MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
SECRETARIA DE CIÊNCIA E TECNOLOGIA
INSTITUTO MILITAR DE ENGENHARIA
CURSO DE MESTRADO EM SISTEMAS E COMPUTAÇÃO

MARCELO JOSÉ CAMILO

MECANISMOS DE SEGURANÇA EM REDES DE RÁDIOS COGNITIVOS

Rio de Janeiro
2013

INSTITUTO MILITAR DE ENGENHARIA

MARCELO JOSÉ CAMILO

MECANISMOS DE SEGURANÇA EM REDES DE RÁDIOS COGNITIVOS

Dissertação de Mestrado apresentada ao Curso de Mestrado em Sistemas e Computação do Instituto Militar de Engenharia, como requisito parcial para obtenção do título de Mestre em Sistemas e Computação.

Orientador: Prof. Ronaldo Moreira Salles - Ph.D
Orientador: Prof. David Fernandes Cruz Moura - DSc

Rio de Janeiro
2013

INSTITUTO MILITAR DE ENGENHARIA
Praça General Tibúrcio, 80-Praia Vermelha
Rio de Janeiro-RJ CEP 22290-270

XXXXXCamilo, M. J.
Mecanismos de Segurança em Redes de Rádios Cognitivos/ Marcelo José Camilo.
– Rio de Janeiro: Instituto Militar de Engenharia, 2013.
xxx p.: il., tab.

Dissertação (mestrado) – Instituto Militar de Engenharia – Rio de Janeiro, 2013.

1. Rádios Cognitivos. 2. Segurança. I. Título. II. Instituto Militar de Engenharia.

CDD 629.892

INSTITUTO MILITAR DE ENGENHARIA

MARCELO JOSÉ CAMILO

MECANISMOS DE SEGURANÇA EM REDES DE RÁDIOS COGNITIVOS

Dissertação de Mestrado apresentada ao Curso de Mestrado em Sistemas e Computação do Instituto Militar de Engenharia, como requisito parcial para obtenção do título de Mestre em Sistemas e Computação.

Orientador: Prof. Ronaldo Moreira Salles - Ph.D

Orientador: Prof. David Fernandes Cruz Moura - DSc

Aprovada em 28 de Janeiro de 2013 pela seguinte Banca Examinadora:

Prof. Ronaldo Moreira Salles - Ph.D do IME - Presidente

Prof. David Fernandes Cruz Moura - DSc do CTEx

Profa. Michele Nogueira Lima - DSc da UFPR

Prof. Luiz Henrique da Costa Araújo - DSc, do IME

Rio de Janeiro
2013

Dedico esta à minha mãe, irmãos, sobrinhos, e, em especial, à minha esposa Luciana que muito me ajudaram, direta ou indiretamente, nesse trabalho.

AGRADECIMENTOS

Agradeço a todas as pessoas que contribuíram com o desenvolvimento desta dissertação de mestrado, tenha sido por meio de críticas, idéias, apoio, incentivo ou qualquer outra forma de auxílio. Em especial, desejo agradecer à minha esposa Luciana, pelo apoio nessa jornada, e ao Maj David e Ten Cel Salles, pela excelente orientação.

Por fim, a todos os professores e funcionários da Seção de Engenharia de Sistemas (SE/8) do Instituto Militar de Engenharia.

Marcelo José Camilo

Não existem atalhos para o sucesso, mas o trabalho intenso é a estrada mais curta.

Bernardo Rezende (Bernadinho)

SUMÁRIO

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SÍMBOLOS

ABREVIATURAS

AFO	-	*Ataque de Função Objetivo*
ANATEL	-	*Agência Nacional de Telecomunicações*
C2	-	*Comando e Controle*
CDMA	-	*Code Division Multiple Access ou acesso múltiplo por divisão de código*
CRAHN	-	*Cognitive Radio Ad Hoc Networks*
DoS	-	*Denial of Service ou negação de serviço*
EUP	-	*Emulação de Usuário Primário*
FCC	-	*Federal Communications Comission ou Comissão Federal de Comunicações*
FDES	-	*Falsificação de Dados do Espectro Sensoriado*
GSM	-	*Global System for Mobile Communications ou sistema global para comunicações móveis*
HF/CNR	-	*High Frequency/Communications Network Radios ou redes de comunicações rádio de alta frequência*
INCA	-	*múltIplos critérios para aNálise Cooperativa da presença de Ataques*
MIMO	-	*Multiple-Input and Multiple-Output ou múltipla-entrada e múltipla-saída*
NS	-	*Network Simulator ou simulador de rede*
PCS	-	*Personal Communications System ou sistemas de comunicações pessoal*
QoS	-	*Quality of Service ou qualidade de serviço*
RC	-	*Rádio Cognitivo*
RDS	-	*Rádio Definido por Software*
RRC	-	*Redes de Rádios Cognitivos*

RSR	-	*Relação Sinal-Ruído*
UP	-	*Usuário Primário*
SDR	-	*Software Definded Radio ou rádio definido por software*
SISTAC	-	*Sistema Tático de Comunicações*
US	-	*Usuário Secundário*
WiFi	-	*Wireless Fidelity ou fidelidade sem fio*
WiMax	-	*Worldwide Interoperability for Microwave Access ou interoperabilidade mundial para acesso em micro-ondas*

RESUMO

Com o rápido crescimento da quantidade de dispositivos e aplicações que utilizam redes sem fio nos últimos anos (redes de sensores, redes veiculares, etc.), a demanda por espectro cresce de maneira sem precedentes (LIU, 2011), acarretando a necessidade de novas faixas de frequência para a operação das novas aplicações. No entanto, boa parte do espectro eletromagnético já se encontra alocado de maneira fixa a uma aplicação, o que tem se mostrado ineficiente, pois esta política acarreta uma baixa utilização da porção do espectro licenciada.

Rádio Cognitivo é uma tecnologia que possibilita o compartilhamento do espectro de maneira oportunista.

Dentre diversos casos promissores para utilização da tecnologia de RC, tem-se as aplicações comumente usadas em sistemas militares como o Sistema C2 e o SISTAC do Exército Brasileiro. Em um ambiente de RC sob ataques, a ausência de mecanismos de proteção ou a utilização de estratégias de mitigação equivocadas podem comprometer o desempenho desejado, seja por meio da redução da confiabilidade, redução da vazão ou no aumento da interferência causada ao UP.

Considerando o exposto acima, o presente trabalho tem por objetivo estudar e propor mecanismos de segurança para RRC, objetivando mitigar ou atenuar os efeitos de ataques de interferência e de emulação de usuário primário.

Nesta dissertação, propomos a arquitetura CMPS para RC que contempla a segurança espectral. Assim, mecanismos de defesa podem ser validados. Como proposta, a arquitetura CMPS apresenta o componente de Segurança Espectral como aprimoramento do ciclo cognitivo descrito em (AKYILDIZ, 2006) e considerando os quatro conjunto de informações de entrada principais listados por (DOYLE, 2009): informações do ambiente rádio, informações dos requisitos de QoS da aplicação, informações dos recursos disponíveis para o dispositivos e informações da política regulatório do uso do espectro.

Estudamos os efeitos do ataque de interferência em redes de rádios cognitivos. Avaliamos os efeitos dos perfis de ocupação espectral do usuário primário e do atacante, bem como de parâmetros da camada física na confiabilidade e na vazão média da rede. Propomos um mecanismo anti-interferência em RRC que calcula a melhor ocupação espectral para o usuário secundário, introduz a aleatoriedade na escolha de canais e transmite as mensagens de controle e os dados de maneira redundante em múltiplos canais.

Estudamos os efeitos do ataque de emulação de usuário primário em redes de rádios cognitivos. Avaliamos os efeitos dos perfis de ocupação espectral do usuário primário e do atacante, bem como de parâmetros da camada física na vazão média da rede. Propomos um mecanismo de mitigação de ataque de EUP em RRC que introduz a aleatoriedade e utiliza informações da camada física para a escolha de canais.

A contribuição esperada deste trabalho é auxiliar e orientar projetistas e desenvolvedores da tecnologia de RC a mitigar ou atenuar os efeitos dos ataques sofridos pelas arquiteturas desta nova tecnologia disponibilizadas para utilização, uma vez que os mecanismos propostos podem ser utilizados.

ABSTRACT

Due to the rapid increase in the number of devices and applications that use wireless networks (network sensors, vehicular networks and so on), the demand for spectrum is growing in an unprecedented way (LIU, 2011). As a consequence, new frequency bands for the operation of new applications are needed. However, most of the frequency bands that may be used with currently available technology is already licensed in a fixed manner to specific type of applications. This policy has shown to be inefficient because it causes a low utilization of the licensed spectrum.

Cognitive Radio is a technology that enables the spectrum sharing in an opportunistic fashion

Whereas, among many promising cases of use for cognitive radio technology, there are the applications commonly used in military scenario, such as Command and Control System, and the Tactical Communications System of the Brazilian Army. In a cognitive radio network under attacks, the absence of defense mechanisms or the use of wrong strategies mitigation can damage the desired performance, by reducing the reliability, reduction the throughput, or increasing the interference caused over the primary user.

Considering the above, this work aims to study and propose defense mechanisms for cognitive radio networks. These mechanisms aims to mitigate or alleviate the effects of jamming and primary user emulation attacks.

In this work, we propose a cognitive radio architecture which includes the spectrum security. Thus, defense mechanisms can be validated. As proposed, the architecture introduces the spectrum security component as an improvement of the of cognitive cycle as described in (AKYILDIZ, 2006) and it considers four broad inputs as described in (DOYLE, 2009): radio environment information, the QoS requirements of the applications, information the resources available for the devices and information about the policy of spectrum usage.

We study the effects of jamming attacks in cognitive radio networks. We analyze the effects of spectral occupation of the primary user and of the attacker, and of the parameters of the physical layer on reliability and throughput Quality of Service requirements. We propose an anti-jamming mechanism for cognitive radio networks that calculates the optimal spectral occupation of the secondary user, introduces the randomness in the choice of channels, and transmits the control messages and the data redundantly across multiple channels.

Finally, We studied the effects of the primary user emulation attack in cognitive radio networks. We analyze the effects of spectral occupation of the primary user and of the attacker, and of the physical layer parameters on reliability and throughput Quality of Service requirements. We propose a mechanism to mitigate primary user emulation attacks in cognitive radio networks. This mechanism introduces the randomness and uses information of the physical layer for choosing channels.

As the proposed mechanisms can be used on new cognitive radio architectures available for use, we expect that this work assists and guides designers and developers of the cognitive radio technology to mitigate or alleviate the effects of the attacks.

1 INTRODUÇÃO

1.1 MOTIVAÇÃO PARA RÁDIOS COGNITIVOS

O espectro eletromagnético é um recurso natural utilizado como meio de transmissão das comunicações sem fio. A utilização do espectro é regulamentada pelas agências governamentais, como a ANATEL (Agência Nacional de Telecomunicações) no Brasil (ANATEL, 2012) e a FCC (Federal Communications Comission ou Comissão Federal de Comunicações) nos Estados Unidos (FCC, 2002). Nesta política, é atribuída aos detentores da licença, chamados de UP (Usuários Primários), a utilização de uma faixa de frequência do espectro, por um longo período de tempo ou de forma permanente, para grandes regiões geográficas (AKYILDIZ, 2006).

