathcal{MAX}$ para normalizar os valores em $\mathcal{S}$ e gerar o conjunto normalizado correspondente, $\overline{\mathcal{S}} = \{\overline{s} \mid 0 \leq \overline{s} \leq 1\}$ (linhas 5–6). Finalmente,

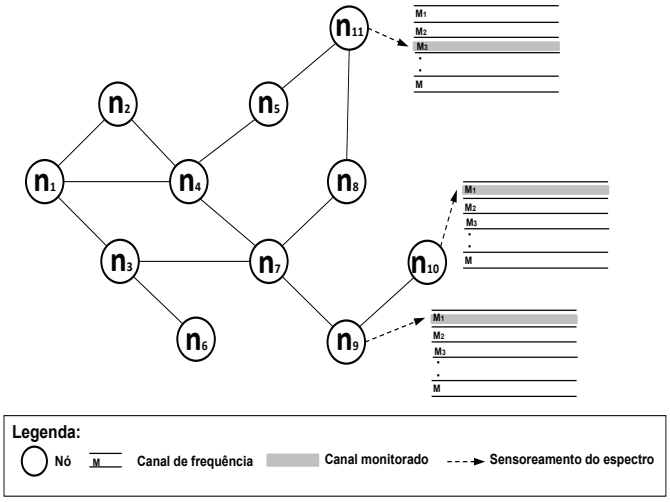


Figura 4.3: Coleta de dados na fase individual do esquema $IMCA$

o método utiliza o conjunto de pesos $\mathcal{W} = \{w_1, w_2, \ldots, w_c \mid \sum_{z=1}^{c} w_z = 1\}$, onde cada peso de importância é atribuído a um critério em $\overline{\mathcal{S}}$ para calcular $P_{n_i}(A)$ (linha 7). Os valores em $\mathcal{W}$ são valores estáticos, e baseados na relevância de estudo de cada critério para determinar a probabilidade preliminar da presença do ataque EUP. Estes métodos podem ser definidos por alguma das técnicas apresentadas em Raj [88].

Algoritmo 1 Análise NWAUF

1: **procedimento** NWAUFAnalysis($\mathcal{S}, \mathcal{W}, \mathcal{MIN}, \mathcal{MAX}$)
2: $P_{n_i}(A) \leftarrow 0$;
3: $\overline{\mathcal{S}} \leftarrow \emptyset$;
4: **para todos** $z = 1 \rightarrow |c|$ **faça**
5: $\overline{s_z} \leftarrow \dfrac{\mathcal{S}_z - \mathcal{MIN}_z}{\mathcal{MAX}_z - \mathcal{MIN}_z}$;
6: $\overline{\mathcal{S}} \leftarrow \overline{\mathcal{S}} \cup \{\overline{s}\}$;
7: $P_{n_i}(A) \leftarrow P_{n_i}(A) + W_z \cdot \overline{s}_z$;
8: **fim para**
9: **fim procedimento**

Cada nó aplica o método NWAUF para calcular uma probabilidade preliminar da presença do ataque EUP através da agregação de dados de múltiplos critérios. Tal resultado é então utilizado para calcular a probabilidade final da presença do ataque EUP na fase de cooperação do IMCA. A Figura 4.4 destaca cada passo da análise NWAUF de múltiplos critérios.

4.3 Fase de cooperação

Na fase de cooperação, o i-ésimo US não só realiza o compartilhamento de $P_{n_i}(A)$, mas também recebe as probabilidades preliminares dos nós vizinhos. A troca de probabilidades preliminares é realizada estabelecendo um canal de comunicação comum entre n_i

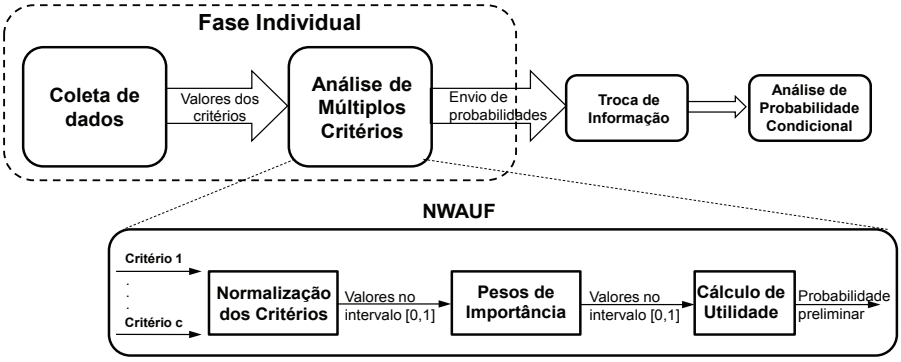


Figura 4.4: Fase de sensoreamento e análise do esquema $IMCA$

e cada um de seus vizinhos n_j. A probabilidade preliminar é enviada a seus vizinhos dentro de um pacote de controle. Desta mesma forma, os vizinhos respondem com outro pacote de controle contendo suas probabilidades preliminares de detecção. A Figura 4.5 ilustra a troca de pacotes entre o nó n_i e seus vizinhos correspondentes $n_j, j = 1, \ldots, k$. Observamos que um nó (ex. n_1) envia sua probabilidade preliminar em um pacote de controle a seus vizinhos (ex. n_2, n_3, n_4) e estes respondem com outro pacote de controle que contém suas respectivas probabilidades preliminares.

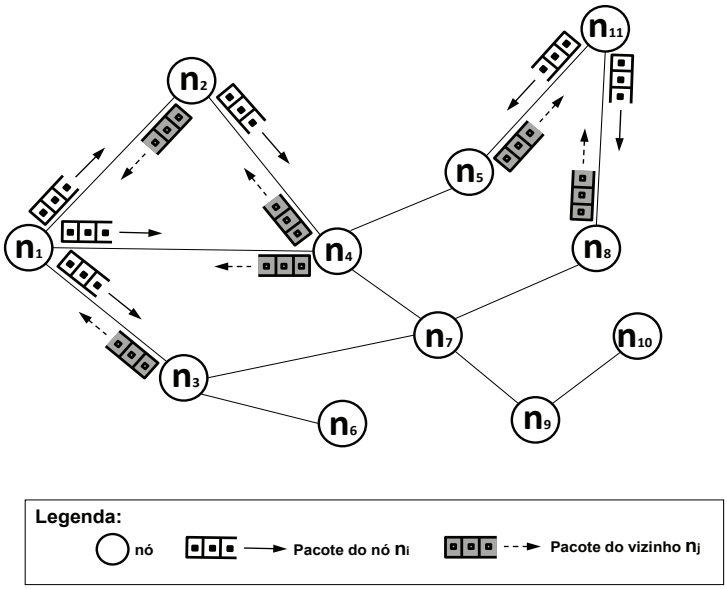


Figura 4.5: Troca de probabilidades preliminares

Depois de receber $k \leq |N_{SL}| - |\{n_i\}|$ probabilidades preliminares de sua vizinhança, o nó $n_i \in N_{SL}$ calcula sua probabilidade final $P_{n_i}(A|B)$ referente à presença de um ataque EUP na rede por meio do teorema de Bayes (Equação 4.1). Este teorema permite calcular a probabilidade condicional $P_{n_i}(A|B)$ de acontecer um dado evento A, mediante a ocorrência de um evento B. Para isso, o teorema considera uma probabilidade preliminar $P_{n_i}(A)$ de acontecer um evento A sem a influência do evento B. Além disso, ele

também considera a probabilidade preliminar $P_{n_j}(B)$ de acontecer o evento B bem como a probabilidade inversa de $P_{n_i}(A|B)$, isto é, $P_{n_j}(B|A)$.

Seguindo o teorema, um nó n_i calcula a probabilidade final da presença de ataque a partir das probabilidades preliminares $P_{n_i}(A)$, $P_{n_j}(B)$ e $P_{n_j}(B|A)$. Em particular, **o evento A denota o acontecimento de um ataque EUP na perspectiva do nó** n_i. A probabilidade $P_{n_i}(A)$ do evento A acontecer é inicialmente estimada por n_i a partir do método NWAUF, como explicado na fase individual do esquema IMCA. Do mesmo modo, cada vizinho do nó n_i calcula sua respectiva probabilidade preliminar sobre um ataque EUP na rede. Da perspectiva do nó n_i, **o evento B denota a detecção da presença de um ataque EUP por cada vizinho** $n_j, j = 1, \ldots, k$, em que k é o total de vizinhos do nó n_i. Cada vizinho n_j calcula sua própria probabilidade preliminar sobre um ataque EUP na rede. Da perspectiva do nó n_i, tal probabilidade é denotada por $P_{n_j}(B)$. O teorema de Bayes requer que cada probabilidade do tipo $P_{n_j}(B|A)$ seja inicialmente estimada a fim de calcular $P_{n_i}(A|B)$. Em particular, para nosso esquema este valor foi estimado considerando rigorosas simulações. Contudo, este valor é regulado pela influência das probabilidades calculadas a partir das medições que cada nó realiza. A Figura 4.6 destaca os passos para que cada US determine a probabilidade da presença do ataque EUP através da probabilidade condicional definida pelo teorema de Bayes.

$$P_{n_i}(A|B) = \frac{P_{n_i}(A).P_{n_1}(B|A)}{[\sum_{j=1}^{k} P_{n_j}(B).P_{n_j}(B|A)]} \tag{4.1}$$

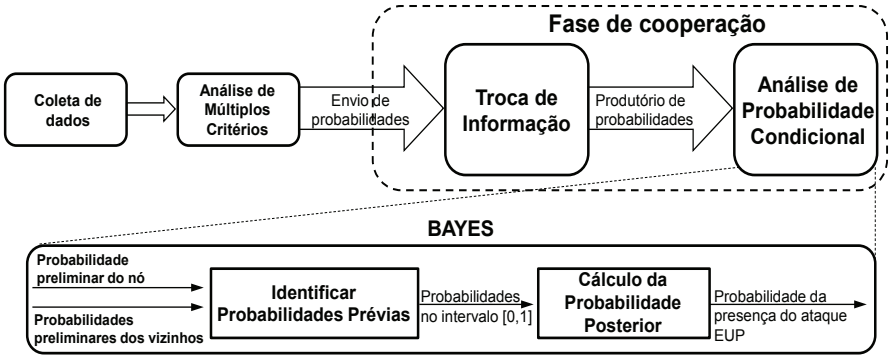


Figura 4.6: Fase de cooperação do esquema $IMCA$

4.4 Resumo

Esse capítulo apresentou o esquema para análise multicritério e cooperativa da presença de ataques EUP em redes ad hoc de rádio cognitivo, denominado $IMCA$. Inicialmente, uma visão geral do esquema $IMCA$ é apresentada, seguida dos modelos de rede e de ataque.