Com o rápido crescimento da quantidade de dispositivos e aplicações que utilizam redes sem fio nos últimos anos (redes de sensores, redes veiculares, etc.), a demanda por espectro cresce de maneira sem precedentes (LIU, 2011), acarretando a necessidade de novas faixas de frequência para a operação das novas aplicações.

No entanto, boa parte do espectro eletromagnético já se encontra alocado de maneira fixa a uma aplicação, o que tem se mostrado ineficiente, pois esta política acarreta uma baixa utilização da porção do espectro licenciada. A FIG. 1.1 (NEEL, 2010) mostra a utilização do espectro para determinadas aplicações, onde nota-se que quantidade significativa permanece inutilizada.

Conclui-se que o problema chave não é a falta de capacidade do espectro, mas sim a sua baixa utilização. O desafio que surge é como utilizar de maneira mais eficiente as faixas de frequência subutilizadas.

RC (Rádio Cognitivo) é uma tecnologia que possibilita o compartilhamento do espectro de maneira oportunista, pois os usuários que não possuem licença para utilização deste recurso, conhecidos como US (Usuários Secundários), estão habilitados a utilizar as lacunas espectrais, a saber, porções do espectro que não estão sendo usadas em um momento ou local específicos, desde que não interfiram nas transmissões dos detentores da licença (LIU, 2011). A FIG. 1.2 ilustra o conceito de lacunas espectrais.

A tecnologia de RC é uma solução promissora para aliviar o problema da ineficiência

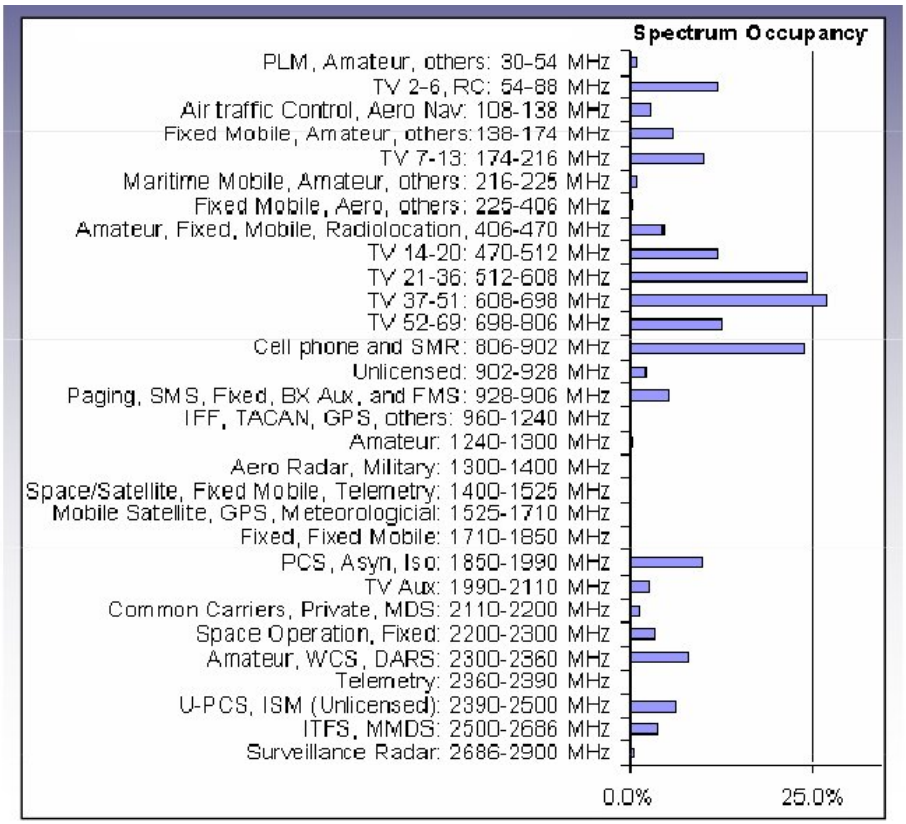

FIG. 1.1: Utilização do Espectro (NEEL, 2010)

na utilização do espectro, pois o uso oportunista do espectro é uma resposta ao desafio descrito e descortina-se no horizonte a medida que saímos de uma política de uso estático do espectro e tem o potencial de reduzir as "barreira "para a entrada de novos empreendimentos e de incrementar a utilização do espectro.

1.1.1 APLICAÇÃO DA TECNOLOGIA DE RÁDIOS COGNITIVOS EM REDES MILITARES

Dentre diversos casos promissores para utilização da tecnologia de RC, tem-se as aplicações comumente usadas em sistemas militares como o Sistema C2 (Comando e Controle) e o SISTAC (Sistema Tático de Comunicações) do Exército Brasileiro.

Aplicações militares, tais como sistemas logísticos, de comunicações, acionamento de armas, navegação, geolocalização, radares e redes de sensores são grandes utilizadoras do espectro e de diferentes tipos de sistemas sem-fio (DOYLE, 2009). Estas aplicações necessitam de acesso eficiente e seguro ao espectro.

Segundo (SALLES, 2008), de maneira geral, os sistemas de enlace mais utilizados em

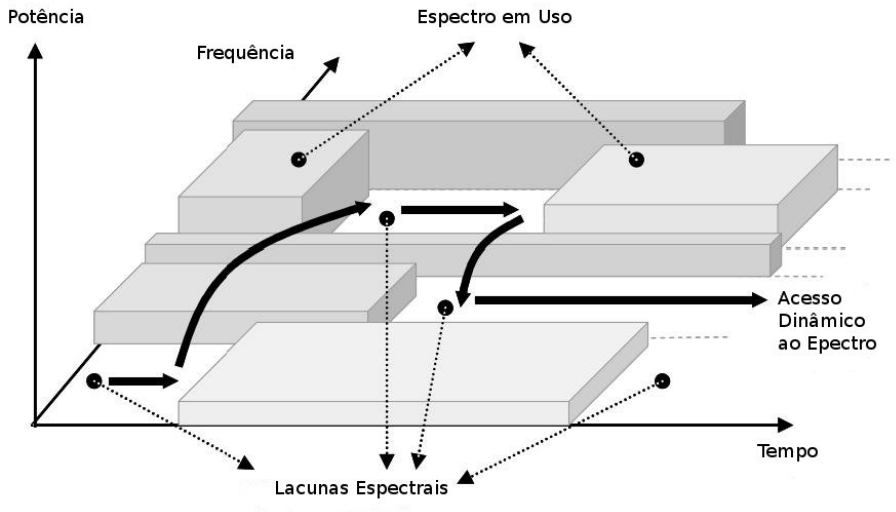

FIG. 1.2: Lacunas espectrais. Adaptado de (AKYILDIZ, 2006)

redes militares são os sistemas rádio e o cabeado. Em especial, o sistema rádio deve ser utilizado de forma restrita, dada a vulnerabilidade a ações de guerra eletrônica; contudo, dada sua flexibilidade e rapidez de desdobramento, pode se constituir na base do SISTAC do Exército Brasileiro.

O autor ainda cita que três requisitos são estritamente relacionados e constituem um forte compromisso em sistemas de comunicação militares: alcance, capacidade e mobilidade. O forte relacionamento existente se dá, em geral, pelo fato que ao variar um dos fatores os outros dois também variam.

Assim, as RRC (Redes de Rádios Cognitivos) figuram como uma solução promissora em redes militares, pois, devido a sua capacidade de alterar seus parâmetros de transmissão com base na interação com o seu ambiente, tal solução aumenta a flexibilidade, a rapidez de desdobramento e a possibilidade de interoperabilidade entre redes heterogêneas, possibilitando maiores alcance, capacidade e mobilidade.

1.1.2 SEGURANÇA EM REDES DE RÁDIOS COGNITIVOS

Em paralelo ao desenvolvimento da tecnologia de RC, surgem os problemas de segurança em RRC (CAMILO, 2012a), tais como a EUP (Emulação de Usuário Primário) (CHEN, 2008b), a FDES (Falsificação de Dados do Espectro Sensoreado) (CHEN, 2008a) e o ataque de interferência (WANG, 2011).

A EUP (CHEN, 2008b) é executada por um US atacante, egoísta ou malicioso, que

emula o comportamento e as características do sinal do UP com o objetivo de ganhar prioridade no uso do espectro, impedindo, assim que os US legítimos acessem o espectro.

A FDES (CHEN, 2008a) ocorre quando, em uma RRC com sensoriamento do espectro cooperativo, US atacantes enviam dados falsos sobre o sensoriamento do espectro, resultando em detecções incorretas pelos US.

O ataque de interferência é um tipo de ataque DoS (*Denial of Service* ou Negação de Serviço) cujo objetivo é impossibilitar ou prejudicar o funcionamento da comunicação nas camadas física e de enlace de dados de uma rede sem fio. Neste ataque, um US malicioso pode impedir que usuários legítimos utilizem as faixas de frequência para as quais estão habilitados, por meio da irradiação, ao longo do tempo, de altos níveis de energia, com ou sem transmissão de dados, em uma faixa de frequência alocada aos usuários sob ataque.

Em um ambiente de RC sob ataques, a ausência de mecanismos de proteção ou a utilização de estratégias de mitigação equivocadas podem comprometer o desempenho desejado, seja por meio da redução da confiabilidade, redução da vazão ou no aumento da interferência causada ao UP, pois o atacante, dada a possibilidade de também dispor da tecnologia RC, pode adotar ações diferentes em cada intervalo de tempo (WANG, 2011), como, por exemplo, interferir em canais diversos utilizando potências diferentes.

1.2 MODELAGEM DO SISTEMA DE REFERÊNCIA

Consideramos que há uma estação base secundária na RRC que coordena a utilização do espectro por todos os US legítimos. Portanto, consideramos, todos os US legítimos como uma única entidade denominada US legítimo. Assumimos que a RRC modelada é um sistema com acesso por divisão de tempo, ou seja, o tempo é dividido em intervalos discretos (*slots*), T_f. As transmissões dos UP sempre começam no início de cada intervalo.

Consideramos uma rede com acesso oportunista ao espectro, onde o US pode ocupar o espectro que pertence a vários UP quando estes não estiverem transmitindo. Consequentemente, as faixas de frequência não utilizadas podem ser selecionadas, compartilhadas com outros usuários e exploradas sem interferências para os UP. Como consequência deste mecanismo e da atividade dos UP, a disponibilidade do espectro, ou seja, o número de canais disponíveis para transmissão, N_c, pode variar em função do tempo.

Como utilizam a tecnologia de RC, tanto o US legítimo quanto o atacante pode identificar as lacunas espectrais que não estão sendo usadas em um momento ou canal específicos.