As duas fases do esquema $IMCA$ são descritas. Na fase *individual* destaca-se a utilização do método NWAUF para a análise de múltiplos critérios e obtenção da probabilidade preliminar da presença do ataque EUP. Na fase de *cooperação*, descreve-se como é obtida a probabilidade final da presença do ataque EUP aplicando o teorema de Bayes.

CAPÍTULO 5

AVALIAÇÃO

Este capítulo apresenta uma avaliação do esquema $IMCA$ (*esquema para análise* **M***ulticritério e* **C***ooperativa da presença de* **A***taques EUP*) em termos de desempenho e eficiência na obtenção da probabilidade da presença dos ataques. A Seção 5.1 descreve os cenários e os parâmetros de simulação utilizados. A Seção 5.2 apresenta as métricas empregadas para a medição do desempenho e da eficiência do $IMCA$. Na Seção 5.3 descreve-se e analisa-se os resultados obtidos. Por fim, a Seção 5.4 resume o conteúdo deste capítulo.

5.1 Cenários de simulação

O simulador de redes NS, versão 2.31, foi utilizado na avaliação do desempenho e da eficiência do $IMCA$. O esquema foi implementado e integrado ao código do módulo CRAHN, desenvolvido por pesquisadores da Universidade de Northeastern, EUA [36]. O esquema $IMCA$ foi avaliado considerando a interferência de nós mal intencionados na rede, sendo que tais nós agem na forma de ataques de emulação de usuário primário (EUP). Estes ataques imitam as características do usuário primário (UP) nos canais de transmissão, emulando assim um usuário primário legítimo. Como mencionado, um ataque EUP reduz a oportunidade de acesso ao espectro os usuários secundários legítimos.

Os cenários de rede simulados são compostos por $|N_S| = 50$ ou $|N_S| =$100 nós estáticos, sendo que a quantidade de $|N_{SL}|$ (USs legítimos) e $|N_{SB}|$ (USs mal intencionados) variam para refletir diferentes taxas de atacantes na rede. Os usuários secundários da CRAHN podem se comunicam utilizando $|M| = 11$ canais utilizando o intervalo de radiofrequências de 2.412 até 2.462 GHz. Apesar desse intervalo de radiofrequências ser considerado livre, o módulo CRAHN emprega este intervalo e força os usuários primários a compartilharem esta faixa de frequência com os usuários secundários. Por tratar-se de um modelo, este aspecto não compromete a generalidade dos resultados alcançados neste trabalho.

Em particular, nós assumimos o modelo de propagação *Free-Space* para o sinal primário detectado por um nó n_i, se $UP \in N_{UP}$, e um modelo de propagação *two ray ground* para o sinal detectado por um nó n_i a partir de um US mal intencionado ou um US legítimo [22, 26]. O conjunto de usuários secundários N_S estão dispostos em uma área de 1000m x 1000m seguindo uma variação do modelo *Random Waypoint*, em que força-se a ausência de movimentação dos nós. O protocolo de roteamento empregado é o *Ad hoc On demand Distance Vector Routing (AODV)*, o raio de alcance dos nós é de 250m como estabelecido no padrão IEEE 802.11.

Cada nó $n_i \in N_S$ implementa as duas fases do esquema $IMCA$. A fase individual realiza uma coleta de dados para os c critérios estabelecidos. Em particular, foram definidos dois casos de simulação: **caso 1** e **caso 2**, os quais empregam quantidades e tipos diferentes de critérios. No caso 1, são considerados três critérios, sendo estes: **a potência de recepção, a potência de transmissão** e **a distância**. No caso 2, consideram-se quatro critérios, sendo estes: **a potência de recepção, o SNR (do inglês, *Signal to noise ratio*), o ruído (do inglês, *noise*)** e **a taxa de transmissão**. O esquema $IMCA$ usa múltiplos critérios que foram amplamente estudados e avaliados na literatura para a detecção ou mitigação de ataques EUP. Estes critérios são agregados utilizando uma técnica de fusão de dados para determinar a presença dos ataques EUP.

Além da coleta de dados, o esquema $IMCA$ realiza primeiramente uma análise de múltiplos critérios. Nesta análise, o esquema utiliza o método NWAUF com base no conjunto de amostras coletadas $\mathcal{S}$ para cada um dos c critérios estabelecidos. Inicialmente, utilizamos os conjuntos de mínimos $\mathcal{MIN}$ e máximos $\mathcal{MAX}$ para normalizar os valores do conjunto $\mathcal{S}$. Estes conjuntos mínimos e máximos são constituídos pelos valores mínimos e máximos para cada critério obtidos a partir das amostras. Em seguida, NWAUF utiliza um conjunto $\mathcal{W}$ de pesos de importância para cada critério. Estes pesos são obtidos aplicando a técnica de **análise de componente principal** (PCA, do inglês, *Principal Component Analysis*).

- **Avaliação de pesos de importância**

  O PCA considera um conjunto de amostras para cada critério como entrada na definição dos pesos de importância. Este conjunto de amostras é obtido a partir de simulações e de medições em cenários reais. As amostras obtidas nas simulações foram utilizadas no caso 1. Estas amostras foram coletadas a partir de simulações realizadas no NS-2. As amostras de cenários reais tiveram como referência os dados disponibilizados no CRAWDAD (*Community Resource for Archiving Wireless Data At Dartmouth*) [102], extraídos de dois diferentes cenários de experimentação de redes em malha sem fio (802.11g e 802.11a). Apesar destas experimentações serem em ambientes de redes em malha sem fio, o comportamento dos dados não se diferenciam dos dados correspondentes em uma rede ad hoc de rádio cognitivo, pois o comportamento dos critérios utilizados independe do tipo de rede sem fio. O cenário que aplica a tecnologia 802.11g utiliza 10 nós com uma potência de transmissão de 15 dBm e uma taxa de transmissão de 11 Mbps. Os dados foram coletados em situações que estabeleceram 54 enlaces com 3 canais ortogonais entre os nós. O cenário que aplica a tecnologia 802.11a é composto de 13 nós com uma potência de transmissão de 15 dBm e uma taxa de transmissão de 6 Mbps em 78 diferentes enlaces com 13 canais ortogonais. As especificações destes cenários e da coleta de amostras são detalhadas em Subramanian et al. [103] e são consideradas para

avaliar e definir os pesos de importância no caso 2.

Inicialmente, as amostras são normalizadas para depois representar o conjunto de principais fatores e posteriormente obter uma matriz de correlação dos critérios para estabelecer os pesos de importância. Cabe destacar que a descrição da técnica PCA é relatada no Capítulo 2. Após a análise PCA utilizando a ferramenta *R* [104] para calcular os pesos com base nas amostras, foram obtidos os seguintes valores para os pesos de importância de cada critério. No **caso 1** foram estabelecidas as percentagens de pesos de 45%, 29% e 26% para os critérios de potência de recepção, potência de transmissão e distância, respectivamente. No **caso 2**, foram estabelecidas as percentagens de pesos de 45%, 25%, 18% e 12% para os critérios de potência de recepção, a relação sinal-ruído, o ruído e taxa de transmissão, respectivamente. Um resumo dos valores dos pesos de importância obtidos para cada critério são mostrados na Tabela 5.1. Para mostrar a importância de uma análise idônea dos pesos, os primeiros resultados apresentados na Seção 5.3 sobre a avaliação do esquema $IMCA$ não aplicam uma análise de pesos de importância. Os demais resultados foram alcançados aplicando a técnica PCA para a definição dos pesos de importância.

Tabela 5.1: Percentagens de pesos de importância

Caso de estudo / **Critérios**	**Caso 1 (%)**	**Caso 2 (%)**
Potência de recepção	45	45
Potência de transmissão	29	
Distância	26	
SNR (relação sinal-ruído)		25
Ruído		18
Taxa de Transmissão		12
Total	100	100

A fase de cooperação do esquema $IMCA$ inicia com uma troca de probabilidades preliminares entre o USs e seus vizinhos. Após esta troca, o esquema realiza uma fusão das probabilidades preliminares utilizando o teorema de Bayes a fim de determinar a probabilidade final da presença de ataques EUP. Para o cálculo da probabilidade final, $P_{n_i}(A|B)$, em um dado nó n_i, o teorema de Bayes precisa da probabilidade final de um vizinho n_j, denotada por $P_{n_j}(B|A)$. Como em uma primeira iteração esta probabilidade do vizinho é desconhecida, ela precisa ser estimada ou adivinhada. Desta forma, a probabilidade estimada para $P_{n_j}(B|A)$, na primeira iteração, foi definida como 0.5, que representa um probabilidade inicial neutra. Este valor é definido a traves de rigorosas simulações do esquema $INCA$, nas simulações observo-se que um valor inicial para Bayes igual ou perto de 1.0 denotava uma alta taxa de falsos positivos, caso contrario acontecia quando o va-

lor inicial ficava perto ou igual a 0.0, uma alta taxa de falsos negativos era gerada. Em particular, verifico-se que um valor neutro inicial ótimo para o teorema de Bayes é 0.5.