1.2.1 DESVANECIMENTO DO CANAL

Consideramos que tanto os UP quanto os US estão conectados através de canais rádios sujeitos a desvanecimento, fenômeno causado pela propagação em várias direções das ondas de rádio entre um transmissor e um receptor. Esta propagação pode levar a flutuações de amplitude, de fase e de ângulo do sinal recebido (SKLAR, 1997).

A principal característica de um canal com desvanecimento é que este é um processo aleatório e correlacionado ao longo do tempo, ou seja, o canal de comunicação é um sistema dinâmico com o ganho do desvanecimento sendo um processo aleatório que varia ao longo do tempo de uma maneira correlata (SADEGHI, 2008).

Definimos a capacidade do canal como a quantidade de bits que podem ser transmitidos, em um dado intervalo de tempo t neste canal. Este valor é diretamente proporcional a largura de banda do canal e muda em função do tempo devido à estratégia de modulação mais adequada em face da RSR (Relação Sinal-Ruído).

Consideramos K estratégias de modulação. Dividimos o intervalo de valores da RSR do canal, γ, em $K+1$ regiões mutuamente exclusivas:

$[v_0 = 0, v_1), [v_1, v_2), ..., [v_{K-1}, v_K), [v_K, v_{K+1} = \infty)$,

sendo $0 < v_1 < v_2 < ... < v_{K-1} < v_K$.

Caso a RSR esteja no intervalo $[v_0 = 0, v_1)$, o US opta por não transmitir. Logo, a qualidade do canal neste caso é igual a 0. É utilizada a estratégia de modulação m, $m \in \{1, 2, ..., K\}$, se o valor da RSR do canal neste período de tempo estiver na região $[v_m, v_{m+1})$. Considerando que a estratégia de modulação m possibilita a transmissão de m bits por símbolo, temos $K+1$ valores para a capacidade do canal, $0, b, 2b, ..., Kb$.

Dado o canal com desvanecimento plano e lento e baixa mobilidade dos transmissores e receptores, cenário típico de operações militares que utilizam as redes táticas em VHF do comando da brigada com os comandos de batalhões, conforme mencionado em (MOURA, 2011), empregamos o modelo de Rayleigh para representação do canal de comunicações.

1.3 OBJETIVOS DA DISSERTAÇÃO E ORGANIZAÇÃO DO TEXTO

Considerando que, dentre diversos casos promissores para utilização da tecnologia de RC, tem-se as aplicações comumente usadas em sistemas militares como o Sistema C2 e o SISTAC do Exército Brasileiro e que em um ambiente de RC sob ataques, a ausência de mecanismos de proteção ou a utilização de estratégias de mitigação equivocadas podem

comprometer o desempenho desejado, seja por meio da redução da confiabilidade, redução da vazão ou no aumento da interferência causada ao UP, o presente trabalho tem por objetivo estudar e propor mecanismos de segurança para RRC, objetivando mitigar ou atenuar os efeitos de ataques de interferência e de emulação de usuário primário.

Os pontos em aberto identificados neste trabalho são:

- Arquitetura de RC que contempla segurança espectral;
- Mecanismos anti-interferência e
- Mecanismos anti-EUP.

Para alcançar tal resultado, o presente trabalho apresenta três propostas. A primeira, com base em (CAMILO, 2012b), é a arquitetura CMPS para RC que contempla segurança espectral. Assim, mecanismos de defesa podem ser validados. Como proposta, a arquitetura CMPS, mostrado na FIG. 1.3, apresenta o componente de Segurança Espectral como aprimoramento do ciclo cognitivo descrito em (AKYILDIZ, 2006) e considerando os quatro conjunto de informações de entrada principais listados por (DOYLE, 2009): informações do ambiente rádio, informações dos requisitos de QoS (Quality of Service ou qualidade de serviço) da aplicação, informações dos recursos disponíveis para o dispositivos e informações da política regulatório do uso do espectro.

A segunda é um mecanismo anti-interferência em RRC que, com base em (CAMILO, 2012a), calcula a melhor ocupação espectral para o usuário secundário, introduz a aleatoriedade na escolha de canais e transmite as mensagens de controle e os dados de maneira redundante em múltiplos canais. Neste fase, estudamos os efeitos do ataque de interferência em RRC. Avaliamos os efeitos dos perfis de ocupação espectral do usuário primário e do atacante, bem como de parâmetros da camada física na confiabilidade e na vazão média da rede. Experimentos numéricos mostram que o mecanismo proposto neste trabalho possibilita valores da probabilidade de transmissão e esperança de vazão, respectivamente, 18,21%, e 106,88% maiores que os da estratégia de escolha aleatória de ocupação espectral do US Legítimo. Na comparação do mecanismo proposto neste trabalho com o proposto por (WANG, 2011), em um cenário onde o número de canais disponíveis para transmissão varia em média a cada 10s, nosso mecanismo proposto possibilita valores da probabilidade de transmissão e esperança da vazão, respectivamente, 16,73% e 20,19% maiores.

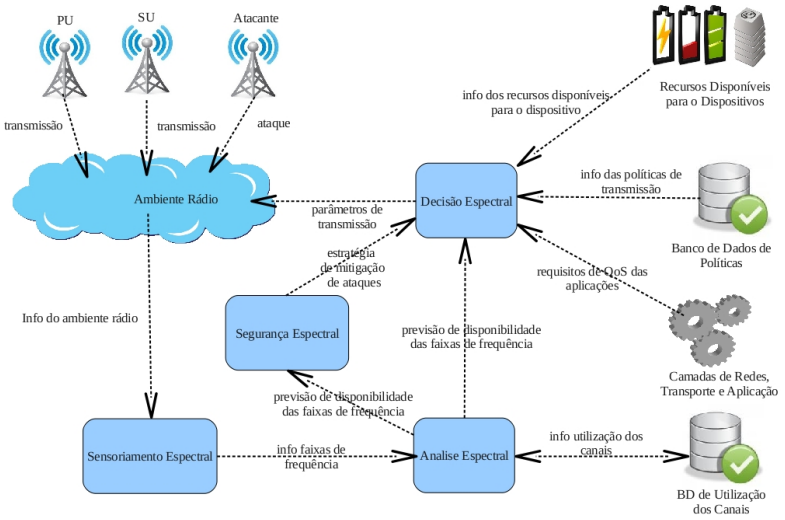

FIG. 1.3: Arquitetura CMPS para RC

Por fim, a terceira proposta é um mecanismo de mitigação de ataque de EUP em RRC que introduz a aleatoriedade e utiliza informações da camada física para a escolha de canais. Neste fase, estudamos os efeitos do ataque de emulação de usuário primário em RRC. Avaliamos os efeitos dos perfis de ocupação espectral do usuário primário e do atacante, bem como de parâmetros da camada física na vazão média da rede. Experimentos numéricos mostram que o mecanismo proposto neste trabalho possibilita valores da probabilidade de transmissão e esperança de vazão, respectivamente, 153,55%, e 399,83% maiores que os da estratégia de atribuição fixa de canais. Na comparação do mecanismo proposto neste trabalho com o mecanismo com base no trabalho de (CHEN, 2009), nosso mecanismo proposto obtêm o mesmo valor da probabilidade de transmissão e possui valor da esperança da vazão 6,86% maior.

A contribuição esperada deste trabalho é auxiliar e orientar projetistas e desenvolvedores da tecnologia de RC a mitigar ou atenuar os efeitos dos ataques sofridos pelas arquiteturas desta nova tecnologia disponibilizadas para utilização, uma vez que os mecanismos propostos podem ser utilizados.

Os demais capítulos desta dissertação obedece à seguinte disposição:

No Capítulo 2, fazemos uma revisão sobre a tecnologia de RC, no qual, definimos seus principais conceitos. Também discutimos as RRC, enumeramos suas prováveis aplicações tanto civis quanto militares e abordamos seus aspectos de segurança. Por fim, citamos

trabalhos relacionados aos ataque de interferência e emulação de usuário primário nas RRC.

No Capítulo 3, descrevemos a metodologia utilizada, iniciamos com a descrição do sistema de referência, depois, enumeramos os indicadores de desempenho em RRC, propomos a arquitetura CMPS para RC, descrevemos os mecanismos anti-interferência e anti-EUP propostos e, por fim, analisamos o desempenhado destes mecanismos.

No Capítulo 4, apresentamos os resultados obtidos, no qual, mostramos os experimentos numéricos e simulações realizados com os mecanismos anti-interferência e anti-EUP, bem como a comparação do desempenho dos nossos mecanismos proposto com outras abordagens.

No Capítulo 5, apresentamos as conclusões do trabalho, indicando as contribuições da dissertação, bem como as oportunidades de trabalhos futuros.

2 RÁDIOS COGNITIVOS

Neste capítulo, fazemos uma revisão sobre a tecnologia de RC, no qual, definimos seus principais conceitos. Também discutimos as RRC, enumeramos suas prováveis aplicações, tanto civis quanto militares, e abordamos seus aspectos de segurança. Por fim, citamos trabalhos relacionados aos ataque de interferência e emulação de usuário primário nas RRC.

2.1 DEFINIÇÃO DE RÁDIO COGNITIVO

Um RC, termo cunhado pelo Prof. Dr. Joseph Mitola em 1999 (MITOLA, 1999), conforme definido em (HAYKIN, 2005), é um sistema de comunicação sem fio inteligente, capaz de utilizar metodologias de aprendizagem e compreensão, tais como *reinforcement learning* (HU, 1998), algoritmos genéticos (LINDEN, 2006), entre outras, para adaptar seus parâmetros operacionais à dinâmica do ambiente ao seu redor. Assim, segundo (REED, 2005), um RC é um rádio que percebe e está ciente de seu ambiente operacional e pode, dinâmica e automaticamente, ajustar seus parâmetros operacionais de acordo com esse ambiente. É um tipo de rádio que aprende com experiências anteriores e lida com situações que não foram planejadas em sua concepção. Segundo (DOYLE, 2009), de maneira simples, um RC é um rádio inteligente.

Em (AKYILDIZ, 2006), RC é definido formalmente como um rádio que pode mudar seus parâmetros de transmissão com base na interação com o ambiente no qual opera. Estes parâmetros podem ser das camadas física (frequência, potência do sinal e estratégias de modulação e de codificação utilizada), de enlace (técnicas de acesso ao meio e de retransmissão) ou das camadas superiores (estratégia de autenticação e algoritmo de criptografia).

Segundo (DOYLE, 2009) para que um RC opere de maneira adequada, mais do que simplesmente informações do espectro eletromagnético, ele deve utilizar 4 tipos de informações, todas fornecidas pelo ambiente de operação no qual está imerso: informações do ambiente rádio, dos requisitos de QoS da aplicação, dos recursos disponíveis para o dispositivo e da política regulatória do uso do espectro.

Como exemplo de informações do ambiente rádio, citam-se as faixas de frequências

livres e utilizadas, o tipo de usuário das faixas (UP, US ou nenhum), a RSR, a potência de transmissão e as estratégias de modulação utilizadas. As informações dos requisitos de QoS das aplicações em execução incluem métricas como vazão, confiabilidade, atraso de transmissão e variação do atraso de transmissão. Como informações dos recursos disponíveis para o dispositivos, tem-se a quantidade de energia disponível nas baterias, o número de antenas em condições de transmissão e/ou recepção, a quantidade de memória livre, a taxa de utilização do processador, entre outras. Por fim, nas informações da política regulatória do uso do espectro figuram canais que tem prioridade ou são proibidos de serem utilizados em determinados momentos e/ou locais, devido a fatores econômicos, estratégicos e/ou de segurança, além da potência máxima de transmissão em determinadas regiões.