Nas simulações, são consideradas as seguintes porcentagens de nós mal intencionados: 10%, 30% e 50% do total do USs na rede. Estes nós agem de forma mal intencionada durante períodos aleatórios na simulação. Além disso, cabe destacar que os nós mal intencionados possuem mecanismos cognitivos para detectar a presença de um usuário primário a fim de não causar colisões ou interferências nas transmissões primárias. Os resultados apresentados são as médias de 35 simulações para cada porcentagem de atacantes nos diferentes cenários, considerando os dois casos do esquema $IMCA$. Além disso, os resultados são mostrados com um intervalo de confiança de 90%. A Tabela 5.2 resume os principais parâmetros e seus valores utilizados nas simulações.

Tabela 5.2: Principais parâmetros de simulação

Parâmetros	**Valor**
Quantidade de nós - usuários secundários (USs)	50, 100
Quantidade de usuários primários (UPs)	2
Porcentagem de nós mal intencionados (EUPs)	10, 30, 50 (%)
Tempo de vida da rede	500 segundos
Área de movimentação	1000x1000 metros
Raio de transmissão dos USs	250 metros
Raio de transmissão dos UPs	1000 metros
Raio de transmissão dos EUPs	250 até 1000 metros
Potência de transmissão USs	24,5 dBm (0.2818 w)
Potência de transmissão UPs	94 dBm (2511886,43 w)
Potência de transmissão EUPs	24,5 até 94 dBm
Protocolo de roteamento	AODV

5.2 Métricas

Foram empregadas cinco métricas para avaliação do esquema $IMCA$. A primeira métrica aborda a probabilidade do sucesso do atacante na CRAHN. As outras quatro métricas consolidam os resultados obtidos com a primeira, além de aferir a eficiência do esquema $IMCA$ frente à detecção da presença de ataques EUPs. A seguir, definimos cada uma das métricas utilizadas.

1. A primeira métrica mede o sucesso do ataque na CRAHN e é denominada de *probabilidade da presença do ataque EUP (Pr)*. Ela quantifica as probabilidades finais dos nós que detectam um possível ataque na rede. A métrica Pr é definida conforme a Equação 5.1 em que $P_{n_i}(A|B)$ representa a probabilidade de sucesso do ataque determinada por um nó n_i, e R a quantidade total de detecções dos atacantes realizada pelo esquema $IMCA$.

$$Pr = \frac{\sum_{i=1}^{|N_S|} P_{n_i}(A|B)}{|R|} \tag{5.1}$$

2. A segunda métrica apresenta uma variação da primeira e é chamada de *Taxa de detecção (T_k)*. Ela representa o impacto das probabilidades vizinhas na probabilidade individual de um nó n_i. Para isto, foi forçada uma variação do valor k, que representa a quantidade de vizinhos cooperadores, em 3, 6 e 10 para poder realizar o cálculo final da probabilidade da presença dos ataques EUP. T_k é calculada de acordo com a Equação 5.2, em que $P_{n_j}(B), j = 1, 2, 3, .., k$ representa a probabilidade preliminar compartilhada pelo j-ésimo vizinho de n_i e k representa quantidade total de vizinhos cooperadores.

$$T_k = \frac{\sum_{j=1}^{k} P_{n_j}(B)}{|k|} \tag{5.2}$$

3. A terceira métrica mede a probabilidade de perda de detecção de um usuário primário por parte de um nó n_i, visto que o esquema $IMCA$ considera a presença de usuários primários legítimos. Esta métrica é chamada de *probabilidade de perda do UP (Pr_{pup})* e significa a probabilidade de um nó n_i não detectar a presença de um usuário primário legítimo no canal monitorado. Esta métrica é calculada pela Equação 5.3, em que pup_{n_i} representa a probabilidade de perda de um nó n_i e Q é a quantidade total de perdas do usuário primário.

$$Pr_{pup} = \frac{\sum_{i=1}^{|N_S|} pup_{n_i}}{|Q|} \tag{5.3}$$

4. A quarta métrica quantifica a taxa de falsos positivos na probabilidade de sucesso do ataque. A *taxa de falsos positivos (Tx_{fp})* determina a razão da quantidade de vezes em que os nós identificaram um ataque sendo este negativo. Essa métrica é calculada pela Equação 5.4, em que B significa o número total de detecções no esquema, na forma de $B = (d, v)$, onde d representa a probabilidade da detecção realizada pelo esquema $IMCA$ e v é a condição real do nó $n_i \in N_S$, onde $v = 1$ representa um nó mal intencionado e $v = 0$ um nó legítimo.

$$Tx_{fp} = \frac{\sum Dp_i}{|B|} \forall i \in B \qquad onde \qquad Dp_i = \begin{cases} 1 \; se \; d_i = 1 \\ 0 \; se \; d_i \neq 0 \end{cases} \tag{5.4}$$

5. A quinta métrica aferida é a *taxa de falsos negativos (Tx_{fn})* que quantifica as vezes que os nós não detectam a presença de ataques EUPs enquanto eles ocorrem de fato. Tx_{fn} é calculada de acordo com a Equação 5.5, em que B representa o número total de detecções no esquema, na forma de $B = (d, v)$, onde d representa a probabilidade da detecção realizada pelo esquema $IMCA$ e v é a condição real do nó $n_i \in N_S$, onde $v = 1$ representa um nó mal intencionado e $v = 0$ representa um nó legítimo.

$$Tx_{fp} = \frac{\sum Dn_i}{|B|} \forall i \in B \qquad onde \qquad Dn_i = \begin{cases} 0 \; se \; d_i = 1 \\ 1 \; se \; d_i \neq 0 \end{cases} \tag{5.5}$$

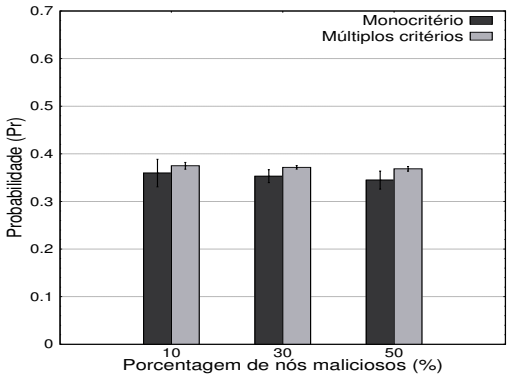
5.3 Avaliação do desempenho do esquema $IMCA$

Nesta seção, apresenta-se uma avaliação do esquema $IMCA$ nas CRAHNs sob ataques EUPs. As métricas são aplicadas a cada cenário simulado, e os resultados obtidos pelo esquema $IMCA$ são comparados aos resultados de um esquema monocritério. Cabe destacar que o esquema monocritério utiliza apenas o critério da potência de recepção do sinal, que é um critério amplamente estudado e avaliado na detecção ou mitigação de ataques EUP em esquemas e análises apresentados na literatura. O esquema monocritério apresenta duas fases, na fase individual, ele calcula a probabilidade preliminar da presença do ataque com base na potência de recepção. Já na fase cooperativa, os nós trocam informações de detecção do ataque EUP. Em seguida, cada nó realiza um cálculo da probabilidade final do sucesso do ataque, com base nas informações trocadas. O esquema monocritério segue os conceitos e as especificações dos esquemas apresentados na literatura e descritos no Capítulo 3.

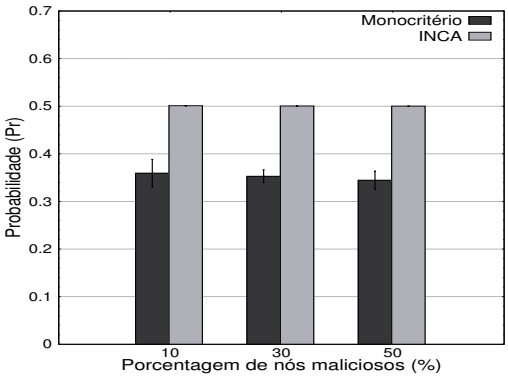
Nas Figuras 5.1(a), 5.1(b) e 5.1(c), são mostrados os resultados do esquema $IMCA$ na detecção de ataques. Para a obtenção desses resultados nenhuma análise foi feita a fim de definir os pesos de importância dos critérios. A Figura 5.1(a), apresenta os resultados do esquema $IMCA$ frente ao esquema monocritério em sua fase individual. Na Figura 5.1(b), mostramos a avaliação do esquema $IMCA$ considerando suas duas fases. Na Figura 5.1(c), apresentamos a taxa de detecção por vizinhos cooperadores. Em todos estes resultados notamos uma pouca variação na probabilidade da presença do ataque EUP, isto pode ter ocorrido pela ausência da análise dos pesos de importância.

A seguir, mostramos os resultados com uma avaliação de pesos de importância determinados pela técnica PCA. Ressaltamos que para o caso 1, os dados utilizados para avaliar os pesos de importância são provenientes de simulações, e no caso 2 os dados são provenientes de experimentações. As Figuras 5.2(a) e 5.2(b) apresentam os resultados referentes à métrica probabilidade da presença do ataque EUP (Pr) obtidos considerando apenas a primeira fase do esquema $IMCA$ na presença de nós mal intencionados. As figuras mostram os resultados para os esquemas monocritério e múltiplos critérios, sendo que os resultados obtidos através do esquema de múltiplos critérios são rotulados como caso 1 e caso 2, tal como definimos anteriormente.

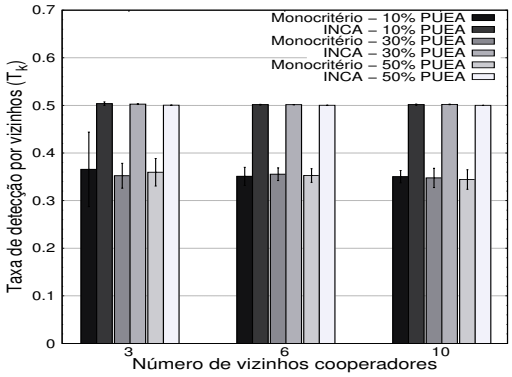
Na Figura 5.2(a), os resultados mostram uma probabilidade preliminar da presença do ataque EUP superior em todos os cenários com relação à probabilidade preliminar obtido pela análise monocritério. O caso 1 apresenta um ganho de 16%, 19% e 18% em relação ao esquema monocritério nas três variações de porcentagens de atacantes na CRAHN,



(a) Fase individual



(b) IMCA vs Monocritério



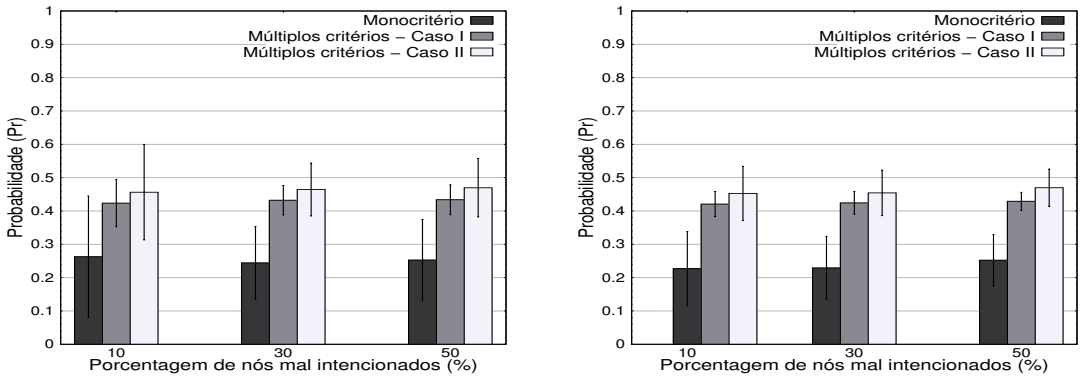
(c) Análise da cooperação

Figura 5.1: Esquema $IMCA$ **sem a análise de pesos de importância**

sendo a rede constituída por um total de 50 nós. Por outro lado, o caso 2 do esquema $IMCA$ mostra um ganho de 19%, 22% e 25% em relação ao esquema monocritério. As variações das probabilidades entre os dois casos do esquema $IMCA$ representa um ganho do caso 2 de 3% em relação ao caso 1, isto determina que a escolha do tipo de critérios junto à quantidade de critérios pode representar um ganho significativo na fase individual sem a execução da fase de cooperação.

A Figura 5.2(b), apresenta os resultados em uma ambiente com 100 nós dispostos na CRAHN. O caso 1 obteve um ganho de até 20% diante de diferentes variações de percentagem de atacantes na rede e em relação com o esquema monocritério. O caso 2 do $IMCA$ obtém um ganho de até um 23% frente ao esquema monocritério. A variação entre os dois tipos do esquema $IMCA$ é de até 4%. Estes resultados refletem a estabilidade na determinação do ataque EUP da fase individual do esquema $IMCA$ e definem que a análise de múltiplos critérios determina uma elevada probabilidade preliminar da presença do ataque EUP independente da importância da quantidade de nós dispostos na rede.

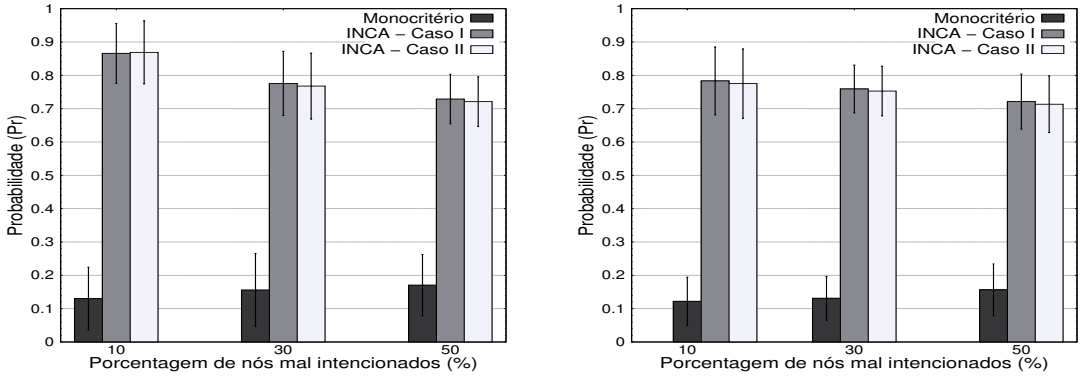
Na Figura 5.3(a), compara-se os resultados dos esquemas $IMCA$ em seus dois casos de estudo frente ao esquema monocritério cooperativo em um cenário com 50 nós na rede. O caso 1 do esquema $IMCA$ tem um ganho de até 77% em relação ao esquema monocritério. O caso 2 obtém um ganho de até um 73% em relação ao esquema monocritério.



(a) Cenário com 50 nós (b) Cenário com 100 nós

Figura 5.2: Pr preliminar das análises de múltiplos critérios e monocritério

Observamos que o esquema monocritério cooperativo apresenta uma diminuição de sua probabilidade de detecção frente ao esquema monocritério individual. Isto se deve ao fato da junção de informação em um nó representar a média de todas as probabilidades, além de contar apenas com uma análise de um único critério para determinar a presença do ataque EUP. Por outro lado, os dois casos do esquema $IMCA$ apresentam uma variação de 1% entre eles, com isto aferimos que uma análise de múltiplos critérios junto com uma abordagem cooperativa com análise de fusão da informação utilizando o teorema de Bayes oferece uma alta probabilidade (Pr) de determinação da presença do ataque EUP nas CRAHNs.



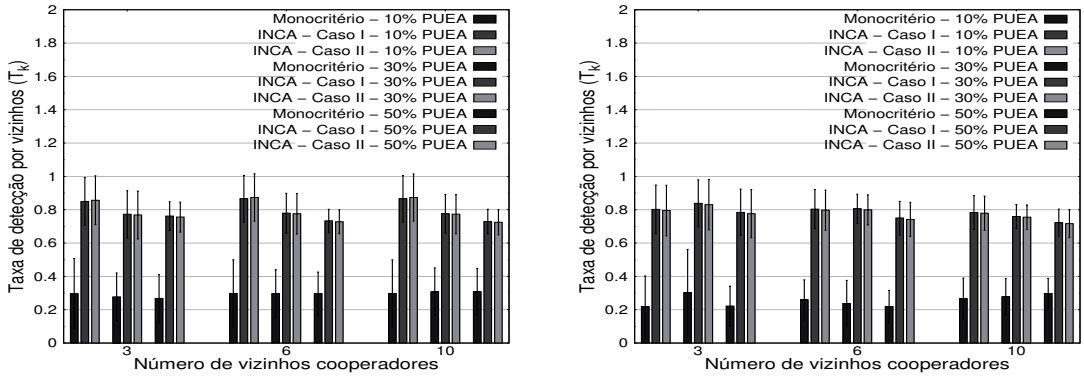
(a) Cenário com 50 nós (b) Cenário com 100 nós

Figura 5.3: Pr do esquema IMCA vs esquema monocritério

A Figura 5.3(b) retrata os resultados obtidos entre os dois casos do esquema $IMCA$ e o esquema monocritério cooperativo em um cenário com 100 nós. Observa-se que os resultados mostram um mesmo comportamento em relação aos resultados apresentados na Figura 5.3(a). No cenário com 100 nós, o caso 1 do esquema $IMCA$ tem um ganho de até um 66% ao comparar com o esquema monocritério. O caso 2 resulta em um ganho de 65% em relação ao esquema monocritério, e a variação entre os dois casos do esquema $IMCA$ é de 1%. Estes resultados demonstram que uma análise de múltiplos critérios em

um abordagem cooperativa oferece uma alta probabilidade da detecção da presença do ataque EUP (Pr).

A Figura 5.4(a) apresenta a taxa de detecção por vizinhos T_k obtida pelo esquema $IMCA$ e pelo esquema monocritério. Na avaliação da cooperação temos como referência a quantidade de nós cooperativos comparado com a porcentagem de ataque na CRAHN. O esquema monocritério apresenta uma variação de aproximadamente 4% da probabilidade entre os cenários com 3, 6 e 10 nós cooperadores. Os dois casos do esquema $IMCA$ apresentam uma variação de 10% e 15% entre os cenários com diferentes quantidades de nós cooperadores. Na Figura 5.4(b) mostra uma variação da T_k no esquema monocritério, esta corresponde até 9% nos cenários com diferentes quantidades de nós cooperadores. Por outro lado, as variações do esquema $IMCA$ representam 11% e 12%, respectivamente.