2.1.1 RÁDIOS COGNITIVOS VERSUS SISTEMAS ADAPTATIVOS

No entanto, é preciso diferenciar um RC de outros sistemas de comunicação sem fio que possuem a capacidade de alterar alguns de seus parâmetros de transmissão. Estes são conhecidos como sistemas adaptativos. Estes últimos ilustram sistemas de comunicação que podem adaptar e alterar seus comportamentos de várias maneiras, objetivando manter a conectividade em face de variações nas condições e circunstâncias do dispositivo e do ambiente rádio.

Como exemplo de sistemas adaptativos, temos as redes de celulares que utilizam o protocolo CDMA (Code Division Multiple Access ou acesso múltiplo por divisão de código). Estes dispositivos transmitem seus sinais com intensidade inversa ao do nível de potência que recebem da estação base ou podem, ao serem instruídos pela estação base, aumentar ou diminuir sua potência de transmissão (TANEMBAUM, 2003) com o objetivo de que os sinais de todos os dispositivos da rede sejam recebidos com a mesma intensidade. Outro exemplo são os sistemas WiMAX (Worldwide Interoperability for Microwave Access ou interoperabilidade mundial para acesso em micro-ondas) que podem adaptar sua modulação de acordo com sua distância da estação base, de forma a manter uma elevada vazão e a estabilidade da conexão (DOYLE, 2009).

Nos exemplos acima, as alterações são bem definidas e podem ser antecipadas como base em condições conhecidas, como o nível de sinal no caso do CDMA e a distância à estação base no caso do WiMAX. Em um RC, essas adaptações podem ser diferenciadas dos sistemas acima de duas maneiras (DOYLE, 2009): todos os parâmetros de transmissão

possíveis podem ser alterados e essas alterações podem ser realizadas não somente no início de uma transmissão, mas em qualquer momento de acordo com suas interações com o ambiente de operação do rádio.

2.1.2 RÁDIOS COGNITIVOS VERSUS RÁDIO DEFINIDO POR SOFTWARE

RC é considerado um sistema mais avançado que os RDS (Rádio Definido por Software), definido pelo *Wireless Innovation Forum* como um rádio em que algumas ou a totalidade das funções da camada física são definidos por software, ou seja, uma coleção de tecnologias de hardware e software que permite sistemas com arquitetura reconfigurável para redes sem-fio e terminais móveis. Ainda segundo o *Wireless Innovation Forum*, a tecnologia RDS provê solução eficiente e comparativamente barata para o problema de construir dispositivos sem-fio, multi-modo, multi-banda e multi-funcionais que podem ser adaptados, atualizados e/ou melhorados através da atualização de seu conjunto de software.

Enquanto um RDS pode ter seus parâmetros de transmissão reconfigurados pelo usuário através de seu conjunto de software, um RC pode alterar seu parâmetros de transmissão de maneira autônoma, com base em sua interação como o ambiente de operação.

2.1.3 CARACTERÍSTICAS PRINCIPAIS DE RÁDIOS COGNITIVOS

A partir das definições citadas, duas características de RC podem ser destacadas: capacidade cognitiva e reconfiguração, definidas a seguir.

- Capacidade Cognitiva

Capacidade cognitiva é a habilidade para capturar e sensorear, em tempo real, o ambiente no qual o equipamento está inserido. Desse modo, um RC pode identificar as lacunas espectrais. Consequentemente, os melhores parâmetros de transmissão podem ser selecionados. Por exemplo, a faixa de frequência mais adequada para a transmissão pode ser selecionada, compartilhada com outros usuários e explorada sem interferência ao UP.

- Reconfiguração

Reconfiguração é a capacidade para, rápida e dinamicamente, alterar seus parâmetros de transmissão em face de mudanças ocorridas em seu ambiente de operação. Um RC dispõe

de várias opções de parâmetros de transmissão e recepção, de acordo com as diferentes tecnologias suportadas pelo seu hardware. Por exemplo, um RC, ao detectar que o canal que está utilizando está sendo interferido, pode alterar sua faixa de frequência de transmissão para outro canal não interferido. Outro exemplo de reconfiguração é o aumento da potência de transmissão com o objetivo de aumentar a RSR.

2.1.4 CICLO COGNITIVO

Ciclo cognitivo representa as tarefas necessárias para que um RC opere utilizando os parâmetros de transmissão de forma a atender aos requisitos de QoS da aplicação, com a menor utilização de seus recursos disponíveis e atendendo as limitações da política de utilização do espectro.

Com inspiração no processo cíclico de observar, decidir e agir, tem que os seguintes passos são executados por um RC (DOYLE, 2009): obtenção das informações de entrada que precisa, processamento das informações, decisão de auto-configuração, execução da decisão tomada no item anterior e aprendizado com os passos executados acima.

Tais passos, presente no ciclo cognitivo, definido por (AKYILDIZ, 2006), são realizados em três fases: Sensoriamento Espectral, Análise Espectral e Decisão Espectral. Estas três fases são mostradas na FIG. 2.1 e explicadas nos parágrafos seguintes.

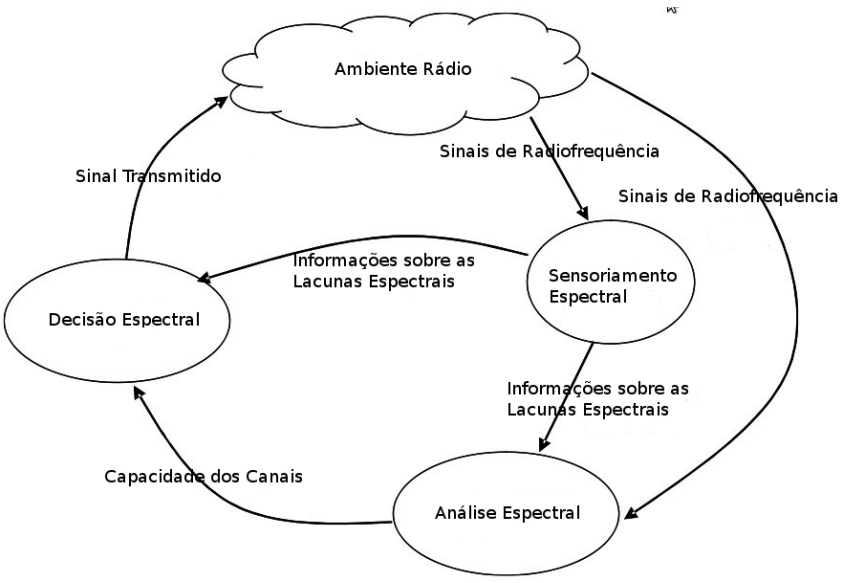

FIG. 2.1: Ciclo Cognitivo. Adaptado de (AKYILDIZ, 2006)

- Sensoriamento Espectral

O sensoriamento espectral permite monitorar as banda licenciadas disponíveis. Este realiza a detecção do início e do fim das atividades do UP, possibilitando identificar as lacunas espectrais. O RC monitora o espectro eletromagnético e produz informações sobre as faixas de frequência, tais como tipo de usuário que a está utilizando (UP, US ou nenhum) e RSR.

De acordo com (TANDRA, 2005), um dos maiores desafios em RC é realizar um balanceamento entre a proteção do UP contra interferência do US e o uso eficiente da faixa de frequência legada, para o qual o sensoriamento do espectro é essencial. Uma vez que essas oportunidades de utilização da frequência são aproveitadas pelo US, as técnicas de sensoriamento do espectro devem detectar o retorno do UP para que o US possa desocupar o canal imediatamente.

Vários trabalhos, como (SAHAI, 2004), (YUCEK, 2009), (ARIANANDA, 2009) e (CABRIC, 2004), citam técnicas de sensoriamento espectral. Entre estas técnicas podemos citar: a detecção de padrões de sinal, quando as carácterísticas dos sinais monitorados são conhecidas pelo RC, a detecção de energia, aplicada quando o RC não conhece suficientemente os sinais monitorados e a detecção de carácterísticas periódicas dos sinais, válida quando o sinal monitorado possui padrões periódicos.

Em uma RRC, o sensoriamento do espectro pode ser feito utilizando abordagens não-cooperativas ou cooperativas. Nas abordagens não-cooperativas, cada dispositivo realiza individualmente o sensoriamento do espectro. Nas abordagens cooperativas, os dispositivos colaboram entre si no sensoriamento do espectro.

- Análise Espectral

A análise espectral é responsável por gerar a lista de previsão de disponibilidade dos canais, com base em uma lista de informações das faixas de frequência recebida da fase de sensoriamento espectral e, possivelmente, um banco de dados de utilização das faixas de frequência. Os trabalhos de (FCC, 2003), (TANG, 2005) e (WILD, 2005) abordam esta fase.

- Decisão Espectral

Para realizar suas transmissões, o RC precisar escolher um ou mais canais e decidir a ocupação espectral (controle, dados, etc.) para cada um dos canais escolhidos. A decisão espectral determina a faixa de frequência e demais parâmetros a serem utilizados na

transmissão, utilizando as informações das fases anteriores. A decisão espectral também é preâmbulo para o compartilhamento do espectro. Alguns algoritmos para decisão espectral são apresentados em (GE, 2009), (KAPLAN, 2009), (CANBERK, 2010) e (LEE, 2011).

2.2 REDES DE RÁDIOS COGNITIVOS

As RRC são compostas por dispositivos utilizando a tecnologia de RC e capazes de sensorear o espectro, objetivando identificar as lacunas espectrais. Com base em medições e em conhecimentos adquiridos através do histórico de acontecimentos passados, cada dispositivo pode escolher e acessar as lacunas espectrais de maneira a maximizar as QoS de suas aplicações.

As RRC possuem dois tipos de arquiteturas: centralizada ou descentralizada, explicadas a seguir.

- Centralizada

Uma arquitetura centralizada é composta por uma estação base e US. A estação base gerencia os dispositivos da rede e o uso das lacunas espectrais. Os US que possuem a capacidade de sensoriamento do espectro, monitoram o meio com o objetivo de coletar informações. Estas informações são enviadas à estação base com a finalidade de determinar as ações a tomar.

- Descentralizada

Uma arquitetura descentralizada é composta somente por US. Consequentemente, cada dispositivo é responsável pelo seu próprio gerenciamento na rede e pelas decisões de utilização das lacunas espectrais. Uma arquitetura descentralizada forma uma RRC *ad-hoc* (AKYILDIZ, 2008) (CHEN, 2008a).