(a) Cenário com 50 nós

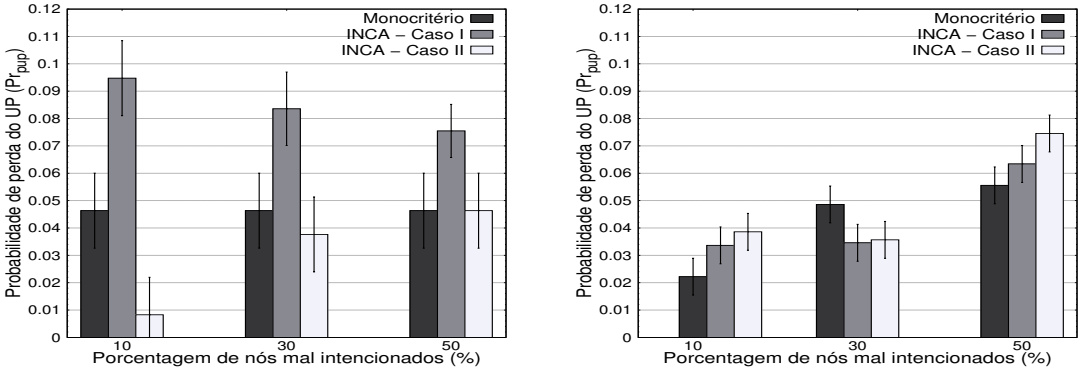
(b) Cenário com 100 nós

Figura 5.4: T_k taxa de detecção por quantidade de vizinhos cooperadores

Nas Figuras 5.4(a) e 5.4(b) ressaltamos que a probabilidade (Pr) apresenta um ganho nos dois casos do esquema $IMCA$ com relação ao esquema monocritério. Isto reforça a eficiência do esquema $IMCA$, onde podemos afirmar que uma abordagem cooperativa junto a uma análise Bayesiana ajuda a obter um melhor desempenho em termos de detecção do ataque EUP. Além disso, observamos que as probabilidades (Pr) do esquema $IMCA$ têm uma variação pequena devido ao acesso aleatório do ataque EUP, isto é, um usuário secundário não necessariamente monitorará o canal que está sendo atacado, devido ao tipo de escolha do canal por parte do usuário secundário.

Assumimos que a rede ad hoc de rádio cognitivo utiliza o espectro de radiofrequências de uma rede primária, por tal motivo consideramos transmissões primárias nos canais licenciados. Contudo, as Figuras 5.5(a) e 5.5(b) apresentam a perda de detecção do usuário primário legítimo (Pr_{pup}). Nos cenários com 50 e 100 nós dispostos na rede com diferentes porcentagens de atacantes, observamos que o Pr_{pup} é menor que 0.1. Estes resultados mostram que o esquema $IMCA$ adiciona a seu desempenho um ganho em relação ao esquema monocritério referente à baixa perda do usuário primário. O esquema $IMCA$ ao adquirir esta vantagem oferece um melhor desempenho na determinação da

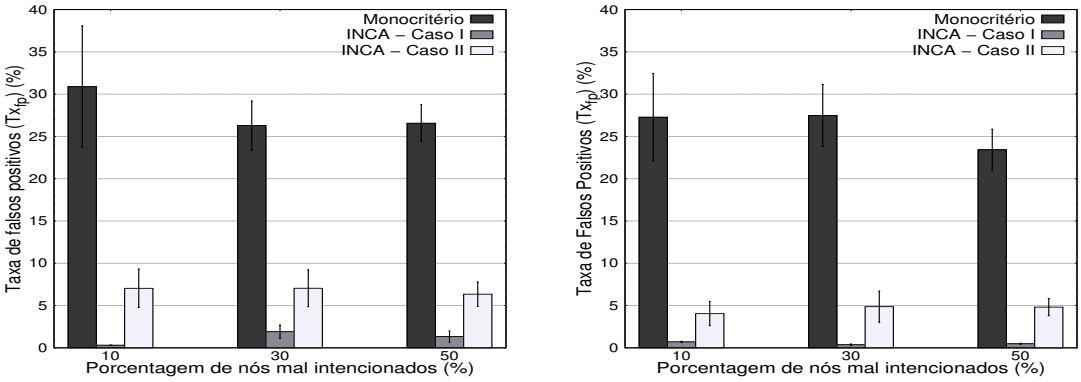
presença do ataque EUP.



(a) Cenário com 50 nós (b) Cenário com 100 nós

Figura 5.5: Pr_{pup} perda de detecção do usuário primário legítimo

O esquema $IMCA$ apresenta uma baixa taxa de falsos positivos, conforme apresentado nas Figuras 5.6(a) e 5.6(b). No cenário com 50 nós e diferentes porcentagens de ataques EUP, mostrado na Figura 5.6(a), a taxa de falsos positivos nos dois casos do esquema $IMCA$ não passa de 7%, enquanto o esquema monocritério tem um alta taxa de falsos positivos que chega até 30%. Nos resultados apresentados na Figura 5.6(b) com 100 nós dispostos na rede, a Tx_{fp} dos dois casos do esquema $IMCA$ não passa de 4% ao comparar com o esquema monocritério que chega até 27%. Nos casos do esquema $IMCA$ esta baixa percentagem de falsos positivos acontece quando o nó detecta que um canal está sendo atacado e na realidade isso não está acontecendo. Nos ambientes de simulação isto ocorre quando um usuário secundário monitora um canal que está sendo utilizado por outro usuário secundário legítimo e estes estão pertos um do outro. Deste modo, o usuário secundário que monitora o canal faz medições dos valores dos critérios no canal e após as análises conclui que é um usuário primário.



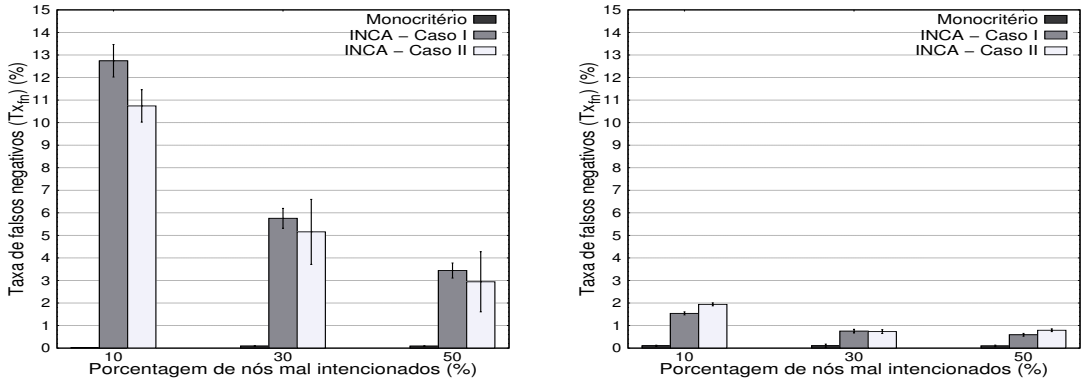
(a) Cenário com 50 nós (b) Cenário com 100 nós

Figura 5.6: Tx_{fp} na detecção de ataques EUPs

Por outro lado, a Tx_{fp} no esquema monocritério apresenta uma alta percentagem nos cenários apresentados. Isto acontece pelo mesmo problema que é visto no esquema

$IMCA$, e outro fator que pode afetar é a ausência de uma análise de múltiplos critérios, já que sua solução é com base em um único critério. Por outro lado, a cooperação não mostra uma melhoria significativa em termos de redução desta taxa de falsos positivos.

O esquema $IMCA$ apresenta uma taxa de falso negativos de 12% e esta diminui até uma taxa de 3% nos diferentes casos do esquema, como mostra a Figura 5.7(a). Essa Tx_{fn} de 12% pode acontecer devido aos atacantes ocuparem os canais de forma aleatória, sendo que alguns usuários secundários podem demorar no sensoreamento desse canal em um momento e no momento seguinte este ataque pode migrar para um outro canal porque um usuário primário iniciou a atividade nesse canal. Dessa forma, os nós que monitoram o canal detectam um usuário primário legítimo com as mesmas características de um atacante.



(a) Cenário com 50 nós (b) Cenário com 100 nós

Figura 5.7: Tx_{fn} na detecção de ataques EUPs

Também pode ser gerado um falso negativo devido ao fato de encontrar um usuário secundário monitorando um canal de frequência que está sendo utilizado por um usuário secundário mal intencionado. Desta forma, pode acontecer que o usuário monitorando o canal determine o atacante como um usuário secundário legítimo, visto que ao realizar as medições, os valores de alguns critérios são correspondentes a um usuário secundário legítimo, o que influencia na análise probabilística para determinar a presença do ataque EUP. Na Figura 5.7(b) a Tx_{fn} é menor a 4% e diminui até 1% para os dois casos do esquema $IMCA$. Por outro lado, o esquema monocritério sempre apresenta uma Tx_{fn} menor a 1%. Contudo, podemos afirmar que o esquema $IMCA$ também apresenta um melhor desempenho em redes com uma quantidade significativa de nós.

5.4 Resumo

Este capítulo apresentou a avaliação do esquema $IMCA$ para a determinação da presença de ataques EUP nas CRAHNs. Foram empregados dois cenários com diferentes quantidades de nós e diferentes porcentagem de nós atacantes. Também foram utilizados dois

estudos de casos do esquema $IMCA$ que apresentam diferentes quantidades e tipos de critérios. Além disso, foi apresentada uma avaliação dos pesos de importância usando a técnica PCA. Inicialmente, apresentamos os resultados do esquema $IMCA$ sem a avaliação de pesos de importância, para depois mostrar os resultados com esta avaliação. Nos cenários empregados o esquema $IMCA$ mostrou ser eficiente na determinação da presença do ataque EUP, frente a outro esquema monocritério que representa aos esquemas tratados na literatura. Porém, o funcionamento do esquema $IMCA$ depende da avaliação de pesos de importância para uma correta análise de múltiplos critérios, juntamente com uma abordagem cooperativa para alcançar uma alta probabilidade da presença do ataque EUP na CRAHN.

CAPÍTULO 6

CONSIDERAÇÕES FINAIS

As redes ad hoc de rádio cognitivo (CRAHN, do inglês, *Cognitive radio ad hoc networks*) são compostas por dispositivos (nós) que utilizam a tecnologia de rádio cognitivo. Esse nós são capazes de monitorar e identificar as frequências ociosas no espectro. Com base em medições e em conhecimentos adquiridos através do histórico de acontecimentos passados, cada nó pode de forma inteligente escolher e reutilizar as porções subutilizadas do espectro. Dois tipos de usuários compartilham o espectro de radiofrequências, estes são denominados de usuários primários e usuários secundários. Sendo que os usuários primários possuem licenças de uso das bandas e maior prioridade para acessá-las, enquanto os usuários secundários não possuem licenças, mas podem usar as bandas quando estas estiverem ociosas.

As CRAHNs são vulneráveis aos ataques de Emulação de Usuário Primário (EUP). Esses ataques são realizados por usuários secundários mal intencionados. Eles usuários imitam as características dos usuários primários legítimos com o objetivo de se beneficiar do uso do espectro. Além disso, estes ataques comprometem o uso das bandas de frequências licenciadas, degradando assim o acesso ao espectro dos usuários secundários legítimos.

Nesse contexto, foi proposto um esquema para anál**I**se **M**ulticritério e **C**ooperativa da presença de **A**taques EUP em redes ad hoc de rádio cognitivo, denominado $IMCA$. O esquema $IMCA$ tem como objetivo determinar a probabilidade da presença de ataque EUP, e ele considera os critérios comumente utilizados em uma transmissão sem fio com uma abordagem cooperativa. O esquema $IMCA$ apresenta duas fases para determinar a presença dos ataques EUPs, a fase *individual* e a fase de *cooperação*.

A fase individual do esquema $IMCA$ permite realizar uma coleta de dados empregando a técnica de detecção pela energia na função de sensoreamento. Posteriormente, os valores coletados são agrupados seguindo a escolha de critérios estabelecidos pelo esquema $IMCA$ e são levados para uma análise individual de múltiplos critérios. Esta análise determina uma probabilidade preliminar do sucesso do ataque EUP calculada individualmente por cada nó da rede. A fase de cooperação inicia com uma troca das probabilidades preliminares entre os nós da rede. Enseguida, cada nó realizará uma fusão das informações aplicando o teorema de Bayes e considerando as probabilidades preliminares trocadas. Esta fusão das probabilidades determinará a probabilidade final da presença do ataque EUP na rede ad hoc de rádio cognitivo.

6.1 Conclusões

O esquema $IMCA$ foi implementado e adicionado aos módulos de uma CRAHN e avaliado na presença de nós mal intencionados na forma de ataques de emulação de usuário primário. Inicialmente, mostramos os resultados sem uma definição dos pesos de importância. Em seguida, os resultados com uma análise de pesos de importância e definidos pela técnica PCA. Os resultados na fase *individual* sem a avaliação de pesos de importância alcançou apenas um ganho de 2.36% em relação a um esquema monocritério definido na literatura. No entanto, os resultados na fase *individual* do esquema $IMCA$ com a definição dos pesos de importância mostraram que houve uma superioridade de até 19% no primeiro estudo de caso, e de até 25% no segundo estudo de caso, frente a um esquema monocritério.

Os resultados alcançados na primeira fase dos dois esquemas concluem que um esquema para detecção dos ataques EUPs não pode ser baseado em um único critério de detecção, pelo fato de que estes atacantes podem modificar suas características de transmissão no espectro. Isto leva que um esquema de detecção monocritério só verifique uma de suas características ou critérios e deixando do lado os critérios restantes que podem influenciar na detecção. Além disso, pode gerar a uma grande taxa de erro de detecção e consequentemente a uma grande taxa de falsos positivos e negativos. Para contrarrestar este problema os resultados do esquema $IMCA$ na primeira fase mostram que uma análise de múltiplos critérios gera uma ótima detecção da presença do ataque EUP, pelo fato de considerar vários destes critérios de transmissão e aplicar um consenso entre eles para determinar se uma presença é mal-intencionada ou não. Como foi apresentado, os resultados mostram que $IMCA$ sem uma avaliação de pesos de importância para cada critério é superior ao esquema monocritério, isto demonstra que uma correta avaliação de pesos de importância pode acrescentar uma correta detecção deste ataque e eliminar as altas taxas de erro de detecção geradas pelo esquema monocritério.

Por outro lado, o esquema $IMCA$ também foi avaliado considerando suas duas fases (*individual* e de *cooperação*). Nesta avaliação os resultados obtidos no esquema $IMCA$ sem a avaliação de pesos de importância mostram um ganho de 15.56% frente a um esquema monocritério. No entanto, os resultados do esquema $IMCA$ com a avaliação de pesos de até importância definida pela técnica PCA mostram um ganho de até 77% e 65% no primeiro e segundo caso respectivamente. Estes resultados alcançados aplicando as duas fases do esquema $IMCA$ reforçam os resultados alcançados na fase *individual*. Como é visto, o esquema monocritério segue uma abordagem cooperativa, mas só considera um único critério, o que pode levar a uma errônea detecção e gerar altas taxas de falsos positivos e negativos. No esquema $IMCA$ isso não acontece porque ele considera a análise de múltiplos critérios juntamente com a correta avaliação de pesos de importância realizada na primeira fase e adiciona o sentido de cooperação entre os nós da rede o que

leva a corrigir detecções errôneas nos nós da rede, e diminuir mais essas taxas de falsos positivos e negativos alcançadas no esquema monocritério.

Desta forma, podemos concluir que o objetivo principal deste trabalho que foi a identificação da presença do ataque EUP na CRAHN foi atingido. Este objetivo foi alcançado pela aplicação da análise de múltiplos critérios definida pela técnica NWAUF, juntamente com uma avaliação de pesos de importância aplicando a técnica PCA e uma abordagem cooperativa. Estes três principais procedimentos foram aplicados e divididos em duas fases para sua ótima iteração e detecção dos ataques EUPs. Cada uma destes procedimentos enriquece mais a detecção, tornando assim um esquema eficiente e eficaz na determinação da presença de ataques EUPs nas CRAHNs.

6.2 Trabalhos futuros

Como trabalhos futuros, pretende-se avaliar o comportamento do esquema $IMCA$ em cenários de nós com movimentação e gasto de energia. Além disso, também pretende-se avaliar cenários mais realísticos, que representem as características autênticas dos usuários secundários. Outras considerações para trabalhos futuros são a análise do custo computacional e a sobrecarga que pode causar o esquema $IMCA$ na rede ad hoc de rádio cognitivo.

6.3 Publicações

Os resultados obtidos com a pesquisa bibliográfica e a análise dos ataques nas redes de rádio cognitivo resultam na publicação seguinte.

- Julio Soto, Robson Melo, Michele Nogueira e Aldri L. dos Santos. Um Modelo Analítico para Avaliação de Desempenho em Redes de Rádio Cognitivo Sob Ataque EUP. *Workshop de Redes de Acesso em Banda Larga (WRA) - SBRC*, Campo Grande, Brasil, 2011.

- Julio Soto, Saulo Queiroz e Michele Nogueira. Managing Sensing and Cooperation to Analyze PUE Attacks in Cognitive Radio Ad Hoc Networks. *8th International Conference on Network and Service Management - CNSM*, Las Vegas, USA, 2012.

- Julio Soto, Saulo Queiroz e Michele Nogueira. Um Esquema Cooperativo para Análise da Presença de Ataques EUP em Redes Ad Hoc de Rádio Cognitivo. *Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais - SBSeg*, Curitiba, Brasil, 2012.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] Anatel. Divisão do espectro no Brasil, último acesso: Agosto 2012. http://www.anatel.gov.br/Portal/exibirPortalInternet.do.

[2] Federal Communication Commision Report FCC. Spectrum policy task force report, no. 02.2135, Novembro 2002.

[3] G. Staple and K. Werbach. The end of spectrum scarcity [spectrum allocation and utilization]. *IEEE Spectrum*, 41(3):48 – 52, Março 2004.

[4] D. Cabric, S.Mishra, D. Willkomm, R. Brodersen, and A. Wolisz. A cognitive radio approach for usage of virtual unlicensed spectrum. In *IST Mobile Wireless Communications Summit*, Junho 2005.

[5] Federal Communication Commision Report FCC. Facilitating opportunities for flexible, efficient, and reliable spectrum use employing cognitive radio technologies, no. 03.108, Novembro 2003.

[6] M. Sousa, R. Lopes, W. Lopes, and M. Alencar. Redes cognitivas um novo paradigmas para as comunicações sem fio. In *Simpósio Brasileiro de Redes de Computadores e Sitemas Distribuídos (SBRC)*, Maio 2010.

[7] Y.-C. Liang, A. Hoang, and H.-H. Chen. Cognitive radio on TV bands: A new approach to provide wireless connectivity for rural areas. *Wireless Communications*, 15(3):16–22, 2008.

[8] D. Cabric, S. Mishra, and R. Brodersen. Implementation issues in spectrum sensing for cognitive radios. In *Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers*, volume 1, pages 772 – 776, Novembro 2004.