Em um arquitetura descentralizada, devido à existência de vários US querendo acessar o espectro ao mesmo tempo de forma autônoma, deve ser utilizado um algoritmo que coordene o compartilhamento do espectro para evitar colisões entre os US ou entre os US e o UP. Alguns algoritmos de compartilhamentos de espectro são apresentados em (NIYATO, 2018) (DUBEY, 2010). A FIG. 2.2 ilustra os componentes e os tipos de arquitetura de uma RRC.

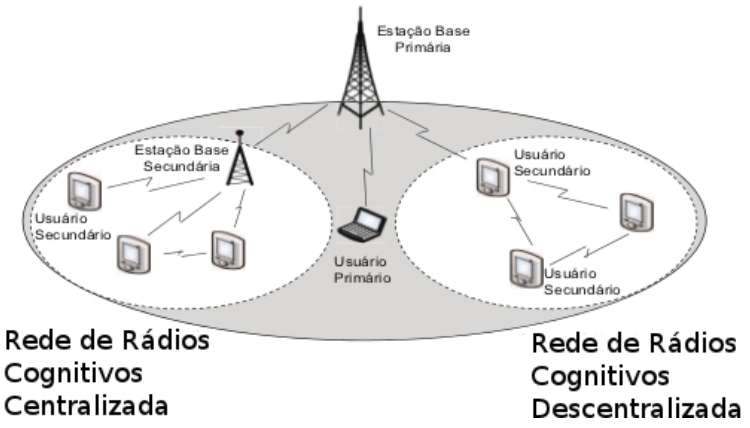

FIG. 2.2: Rede de Rádios Cognitivos. Adaptado de (SOTO, 2012)

2.3 APLICAÇÕES DE REDES DE RÁDIOS COGNITIVOS

Uma RRC pode possuir aplicações civis e militares, conforme descritas, respectivamente, nas seções 2.3.1 e 2.3.2.

2.3.1 APLICAÇÕES CIVIS DE REDES DE RÁDIOS COGNITIVOS

Aplicações civis de RRC incluem, entre outros cenários, faixas de frequência alugadas e redes de emergência (DOYLE, 2009), descritos nos parágrafos seguintes.

- Faixas de Frequência Alugada

Em um cenário de faixas de frequência alugada, a administração de uma rede primária pode permitir, via aluguel ou outra forma de concessão, que uma RRC utilize sua faixa de frequência licenciada com a condição que esta não interfira na utilização normal do UP. Por exemplo: uma rede de telefonia móvel pode permitir a utilização de um ou mais de seus canais de forma oportunista. Este tipo de utilização pode ser interessante visto que em certos períodos, madrugadas, por exemplo, a maioria dos canais está livre. No entanto, este tipo de utilização precisa ainda ser regulamentado na maioria dos países (DOYLE, 2009).

- Redes de Emergências

Em casos de emergências, como desastres naturais e catástrofes, as infraestruturas de comunicações tradicionais podem se encontrar total ou parcialmente destruídas. Por

sua capacidade de reconfiguração, um RC pode utilizar facilmente as várias partes das redes de comunicações existentes e formar uma única rede de comunicação. Por exemplo, uma RRC pode utilizar parte de uma rede de telefonia móvel e parte de uma rede de transmissão de TV e formar uma única RRC operativa.

2.3.2 APLICAÇÃO DE REDE DE RÁDIOS COGNITIVOS EM REDES MILITARES

Aplicações militares, tais como sistemas logísticos, de comunicações, acionamento de armas, navegação, geolocalização, radares e redes de sensores são grandes utilizadoras do espectro e de diferentes tipos de sistemas sem-fio (DOYLE, 2009). Estas aplicações necessitam de acesso eficiente e seguro ao espectro.

Segundo (SALLES, 2008), de maneira geral, os sistemas de enlace mais utilizados em redes militares são os sistemas rádio e o cabeado. Em especial, o sistema rádio deve ser utilizado de forma restrita, dada a vulnerabilidade a ações de guerra eletrônica; contudo, dada sua flexibilidade e rapidez de desdobramento, pode se constituir na base do SISTAC do Exército Brasileiro.

Num cenário militar, tipicamente, há um grande número de dispositivos e sistemas de comunicações heterogêneos que precisam ser interconectados (DOYLE, 2009). Por exemplo: diferentes sistemas táticos (manobra, guerra eletrônica, defesa anti-aérea, etc) de uma mesma força militar, diferentes forças armadas de um país ou mesmo de diferentes países em uma aliança internacional. Pode haver operações em terra, mar e ar. Ainda pode ocorrer uma mistura de redes centralizadas e descentralizadas. Muitos deste sistemas precisam ser instalados rapidamente em locais desconhecidos e muitas vezes hostis. Pode haver conexões cujo emprego seja de duração curta, por exemplo, conexões entre aeronaves, ou de longa, como sistemas de comunicações entre os presidentes dos países de uma aliança multinacional e o general comandante da operação militar.

Em casos onde sistemas legados não-cognitivos existem, as RRC podem evitar problemas escolhendo faixas de frequência que não estão sendo utilizadas pelos sistemas legados.

Ainda segundo (SALLES, 2008), três requisitos são estritamente relacionados e constituem um forte compromisso em sistemas de comunicação militares: alcance, capacidade e mobilidade. O forte relacionamento existente se dá, em geral, pelo fato que ao variar um dos fatores os outros dois também variam. A FIG. 2.3 exemplifica tal situação.

O triângulo de compensação se constitui em uma forma rápida e simples de avaliação da pertinência de uma determinada tecnologia de comunicação quanto ao emprego em uma

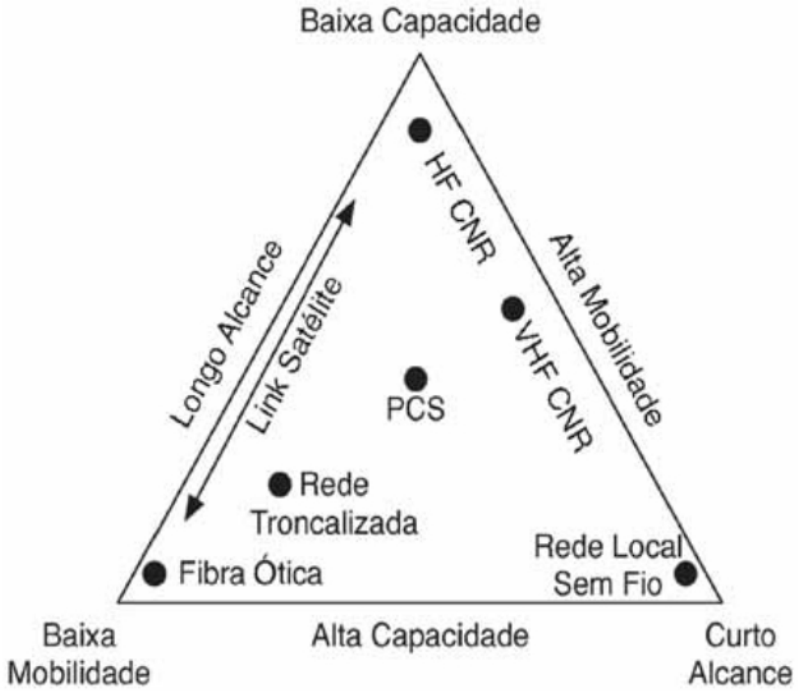

FIG. 2.3: Alcance x Capacidade x Mobilidade (SALLES, 2008)

operação militar. Por exemplo, as HF/CNR (*High Frequency/Communications Network Radios* ou redes de comunicações rádio de alta frequência) possuem baixa capacidade, entretanto, possuem longo alcance e alta mobilidade. Por outro lado, os PCS (*Personal Communications System* ou sistemas de comunicações pessoal) possuem capacidade, mobilidade e alcance médios.

Assim, as RRC figuram como uma solução promissora em redes militares, pois, devido a sua capacidade de alterar seus parâmetros de transmissão com base na interação com o seu ambiente, tal solução aumenta a flexibilidade, a rapidez de desdobramento e a possibilidade de interoperabilidade entre redes heterogêneas, possibilitando maiores alcance, capacidade e mobilidade.

A coexistência e a interoperabilidade de redes também é de vital importância no caso de alianças. Como um RC pode receber um sinal no padrão de uma *rede A* e necessitar transformá-lo no padrão de uma *rede B* para reencaminhamento, tem-se que, neste cenário, uma RC pode funcionar como *ponte*, permitindo uma rápida integração entre forças distintas em coalizão.

Posto que, em operações militares, todos os cenários descritos acima funcionam em

ambientes hostis, sujeitos à ação de tropas inimigas, consequentemente as medidas de segurança devem ser reforçadas, pois ataques como o de interferência, a EUP e a FDES podem diminuir ou mesmo anular a probabilidade de transmissão, comprometer a vazão da rede ou ainda aumentar a interferência ao UP a níveis maiores que o acordado, prejudicando assim o desempenho da rede.

2.4 SEGURANÇA EM REDES DE RÁDIOS COGNITIVOS

Com o objetivo de utilizar o espectro eficientemente, várias algoritmos de gerenciamento do espectro tem sido propostos na literatura, tais como o compartilhamento do espectro com base no preço (HALLDORSON, 2004) (WANG, 2010), no qual os UP alugam as bandas do espectro disponíveis aos US, e o compartilhamento do uso oportunista do espectro (XING, 2006) (WANG, 2009), com base no monitoramento e modelagem estocástica sobre o acesso do UP.

Embora essas abordagens propostas tenham se mostrado capazes de melhorar a utilização do espectro, elas tem por base a suposição de que usuários têm por objetivo principal a maximização de sua utilização espectral, e não a minimização da ocupação espectral dos demais usuários.

No entanto, em paralelo ao desenvolvimento da tecnologia RC, surgem os problemas de segurança em RRC (CAMILO, 2012a). Usuários maliciosos podem lançar vários tipos de ataques em uma RRC. O primeiro exemplo é a EUP (CHEN, 2008b), onde atacantes cognitivos imitam o sinal do UP para impedir que outros US acessem o espectro licenciado. Além daquele, há a FDES (CHEN, 2008a), na qual atacantes, em uma RRC com sensoriamento do espectro cooperativo, enviam dados falsos sobre o espectro, resultando em detecções incorretas pelos US. Outro exemplo é o ataque de interferência, um tipo de ataque DoS, que tem por objetivo impossibilitar ou prejudicar o funcionamento da comunicação nas camadas física e de enlace de dados de uma rede sem fio por meio da irradiação, ao longo do tempo, de altos níveis de energia, com ou sem transmissão de dados, em uma faixa de frequência alocada aos usuários sob ataque.

Assim, quando os US estão em um ambiente hostil, onde existem usuários maliciosos, cujo objetivo é causar danos aos demais usuários, com a diminuição ou o impedimento da utilização do espectro, as abordagens mencionadas podem acarretar em problemas de desempenho e/ou segurança. Assim, manter, ao mesmo tempo, o desempenho e a segurança na utilização do espectro é de importância crítica para a implantação da tecnologia

de RC em ambientes militares.

Como descrito anteriormente, RRC 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 (ANAND, 2008). Tais redes, são mais flexíveis e expostas em comparação com outras redes de rádio tradicionais. Assim, existem mais ameaças à segurança em RRC que a outros ambientes rádio tradicionais, pois as características únicas do RRC tornam os aspectos de segurança mais desafiadores.