[9] I. Akyildiz, W. Lee, M. Vuran, and S. Mohanty. A survey on spectrum management in cognitive radio networks. *IEEE Communications Magazine*, 46(4):40 –48, Abril 2008.

[10] W. Lee and I. Akyldiz. A spectrum decision framework for cognitive radio networks. *IEEE Transactions on Mobile Computing*, 10(2):161 –174, Fevereiro 2011.

[11] S. Tang and B. Mark. Modeling an opportunistic spectrum sharing system with a correlated arrival process. In *IEEE Wireless Communications and Networking Conference (WCNC)*, pages 3297–3302, Abril 2008.

[12] H. Arslan. *Cognitive Radio, Software Defined Radio, and Adaptive Wireless Systems (Signals and Communication Technology)*. Springer-Verlag New York, Inc., Secaucus, EUA, 2007.

[13] C. Haro and L. Giupponi. Radio y redes cognitivas. Technical report, AEI eMOV Plataforma Tecnológica Española de Comunicaciones Inalambricas, Março 2010.

[14] J. Mitola and G. Maguire. Cognitive radio: making software radios more personal. *IEEE Personal Communications*, 6(4):13–18, 1999.

[15] K.-C. Chen, Y.-J. Peng, N. Prasad, Y.-C. Liang, and S. Sun. Cognitive radio network architecture: part I – general structure. In *International Conference on Ubiquitous Information Management and Communication (ICUIMC)*, pages 114 – 119, New York, EUA, 2008. ACM.

[16] I. Akyildiz, W. Lee, M. Vuran, and S. Mohanty. Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey. *Computer networks journal (ELSEVIER)*, 50:2127– 2159, Setembro 2006.

[17] Z. Jin, S. Anand, and K. Subbalakshmi. Detecting primary user emulation attacks in dynamic spectrum access networks. In *IEEE International Conference on Communications (ICC)*, pages 2749– 2753, 2009.

[18] W. Webb. On using white space spectrum. *IEEE Communications Magazine*, 50(8):145 –151, Agosto 2012.

[19] L. Giupponi and A. Perez-Neira. Fuzzy-based spectrum handoff in cognitive radio networks. In *Cognitive Radio Oriented Wireless Networks and Communications (CrownCom)*, pages 1 –6, Maio 2008.

[20] B. Ishibashi, N. Bouabdallah, and R. Boutaba. QoS performance analysis of cognitive radio-based virtual wireless networks. In *IEEE Conference on Computer Communications (INFOCOM)*, pages 2423 –2431, Abril 2008.

[21] A. Yau, P. Komisarczuk, and P. Teal. C2net: A cross-layer quality of service (QoS) architecture for cognitive wireless ad hoc networks. *Australasian Telecommunication Networks and Applications Conference*, pages 306–311, 2008.

[22] S. Anand, Z. Jin, and K. Subbalakshmi. An analytical model for primary user emulation attacks in cognitive radio networks. In *IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, pages 1–6, Outubro 2008.

[23] O. León, J. Hernández-Serrano, and M. Soriano. A new cross-layer attack to TCP in cognitive radio networks. In *IEEE Second International Workshop on Cross Layer Design (IWCLD)*, Junho 2009.

[24] T. Clancy and N. Goergen. Security in cognitive radio networks: Threats and mitigation. In *Cognitive Radio Oriented Wireless Networks and Communications (CrownCom)*, pages 1 –8, Maio 2008.

[25] O. León, J. Hernández-Serrano, and M. Soriano. Securing cognitive radio networks. *International Journal Communication Systems*, 23(5):633–652, 2010.

[26] Z. Jin, S. Anand, and K. Subbalakshmi. NEAT: A neighbor assisted spectrum decisionprotocol for resilience against primary user emulation attacks. *Relatório técnico*, 2010.

[27] O. León, J. Hernández-Serrano, and M. Soriano. Cooperative detection of primary user emulation attacks in CRNs. *Computer Networks*, 2012.

[28] R. Chen and J. Park. Ensuring trustworthy spectrum sensing in cognitive radio networks. In *IEEE Workshop on Networking Technologies for Software Defined Radio Networks*, pages 110 –119, Setembro 2006.

[29] R. Chen, J. Park, and J. Reed. Defense against primary user emulation attacks in cognitive radio networks. *IEEE Journal on Selected Areas in Communications*, 26(1):25–37, Janeiro 2008.

[30] H. Li and Z. Han. Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems, part I: Known channel statistics. *IEEE Transactions on Wireless Communications*, 9(11):3566 –3577, Novembro 2010.

[31] S. Chen, K. Zeng, and P. Mohapatra. Hearing is believing: Detecting mobile primary user emulation attack in white space. In *IEEE Conference on Computer Communications (INFOCOM)*, pages 36 –40, Abril 2011.

[32] Z. Jin, S. Anand, and K. Subbalakshmi. Robust spectrum decision protocol against primary user emulation attacks in dynamic spectrum access networks. In *IEEE Global Telecommunications Conference (GLOBECOM)*, pages 1–5, 2010.

[33] C. Chen, H. Cheng, and Y.-D. Yao. Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack. *IEEE Wireless Communications*, 10(7):2135 –2141, Julho 2011.

[34] A. Min, K.-H. Kim, and K. Shin. Robust cooperative sensing via state estimation in cognitive radio networks. In *IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, pages 185 –196, Maio 2011.

[35] Z. Jin, S. Anand, and K. Subbalakshmi. Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis esting. *Mobile Computing and Communications Review (SIGMOBILE)*, 13:74–85, Setembro 2009.

[36] M. Di Felice, K. Chowdhury, W. Kim, A. Kassler, and L. Bononi. End-to-end protocols for cognitive radio ad hoc networks: An evaluation study. *Performance Evaluation*, 68(9):859 – 875, 2011.

[37] Federal Communication Commision Report FCC. Frequency spectrum allocation chart in united sated, http://www.ntia.doc.gov/osmhome/allochrt.pdf, Outubro 2003.

[38] C. Chen. *Investigation of Primary User Emulation Attack in Cognitive Radio Networks*. Tese de doutorado, Faculty of the Stevens Institute of Technology, Hoboken, EUA, 2011.

[39] B. Ealey. Primary user emulation attacks in cognitive radio - an experimental demonstration and analysis. Dissertação de mestrado, The University of Tennessee, Knoxville, EUA, 2011.

[40] T. Yucek and H. Arslan. A survey of spectrum sensing algorithms for cognitive radio applications. *IEEE Communications Surveys Tutorials*, 11(1):116 –130, Abril 2009.

[41] D. Arianandа, M. Lakshmanan, and H. Nikoo. A survey on spectrum sensing techniques for cognitive radio. In *International Workshop on Cognitive Radio and Advanced Spectrum Management (CogART)*, pages 74 –79, Maio 2009.

[42] E. Axell, G. Leus, and E. Larsson. Overview of spectrum sensing for cognitive radio. In *2nd International Workshop on Cognitive Information Processing (CIP)*, pages 322 –327, Junho 2010.

[43] Y. Ge, Y. Sun, S. Lu, and E. Dutkiewicz. Adsd: An automatic distributed spectrum decision method in cognitive radio networks. In *First International Conference on Future Information Networks (ICFIN)*, pages 253 –258, Outubro 2009.

[44] M. Kaplan and F. Buzluca. A dynamic spectrum decision scheme for heterogeneous cognitive radio networks. In *24th International Symposium on Computer and Information Sciences (ISCIS)*, pages 697 –702, Setembro 2009.

[45] B. Canberk, I. Akyildiz, and S. Oktug. A qos-aware framework for available spectrum characterization and decision in cognitive radio networks. In *IEEE 21st International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC)*, pages 1533 –1538, Setembro 2010.

[46] W. Lee and I. Akyldiz. A spectrum decision framework for cognitive radio networks. *IEEE Transactions on Mobile Computing*, 10(2):161 –174, Fevereiro 2011.

[47] D. Niyato and E. Hossain. Market-equilibrium, competitive, and cooperative pricing for spectrum sharing in cognitive radio networks: Analysis and comparison. *IEEE Transactions on Wireless Communications*, 7(11):4273 –4283, Novembro 2008.

[48] R. Dubey and S. Sharma. Distributed shared spectrum techniques for cognitive wireless radio networks. In *International Conference on Computational Intelligence and Communication Networks (CICN)*, pages 259 –264, Novembro 2010.

[49] R. Zhou, X. Li, V. Chakravarthy, and Z. Wu. Spectrum mobility demonstration of smse based overlay cognitive radio via software defined radio. In *New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, pages 668 –669, Maio 2011.

[50] I. Christian, S. Moh, I. Chung, and J. Lee. Spectrum mobility in cognitive radio networks. *IEEE Communications Magazine*, 50(6):114 –121, Junho 2012.

[51] I. Akyildiz, W. Lee, and K. Chowdhury. Spectrum management in cognitive radio ad hoc networks. *IEEE Network*, 23(4):6 –12, Julho-Agosto 2009.

[52] L. Wang and C. Wang. Spectrum management techniques with qos provisioning in cognitive radio networks. In *IEEE International Symposium on Wireless Pervasive Computing (ISWPC)*, pages 116 –121, Maio 2010.

[53] G. Salami, O. Durowoju, A. Attar, O. Holland, R. Tafazolli, and H. Aghvami. A comparison between the centralized and distributed approaches for spectrum management. *IEEE Communications Surveys Tutorials*, 13(2):274 –290, Abril 2011.

[54] K. Du, M. Swamy, and Q. Ni. A dynamic spectrum access scheme for cognitive radio networks. In *Canadian Conference on Electrical and Computer Engineering (CCECE)*, pages 450 –454, Maio 2009.