Esta dissertação tem por objetivo estudar e propor mecanismos de segurança em, objetivando mitigar ou atenuar os efeitos de ataques de interferência e de emulação de usuário primário. Os mecanismos propostos podem ser utilizados por projetistas e desenvolvedores da tecnologia de RC para mitigar ou atenuar os efeitos dos ataques mencionados, sofridos pelas arquiteturas de RC disponibilizados para utilização.

2.4.1 MOTIVAÇÕES PARA ATAQUES EM REDES DE RÁDIOS COGNITIVOS

As motivações para ataques em RRC são discutidas em (CHEN, 2008c). Neste trabalho, os autores classificam as motivações em dois tipos: egoístas e maliciosas, descritas a seguir.

- Motivações Egoístas

Um ataque egoísta ocorre quando atacantes desejam aumentar sua capacidade de utilização do espectro e, consequentemente, impedem que outros usuários utilizem este recurso.

Um exemplo ocorre quando o atacante engana os US legítimos fazendo-os acreditarem que o UP está transmitindo naquele momento. Em consequência, os US legítimos não podem ocupar o espectro enquanto os atacantes desejarem. Uma RRC é vulnerável a ataques egoístas quando US atacantes aumentam a sua probabilidade de utilizar o espectro alterando os parâmetros de transmissão. Como os atacantes não obedecem as regras de compartilhamento do espectro, eles aumentam seu desempenho e degradam o desempenho dos US legítimos.

Um outro exemplo ocorre quando, visando somente aumentar seu desempenho, um dispositivo aumenta sua potência na intenção de aumentar sua RSR. No entanto, ao aumentar sua RSR, ele diminui esta relação para os demais dispositivos da rede, o que diminui o desempenho destes últimos (MACKENZIE, 2006).

- Motivações Maliciosas

Ataque malicioso ocorre quando os atacantes intencionalmente impedem que outros US utilizem o espectro. Como consequência, um ataque malicioso pode degradar drasticamente o desempenho da rede.

Por exemplo: em um campo de batalha por motivos estratégicos, o comando de um exército pode executar um ataque de interferência nas faixas de frequência do exército inimigo para tentar degradar ou anular a capacidade de comunicação da tropa inimiga, impedindo assim que este coordene suas operações, o que diminui o seu poder de combate.

Tais tipos de usuários estão presentes nos ataques de interferência e de emulação de usuário primário, objetos desta dissertação.

2.4.2 ATAQUES EM REDES DE RÁDIOS COGNITIVOS

Há vários ataques em RRC. Entre estes incluem o ataque de interferência, emulação de usuário primário, falsificação de dados do espectro monitorado, de função objetivo, de canal de controle comum, de injeção de pacotes e de falso feedback, descritos em (PARVIN, 2012). Descrevemos a seguir os ataques de interferência e de emulação de usuário primário, objetos deste trabalho.

- Ataque de Interferência

O ataque de interferência, um tipo de ataque DoS, tem por objetivo impossibilitar ou prejudicar o funcionamento da comunicação nas camadas física e de enlace de dados de uma rede sem fio. Um atacante pode impedir que usuários legítimos utilizem as faixas de frequência para as quais estão habilitados, por meio da irradiação, ao longo do tempo, de altos níveis de energia, com ou sem transmissão de dados, em uma faixa de frequência alocada aos usuários sob ataque. O atacante, dada a possibilidade de também dispor da tecnologia RC, pode adotar ações diferentes em cada intervalo de tempo (WANG, 2011), por exemplo, interferir em canais diversos utilizando potências diferentes.

A escolha do ataque de interferência como objeto deste trabalho se deve ao fato de que este ataque é o mais tradicional em comunicações militares. Encontramos relatos deste ataque em (BROWN, 1999), onde o autor cita que, na segunda guerra mundial, os alemães possuíam um detalhado plano para causar interferência nos radares britânicos, e em (WERRELL, 1992), onde é citada a preocupação dos americano com a defesa anti-interferência na guerra do Vietnã.

- Ataque de Emulação de Usuário Primário

Um ataque EUP é gerado por um US atacante, egoísta ou malicioso, que emula o comportamento e as características do sinal do UP com o objetivo de ganhar prioridade no uso do espectro, impedindo, assim que os US legítimos acessem o espectro. Por possuir capacidade cognitiva, o atacante pode alterar, por exemplo, sua potência de transmissão, estratégia de modulação, frequência utilizada, largura de banda e/ou taxa de transmissão para passar-se por um UP, tornando este tipo de ataque de grande dificuldade de detecção.

A defesa em face de um ataque de EUP gera dois desafios: a detecção deste ataque e sua mitigação.

A literatura propõe contra-medidas frente ao ataque EUP utilizando as abordagens centralizada não-cooperativa, centralizada cooperativa, descentralizada não-cooperativa e descentralizada cooperativa, explicadas a seguir.

- Centralizada Não-Cooperativa

Os trabalhos indicam a primazia da abordagem centralizada não-cooperativa. Neste tipo de abordagem, a estação base realiza sozinha a detecção do ataque EUP. Esta abordagem gera uma alta latência. Além disso, esta abordagem também gera um ponto único de falha na estação base, ou seja, caso a estação base não consiga detectar o ataque EUP, todo a rede ficará vulnerável (JIN, 2009a) (CHEN, 2006) (CHEN, 2008d) (LI, 2010) (CHEN, 2011b).

- Centralizada Cooperativa

Devido aos problemas de latência da abordagem centralizada não-cooperativa, surgiu a abordagem centralizada cooperativa, na qual a estação base recebe dados oriundos dos demais dispositivos da rede para efetuar a detecção do ataque de EUP. Esta abordagem diminui a latência de decisão, pois o trabalho de detecção é compartilhado pelos vários dispositivos da rede. No entanto, persisti a existência do ponto único de falha na estação base (JIN, 2010) (CHEN, 2011a) (MIN, 2011).

- Descentralizada Não-Cooperativa

Então foi proposta a abordagem descentralizada não-cooperativas. Nesta abordagem, cada dispositivo realiza individualmente a detecção do ataque de EUP. Estas apresentam um maior desempenho podendo neutralizar as dificuldades das soluções que seguem uma abordagem centralizada; entretanto, tal artifício pode gerar detecções erradas tanto de canais atacados quanto de canais não atacados (ANAND, 2008) (JIN, 2009b).

- Descentralizada Cooperativa

Por fim, visando diminuir as detecções erradas tanto de canais atacados quanto de canais não atacados, foi proposta a abordagem descentralizada cooperativa, na qual cada dispositivo realiza individualmente a detecção do ataque de EUP utilizando, além dos dados obtidos por ele, também dados oriundos dos demais dispositivos da rede (SOTO, 2012).

Outro aspecto a ser abordado na detecção de ataque de EUP é quanto ao número de critérios que é utilizado nas técnicas de detecção. Estas podem ser mono-critério ou multi-critério, explicadas a seguir.

- Técnica Mono-Critério

A maioria dos trabalhos encontrados na literatura apresenta uma análise de um único critério, ou seja, realizam a detecção do ataque de EUP analisando uma única característica do sinal emitido pelo atacante. Exemplos de características que podem ser utilizadas são a potência do sinal, a taxa de utilização do espectro do UP e características periódicas do sinal do UP.

A utilização de um único critério pode levar a uma identificação errônea do ataque, pois o atacante não é detectado quando somente imita a característica do sinal do UP que está sendo analisada.

- Técnica Multi-critério

Esta técnica realiza a detecção do ataque de EUP analisando mais de uma característica do sinal emitido pelo atacante. A utilização de múltiplos critérios aumenta a detecção de ataque de EUP, pois o ataque é bem sucedido somente se o atacante imitar todas as características do sinal do UP analisadas.

A escolha do ataque de emulação de usuário primário como objeto deste trabalho se deve ao fato deste ataque comprometer severamente o aproveitamento das lacunas espectrais, comprometendo o desempenho da rede.

2.5 TRABALHOS RELACIONADOS

Nesta seção, citamos alguns trabalhos relacionados aos ataques de interferência e emulação de usuário primário estudados durante a realização desta dissertação.

2.5.1 ATAQUE DE INTERFERÊNCIA

Vários trabalhos estudam o ataque de interferência bem como medidas anti-interferência em RRC. Destacamos alguns nos próximos parágrafos.

(SU, 2011) propõe uma estratégia que permite que o transmissor e o receptor saltem para um mesmo conjunto de canais com alta probabilidade. As simulações feitas mostram que a estratégia proposta é resistente aos ataques de interferência diferentes, e que os US transmissor e o receptor podem desenvolver o conhecimento comum sobre a disponibilidade de canal através da aprendizagem.

(SODAGARI, 2011) aborda uma estratégia anti-interferência de acesso ao canal em uma RRC quando alguns canais ociosos do UP estão sendo interferidos em cada intervalo de tempo. Dado que o US não sabe quais bandas ociosas estão sob ataque, no método proposto pelo autor o US tenta escolher o melhor canal possível em cada intervalo de tempo para evitar a interferência. Simulações mostram que os canais escolhidos utilizando o método proposto tiveram uma RSR 50% maior que os escolhidos aleatoriamente.

(LI, 2011) estuda tanto a capacidade de interferência dos atacantes cognitivos como a capacidade de defesa anti-interferência das RRC. São analisadas várias estratégias de ataque de interferência onde os atacantes utilizam grande potência de transmissão com o objetivo de interferir em vários períodos de tempo. As médias da vazão e da probabilidade de interferência são derivadas e verificadas por simulações.

Em (WANG, 2011) o sistema anti-interferência é modelado de acordo com um jogo estocástico e é proposto um mecanismo de defesa, considerando como restrições do modelo que os US sempre possuem dados para transmitir, bem como restrições de energia. Devido a estas considerações, o objetivo dos US é maximizar sua vazão *spectrum-efficient*, definida como a razão entre o vazão esperada e o número total de canais usados para a transmissão de dados e de mensagens de controle. Utilizando a metodologia de aprendizagem *reinforcement learning*, o US pode gradualmente aprender a estratégia de ocupação espectral mais adequada considerando as restrições descritas pelo autor.

2.5.2 EMULAÇÃO DE USUÁRIO PRIMÁRIO

Vários trabalhos estudam o ataque de EUP bem como medidas para detecção e mitigação deste ataque em RRC. Destacamos alguns nos próximos parágrafos.

Os autores de (CHEN, 2008d) mostram que um ataque EUP podem interferir severa-

mente no monitoramento do espectro, reduzindo significantemente o espectro disponível aos US legítimos. Para mitigar este ataque, é mostrado um framework de detecção de ataques EUA chamado Procedimento de Verificação de Transmissão. Este procedimento utiliza as informações da localização e da potência do sinal dos UP. Mostrou-se eficiente no cenário definido com UP fixos e com potência de transmissão constantes.