[55] R. Mahapatra and E. Strinati. Interference-aware dynamic spectrum access in cognitive radio network. In *IEEE 22nd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC)*, pages 396 –400, Setembro 2011.

[56] X. Zhang and C. Li. The security in cognitive radio networks: a survey. In *International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly (IWCMC)*, pages 309–313, 2009.

[57] A. Araujo, J. Blesa, E. Romero, and D. Villanueva. Security in cognitive wireless sensor networks. challenges and open problems. *EURASIP J. Wireless Comm. and Networking*, page 48, 2012.

[58] N. Shankar, C. Cordeiro, and K. Challapali. Spectrum agile radios: utilization and sensing architectures. In *IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, pages 160 –169, Novembro 2005.

[59] Y. Yuan, P. Bahl, R. Chandra, P. Chou, J. Ferrell, T. Moscibroda, S. Narlanka, and Y. Wu. Knows: Cognitive radio networks over white spaces. In *IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, pages 416 –427, Abril 2007.

[60] P. Pawelczak, G. Janssen, and R. Venkatesha Prasad. Performance measures of dynamic spectrum access networks. In *IEEE Global Telecommunications Conference (GLOBECOM)*, Novembro 2006.

[61] M. Subhedar and G. Birajdar. Spectrum sensing techniques in cognitive radio networks: A survey. *International Journal of NextGeneration Networks*, 3(2):37–51, 2011.

[62] D. Cabric, A. Tkachenko, and R. Brodersen. Experimental study of spectrum sensing based on energy detection and network cooperation. In *ACM International Workshop on Technology and Policy for Accessing Spectrum (TAPAS)*, 2006.

[63] H. Tang. Some physical layer issues of wide-band cognitive radio systems. In *IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, pages 151 –159, Novembro 2005.

[64] F. Digham, M.-S. Alouini, and M. Simon. On the energy detection of unknown signals over fading channels. *IEEE Transactions on Communications*, 55(1):21 –24, Janeiro 2007.

[65] J. Proakis. *Digital Communications*. McGraw-Hill Science/Engineering/Math, 4 edition, Agosto 2000.

[66] R. Tandra and A. Sahai. Fundamental limits on detection in low snr under noise uncertainty. In *International Conference on Wireless Networks, Communications and Mobile Computing*, volume 1, pages 464 – 469, Junho 2005.

[67] N. Khambekar, L. Dong, and V. Chaudhary. Utilizing ofdm guard interval for spectrum sensing. In *IEEE Wireless Communications and Networking Conference (WCNC)*, pages 38 –42, Março 2007.

[68] W. Gardner. Exploitation of spectral redundancy in cyclostationary signals. *IEEE Signal Processing Magazine*, 8(2):14 –36, Abril 1991.

[69] A. Fehske, J. Gaeddert, and J. Reed. A new approach to signal classification using spectral correlation and neural networks. In *IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, pages 144 –150, Novembro 2005.

[70] M. Ghozzi, F. Marx, M. Mischa, and J. Palicot. Cyclostatilonarilty-based test for detection of vacant frequency bands. In *Cognitive Radio Oriented Wireless Networks and Communications*, pages 1 –5, Junho 2006.

[71] S. Mishra, S. Brink, R. Mahadevappa, and R. Brodersen. Cognitive technology for ultra-wideband/wimax coexistence. In *IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, pages 179 –186, Abril 2007.

[72] D. Cabric, A. Tkachenko, and R. Brodersen. Spectrum sensing measurements of pilot, energy, and collaborative detection. In *Military Communication Conference (MILCOM)*, Outubro 2006.

[73] A. Ghasemi and E. Sousa. Asymptotic performance of collaborative spectrum sensing under correlated log-normal shadowing. *IEEE Communications Letters*, 11(1):34 –36, Janeiro 2007.

[74] *Efficient Signaling of Spectral Resources in Spectrum Pooling Systems*, Holanda, Novembro 2003.

[75] C. Guo, T. Zhang, Z. Zeng, and C. Feng. Investigation on spectrum sharing technology based on cognitive radio. In *International Conference on Communications and Networking in China (ChinaCom)*, pages 1 –5, Outubro 2006.

[76] J. Perez-Romero, O. Salient, R. Agusti, and L. Giupponi. A novel on-demand cognitive pilot channel enabling dynamic spectrum allocation. In *IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, pages 46 –54, Abril 2007.

[77] M. Buddhikot, P. Kolodzy, S. Miller, K. Ryan, and J. Evans. Dimsumnet: new directions in wireless networking using coordinated dynamic spectrum. In *IEEE International Symposium on World of Wireless Mobile and Multimedia Networks (WoWMoM)*, pages 78 – 85, Junho 2005.

[78] P. Pawelczak, C. Guo, R. Venkatesha Prasad, and R. Hekmat. Clusterbased spectrum sensing architecture for opportunistic spectrum access networks. Technical report, IEEE Vehicular Technology Conference (VTC), 2006.

[79] R. Keeney. Decision analysis: An overview. *Operations Research*, 30(5), 1982.

[80] M. Marttunen. *Interactive Multi-Criteria Decision Analysis in the Collaborative Management of Watercourses*. Tese de doutorado, Aalto University School of Science, Espoo, Finlândia, Maio 2011.

[81] L. Xu and J.-B. Yan. *Introduction to Multi-Criteria Decision Making and the Evidential Reasoning Approach*. Tese de doutorado, University of Manchester Institute of Science and Technology, Maio 2001.

[82] B. Malakooti, I. Thomas, S. Tanguturi, S. Gajurel, and H. Kim. Multiple criteria network routing with simulation results. *Industrial Engineering Research Conference (IERC)*, 2006.

[83] T. Saaty. The analytic hierarchy process. *McGraw Hill*, 1980.

[84] R. Benayoun, B. Roy, and N. Sussman. Manual de reference du programme electre. *Note De Synthese et Formaton*, 1966.

[85] X. Wang and E. Triantaphyllou. Ranking irregularities when evaluating alternatives by using some electre methods. *Omega*, 36(1):45 – 63, Março 2008.

[86] S. Gajurel and B. Malakooti. Re-configurable antenna & transmission power for location aware manet routing with multiple objective optimization. *Journal of Networks (JNW)*, 3(3):11–18, 2008.

[87] B. Malakooti and I. Thomas. A distributed composite multiple criteria routing using distance vector. In *International Conference on Networking, Sensing and Control (ICNSC)*, pages 42 –47, 2006.

[88] Raj Jain. *The Art of Computer Systems Performance Analysis*. John Wiley and Sons, 1th edition, 1991.

[89] I.T. Jolliffe. *Principal Component Analysis*. Springer Series in Statistics. Springer, 2002.

[90] W. Liang-chen, Z. Xue-feng, and W. Hui. Method of synthetic evaluation based on the principal component analysis and entropy weight. In *International Conference on Computer Application and System Modeling (ICCASM)*, volume 8, pages V8–312 –V8–315, Outubro 2010.

[91] Z. Hui and Y. Honggeng. Application of weighted principal component analysis in comprehensive evaluation for power quality. In *IEEE Power Engineering and Automation Conference (PEAM)*, volume 3, pages 369 –372, Setembro 2011.

[92] M. Triola. *Elementary Statistics*. Addison Wesley, 11 edition.

[93] E. Nakamura, A. Loureiro, and A. Frery. Information fusion for wireless sensor networks: Methods, models, and classifications. *ACM Comput. Surv.*, 39(3), Setembro 2007.

[94] St. Andrews. *Bayes*. School of Mathematics and Statistics, University of St Andrews, Escócia, 2003.

[95] C. Brown. *Bayes' Theorem and the Philosophy of Science*. 2005.

[96] E. Medova. *Bayesian Analysis and Markov Chain Monte Carlo Simulation*. John Wiley Sons, Ltd, 2008.

[97] C. Zhao, W. Wang, L. Huang, and Y. Yao. Anti-pue attack based on the transmitter fingerprint identification in cognitive radio. In *5th International Conference on Wireless Communications, Networking and Mobile Computing (WiCom)*, pages 1 –5, Setembro 2009.

[98] Z. Jin, S. Anand, and K. P. Subbalakshmi. Performance analysis of dynamic spectrum access networks under primary user emulation attacks. In *IEEE Global Telecommunications Conference (GLOBECOM)*, pages 1–5, USA, Miami, Florida, Dezembro 2010.

[99] L. Huang, L. Xie, H.n Yu, W. Wang, and Y. Yao. Anti-pue attack based on joint position verification in cognitive radio networks. In *International Conference on-Communications and Mobile Computing (CMC)*, volume 2, pages 169 –173, Abril 2010.

[100] N.T. Nguyen, R. Zheng, and Z. Han. On identifying primary user emulation attacks in cognitive radio systems using nonparametric bayesian classification. *Signal Processing, IEEE Transactions on*, 60(3):1432 –1445, Março 2012.

[101] A. Fragkiadakis, E. Tragos, and I. Askoxylakis. A survey on security threats and detection techniques in cognitive radio networks. *IEEE Communications Surveys Tutorials*, (99):1 – 18, 2012.

[102] CRAWDAD. Community Resource for Archiving Wireless Data At Dartmouth, último acesso: Agosto 2012. http://crawdad.cs.dartmouth.edu/.

[103] A. Subramanian, J. Cao, Ch. Sung, and S. Das. Understanding channel and interface heterogeneity in multi-channel multi-radio wireless mesh networks. In *Proceedings of the 10th International Conference on Passive and Active Network Measurement*, pages 89–98, Berlin, Heidelberg, 2009. Springer-Verlag.

[104] The R Project for Statistical Computing, último acesso: Agosto 2012. http://www.r-project.org/.