(LI, 2010) Estuda o ataque de EUP em uma rede multicanal. No procedimento proposto, chamado, *blind dogfight*, o US escolhe aleatoriamente um canal para monitorar e transmitir, com o objetivo de evitar o ataque de EUP estatisticamente. Mostrou-se eficiente na utilização em um único canal.

(SOTO, 2012) apresenta a estratégia INCA (múltiplos critérios para aNálise Cooperativa da presença de Ataques), uma proposta de abordagem descentralizada cooperativa que utiliza multi-critérios para detecção de ataques EUP. Esta estratégia é composta de duas fase. Na primeira, denominada fase individual, é realizado um sensoriamento do espectro com o objetivo de coletar dados. Estes dados formam um conjunto de valores para cada critério estabelecido pela estratégia INCA. A segunda fase consiste na troca de informações entre vizinhos, seguida da análise, através do teorema de Bayes, das informações trocadas. O autor implementou o INCA no simulador NS (Network Simulator ou simulador de rede) e o avaliou. Os resultados obtidos mostraram que a estratégia apresenta uma superioridade de até 25% comparado com um esquema mono-critério 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.

(CHEN, 2009) Caracteriza um ataque de EUP bem como uma defesa contra este ataque. O autor mostra que tanto o atacante quanto o defensor são inteligentes para obter as informações do ambiente por meio de estimativas e de aprendizagem e, assim, projetar melhores estratégias de adaptação em virtude de alterações no ambiente rádio. A estratégia de defesa baseia-se na invariância dos canais de comunicação para eficazmente neutralizar o ataque.

2.6 RESUMO

RC traz muitos desafios, tais como preocupações com a regulamentação, adaptação de protocolos existentes, desenvolvimento de tecnologia para ambiente de acesso não estático ao especto e mecanismos de segurança, explicados nos parágrafos seguintes.

- Adaptação dos Protocolos Existentes

Os protocolos atuais foram desenvolvidos com base na filosofia de parâmetros de transmissão e recepção (quase) fixos. Faz-se necessário a adaptação dos protocolos atuais para a realidade de RC.

- Tecnologia para Acesso ao Espectro não Estático

O balanceamento entre a proteção do UP contra a interferência dos US e o uso eficiente da faixa de frequência legada torna-se um fator crítico para o sucesso das RRC, consequentemente, a tecnologia para ambiente de acesso não estático, principalmente no sensoriamento do espectro, torna-se de fundamental importância.

- Mecanismos de Segurança

Devido às interações e à colaboração numa RRC, a segurança passa a ser um aspecto de fundamental importância. Nesta rede, os dispositivos são inteligentes e tem a habilidade de observar, aprender e agir de maneira a otimizar sua performance (LIU, 2011). Considerando que estes dispositivos podem pertencer a administrações diferentes e com interesses conflitantes, a política de cooperação pode não funcionar de maneira adequada, sejam por motivos intencionais ou não. Consequentemente, mecanismos de segurança eficientes e confiáveis precisam ser desenvolvidos.

Apesar de todos os desafios técnicos ainda existentes da tecnologia de RC, seu maior desafio consiste em definir o modelo de operação da tecnologia. Em outras palavras, além da premissa de uso de RRC, resta em aberto a definição da política regulatória para sua operação.

No entanto, RC podem proporcionar para as comunicações do futuro um melhor desempenho do enlace, pois um RC procura sair de canais instáveis e com interferência alterando sua transmissão para canais com maior estabilidade e menor interferência, o que aumenta vazão da rede (REED, 2005). RC também proporciona uma melhor utilização do espectro, pois preenche faixas do espectro inutilizadas e sai das muito utilizadas. Além disso, RC possui maior imunidade a Guerra Eletrônica, possibilitando comunicações com mais segurança.

RRC, além de realizar um melhor aproveitamento das frequências ociosas do espectro, também beneficiam diretamente os usuários finais. Como as RRC utilizam melhor o

espectro, podem prover melhores requisitos de QoS, menores tempos de resposta, maior cobertura, entre outras vantagens (ISHIBASHI, 2008).

Resumindo, segundo (DOYLE, 2009), RC nos permite fazer melhor o que fazemos com os rádios tradicionais e nos possibilita implementar funcionalidades que não conseguimos com a tecnologia de rádios atual. RC traz aos sistemas de comunicação a possibilidade de operarem em circunstâncias muito mais desafiadoras e sobrecarregadas.

No próximo capítulo, utilizaremos os conceitos aqui estudados para apresentarmos a metodologia utilizada na arquitetura para RC com segurança espectral e nos mecanismos propostos nesta dissertação.

3 METODOLOGIA UTILIZADA

Neste capítulo, descrevemos a metodologia utilizada. Iniciamos com a descrição do sistema de referência. Depois, enumeramos os indicadores de desempenho em RRC e propomos a arquitetura para RC que contempla segurança espectral. Por fim, descrevemos e analisamos o desempenho dos mecanismos anti-interferência e anti-EUP propostos e de algumas estratégias de mitigação de ataques de interferência e emulação de usuário primário.

3.1 MOTIVAÇÃO PARA MECANISMOS DE SEGURANÇA EM REDES DE RÁDIOS COGNITIVOS

Os mecanismos estudados para defesa anti-interferência e anti PUEA são validados considerando os mecanismos isolados das fases do ciclo cognitivo, em lugar de uma abordagem integrada. Com o desenvolvimento de mecanismos de defesa em RRC, surge a necessidade de arquiteturas validadas e integradas para RC que contemplem mecanismos de segurança.

O ciclo cognitivo proposto por (AKYILDIZ, 2006) limita as mudanças dos parâmetros de transmissão (faixa de frequência, potência de transmissão, estratégia de modulação, etc.) apenas em face de mudanças no ambiente rádio. Entretanto, conforme é citado em (DOYLE, 2009), um RC precisa alterar seus parâmetros de transmissão em virtude de mudanças em 4 conjuntos de parâmetros de entrada: informações do ambiente radio no qual está inserido, requisitos de QoS da aplicação, recursos disponíveis para o dispositivo e política de utilização do espectro, com o objetivo de maximizar os requisitos de QoS da aplicação.

Os trabalhos de (AKYILDIZ, 2006) e (DOYLE, 2009) são baseados na suposição de que todos os RC têm por objetivo apenas a maximização de sua utilização espectral. No entanto, em um ambiente hostil, onde existem RC maliciosos cujo objetivo é causar danos aos demais, como a diminuição ou o impedimento de suas transmissões e/ou recepções, as abordagens mencionadas podem acarretar na utilização ineficiente do espectro. Dado que o aumento da eficiência na utilização do espectro é uma das principais propostas da tecnologia de RC, mitigar os efeitos dos ataques destes usuários maliciosos é de importância

crítica para a implantação desta tecnologia.

3.2 DESCRIÇÃO DO SISTEMA DE REFERÊNCIA

Consideramos que há uma estação base secundária na RRC que coordena a utilização do espectro por todos os US legítimos. Portanto, todos os US legítimos são considerados uma única entidade denominada US legítimo. Assumimos que a RRC modelada é um sistema com acesso por divisão de tempo, ou seja, o tempo é dividido em intervalos discretos (*slots*), T_f. As transmissões dos UP sempre começam no início de cada intervalo.

Consideramos uma rede com acesso oportunista ao espectro, onde o US pode ocupar o espectro que pertence a vários UP quando os últimos não o estiverem utilizando. Consequentemente, as faixas de frequência não utilizadas podem ser selecionadas, compartilhadas com outros usuários e exploradas sem interferências para os UP. Como consequência deste mecanismo e da atividade dos UP, a disponibilidade do espectro, ou seja, o número de canais disponíveis para transmissão, N_c, varia em função do tempo.

Como utilizam a tecnologia de RC, tanto os US legítimos quanto os US atacantes podem identificar as lacunas espectrais que não estão sendo usadas em um momento ou canal específicos.

3.2.1 DESVANECIMENTO DO CANAL

Consideramos que tanto os UP quanto os US estão conectados através de canais rádios sujeitos a desvanecimento, fenômeno causado pela propagação em várias direções das ondas de rádio entre um transmissor e um receptor. Esta propagação pode levar a flutuações de amplitude, de fase e de ângulo do sinal recebido (SKLAR, 1997).

A principal característica de um canal com desvanecimento é que este é um processo aleatório e correlacionado ao longo do tempo, ou seja, o canal de comunicação é um sistema dinâmico com o ganho do desvanecimento sendo um processo aleatório que varia ao longo do tempo de uma maneira correlata (SADEGHI, 2008).

Definimos a capacidade do canal como a quantidade de bits que podem ser transmitidos, em um dado intervalo de tempo t. Este valor é diretamente proporcional a largura de banda do canal e muda em função do tempo devido à estratégia de modulação mais adequada em face da RSR. Considerando um canal com largura de banda de b MHz, utilizamos a metodologia citada em (MOURA, 2011), resumida a seguir:

Consideramos K estratégias de modulação. Dividimos o intervalo de valores da RSR do canal, γ, em $K+1$ regiões mutuamente exclusivas:

$[v_0 = 0, v_1), [v_1, v_2), ..., [v_{K-1}, v_K), [v_K, v_{K+1} = \infty)$,

sendo $0 < v_1 < v_2 < ... < v_{K-1} < v_K$.

Caso a RSR esteja no intervalo $[v_0 = 0, v_1)$, o US opta por não transmitir. Logo, a qualidade do canal neste caso é igual a 0. É utilizada a estratégia de modulação m, $m \in \{1, 2, ..., K\}$, se o valor da RSR do canal neste período de tempo estiver na região $[v_m, v_{m+1})$. Considerando que a estratégia de modulação m possibilita a transmissão de m bits por símbolo, temos $K+1$ qualidades do canal, $0, b, 2b, ..., Kb$.

Dado o canal com desvanecimento plano e lento e baixa mobilidade dos transmissores e receptores, cenário típico de operações militares que utilizam as redes táticas em VHF do comando de brigada com os comandos de batalhões, conforme mencionado em (MOURA, 2011), empregamos o modelo de Rayleigh para representação do canal de comunicações.

Assim, segundo (SKLAR, 1997), dada uma RSR média do canal, $\overline{\gamma}$, o valor da RSR do canal, γ, tem uma probabilidade regida pela função de densidade de probabilidade:

$$f_A(\gamma) = \frac{\gamma}{\overline{\gamma}^2} exp\left(\frac{\gamma^2}{2\overline{\gamma}^2}\right), \gamma \in [0, \infty) \tag{3.1}$$

Consequentemente, a probabilidade, p_m, de a RSR, γ estar no intervalo $[v_m, v_{m+1})$ é dada por:

$$p_m = \int_{v_m}^{v_{m+1}} \frac{\gamma}{\overline{\gamma}^2} exp\left(\frac{\gamma^2}{2\overline{\gamma}^2}\right) d\gamma \tag{3.2}$$

Consideramos que cada estratégia de modulação m possui uma probabilidade alvo de erro de transmissão constante, p_e, a fim de atender aos requisitos de QoS.

3.2.2 INDICADORES DE DESEMPENHO EM REDES DE RÁDIOS COGNITIVOS MILITARES

Aplicações como acesso à web, transferência de arquivos, áudio, vídeo por demanda e videoconferência tem como principal requisito de QoS a vazão. Como as aplicações citadas figuram entre as mais comumente usadas em sistemas militares, como o SISTAC do Exército Brasileiro, no qual (SALLES, 2008) cita que o tráfego de uma rede de uma divisão de exército é de 2 Mbps e de um corpo de exército é de 8 Mbps, consideramos que um dos objetivos principais de uma RRC é maximizar sua vazão média.

Definimos a vazão média, $\overline{v_r}$, da RRC, como o somatório das vazões médias definidas nas QoS das aplicações que utilizam a infra-estrutura da rede em questão, ou seja, $\overline{v_r} = \sum_{i=1}^{n} \overline{v_i}$, na qual n é o número de aplicações que utilizam a infra-estrutura da rede e $\overline{v_i}$ é a vazão média da aplicação i.

Definimos a taxa de utilização do UP, t_u, em um dado canal, como a razão entre o número de períodos de tempo que o UP utiliza para transmitir e o número total de períodos de tempo considerados.

Definimos ainda a taxa de interferência ao UP, i_p, como a razão entre o tempo de transmissões simultâneas entre o UP e o US e o tempo total de transmissões do UP. Esta métrica é de fundamental importância, pois o objetivo de maximizar a vazão média da rede deve ser atingido sem causar uma taxa de interferência ao UP maior que a taxa de interferência máxima, i_{max}, especificada em contrato entre o UP, o US e a agência reguladora do uso do espectro, em um cenário civil, ou na ordem de operação do comandante, em um cenário militar. O objetivo de uma RRC pode ser resumido no seguinte problema de otimização com restrição: $max\ \overline{v_r}$, sujeito a: $i_p \leq i_{max}$.

3.3 ARQUITETURA DE RÁDIO COGNITIVO PROPOSTA

Este seção, com base em (CAMILO, 2012b), propõe, formaliza e avalia uma arquitetura para rádios cognitivos que contempla a segurança espectral. Assim, mecanismos de defesa podem ser validados. Como proposta, a arquitetura CMPS, mostrado na FIG. 3.1, apresenta o componente de Segurança Espectral como aprimoramento do ciclo cognitivo descrito em (AKYILDIZ, 2006) e considerando os quatro conjunto de informações de entrada principais listados por (DOYLE, 2009): informações do ambiente rádio, informações dos requisitos de QoS da aplicação, informações dos recursos disponíveis para o dispositivos e informações da política regulatório do uso do espectro.

O trabalho realizado em cada uma das fases é detalhado nos parágrafos seguintes.

3.3.1 SENSORIAMENTO DO ESPECTRO

Nesta fase, o RC monitora o espectro eletromagnético objetivando capturar as ondas de radiofrequência e produzir informações sobre as faixas de frequência, tais como o tipo de usuário (UP, US ou nenhum) que ocupa o espectro no momento e a RSR, que serão úteis na fase de Análise Espectral.

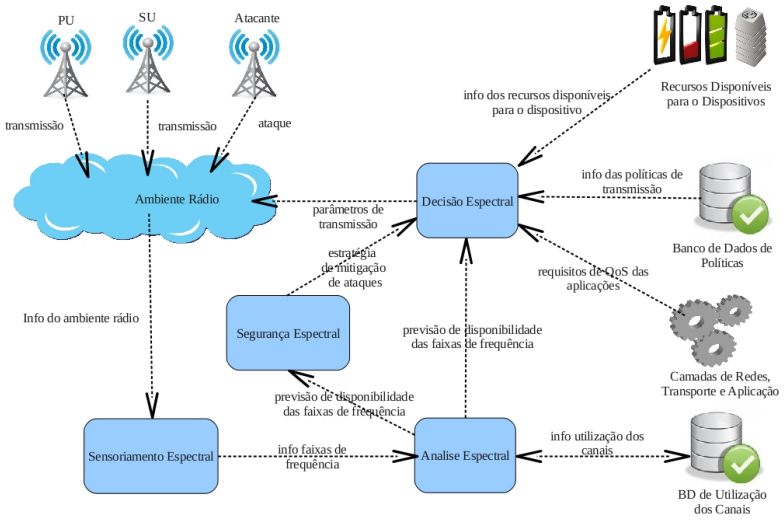

FIG. 3.1: Arquitetura CMPS para RC

A entrada desta fase é composta das ondas de radiofrequência do ambiente rádio monitorado e a saída é, por exemplo, uma lista de faixas de frequências contendo a relação de tipos de usuários responsáveis pela ocupação espectral e a RSR referente a cada faixa, conforme mostra o exemplo descrito na TAB. 3.1.

Canal	Faixa de Frequência (MHz)	Usuário	RSR (dB)
1	1820-1825	UP	10
2	1825-1830	Não utilizada	50
3	1830-1835	US	8

TAB. 3.1: Exemplo de Saída da Fase de Sensoriamento Espectral

No exemplo da TAB. 3.1, considera-se que o RC está monitorando apenas 3 faixas de frequência. No entanto, o RC pode monitorar tantas faixas de frequências quantas o seu hardware permitir. Tem-se também que estas são as informações de interesse do RC do exemplo. Caso outras informações sejam necessárias e possam ser detectadas do ambiente rádio, tais como a estratégia de modulação e a técnica de codificação empregadas, estas podem ser incluídas na saída desta fase.

As transmissões dos UP sempre começam no início de cada intervalo. Para evitar conflito ou interferência prejudicial aos UP, os US necessitam monitorar o espectro antes de cada tentativa de transmissão. Denominamos tempo de detecção do UP ao tempo

decorrido entre o início do intervalo de transmissão e a verificação da presença ou ausência do UP. O tempo de detecção do UP inclui, além do tempo gasto pelo algoritmo de sensoriamento do espectro, o tempo de recebimento e fusão das informações do espectro monitorado recebidas do outros US, no caso de monitoração cooperativo do espectro. Neste trabalho, consideramos que o tempo de detecção do UP é desprezível.

3.3.2 ANÁLISE ESPECTRAL

Esta fase recebe a lista de informações das faixas de frequência da fase de Sensoriamento Espectral e, utilizando um banco de dados de utilização das faixas de frequência, gera a lista de previsão de disponibilidade dos canais. A saída desta fase é, por exemplo, uma lista de informações das faixas de frequência acrescida da probabilidade de utilização de cada canal, conforme mostra o exemplo descrito na TAB. 3.2.

Canal	Faixa de Frequência (MHz)	Usuário	RSR (dB)	Utilização (%)
1	1820-1825	UP	10	10%
2	1825-1830	Não utilizada	50	90%
3	1830-1835	US	8	25%

TAB. 3.2: Exemplo de Saída da Fase de Análise Espectral

As considerações feitas em 3.3.1 sobre os dados da fase de Sensoriamento Espectral também se aplicam aos dados da TAB. 3.2 da fase de Análise Espectral.

3.3.3 SEGURANÇA ESPECTRAL

Esta fase executa os mecanismos de segurança em RC, os quais definem as ações para detectar, atenuar e/ou mitigar os efeitos de ataques em RRC.

Como ilustração de um mecanismo de segurança, considera-se um cenário no qual o RC esteja sobre um ataque de interferência. Dados uma quantidade de canais disponíveis para transmissão, a quantidade máxima de canais que o atacante pode interferir e o requisito de QoS da aplicação, há várias estratégias, representada pela quantidades de canais de controle e de dados, para minimizar os efeitos do ataque.

Por exemplo, considera-se um cenário em que o número de canais disponíveis para transmissão é igual a 8, todos com a mesma largura de banda, o número máximo de canais que o atacante pode interferir é igual a 4 e o principal requisito de QoS da aplicação é vazão. Tal cenário é adequado em casos em que o objetivo é transmitir o máximo de

dados por unidade de tempo, como ema uma transferência de vídeo. Nesta situação, uma estratégia "arrojada"é utilizar apenas 1 canal de controle e 7 de dados. Já uma estratégia mais "conservadora"é utilizar 2 canais de controle e 6 de dados.

Alterando-se o principal requisito de QoS da aplicação do cenário acima para confiabilidade, ou seja, quando o objetivo for obter sucesso na transmissão de um reduzido conjunto de dados no máximo de intervalos de tempo, como em uma aplicação de correio eletrônico, uma estratégia extremamente "conservadora"é utilizar 5 canais de controle e 3 de dados. Outra estratégia disponível é utilizar 4 canais de controle e 4 de dados.

3.3.4 DECISÃO ESPECTRAL

O RC, utilizando as informações das fases de Análise e de Segurança Espectral, dos requisitos de QoS da aplicação, dos recursos disponíveis para o dispositivo e da política regulatória de uso do espectro, determina a faixa de frequência e demais parâmetros a serem utilizados na transmissão. Também é coordenado o acesso com outros usuários e feita a desocupação do canal quando um usuário primário é detectado.

Como exemplo de procedimento desta fase temos que no cenário descrito na Seção 3.3.3 e considerando a inexistência de restrições de energia e vazão como requisito de QoS da aplicação e que o RC utilizará 2 canais de controle e 6 de dados. Se o RC adotar uma estratégia fixa, como os canais 1 e 2 para mensagens de controle e 3 a 8 para dados, o atacante, por possuir capacidade cognitiva, detecta tal padrão e utiliza uma estratégia de ataque mais eficiente, como atacar somente os dois canais de controle. Uma estratégia aleatória dos canais de controle e de dados dificulta a ação do atacante. Outro exemplo é a não utilização de um determinado canal mesmo estando disponível, em função de informações da política de utilização do espectro, indicando, por exemplo, que este canal não é seguro no momento.

Concluímos que, objetivando o estudo dos mecanismos de segurança para RRC de maneira integrada ao ciclo cognitivo e que seja sensível aos quatro tipos de informações listados por (DOYLE, 2009), há a necessidade de uma arquitetura para RC que contemple o componente de Segurança Espectral como aprimoramento do ciclo cognitivo descrito em (AKYILDIZ, 2006) e que considere os quatro conjunto de informações de entrada citados.

3.4 MECANISMOS DE SEGURANÇA EM REDES DE RÁDIOS COGNITIVOS

Os trabalhos relacionados em 2.5.1 possuem duas limitações principais: a insensibilidade dos modelos à diferença de requisitos de QoS e a adoção de um modelo com restrição de energia e que não contempla outras aplicações.

3.4.1 MODELAGEM DOS MECANISMOS

- US Legítimos

Conforme mencionados em 3.2, consideramos todos os US legítimos como uma única entidade denominada US legítimo.

- Atacantes

Considera-se também que os atacantes trabalham em conjunto para causar o maior dano possível aos US legítimos. Por exemplo: num cenário militar, o comandante de uma força armada coloca todos os rádios transmissores sob seu comando para executar de forma coordenada o ataque de interferência sobre o inimigo. Portanto, todos os atacantes são considerados uma única entidade denominada atacante.

Neste trabalho, assumimos que os sinais transmitidos pelos UP e US legítimo são distinguíveis. O atacante monitora tanto as transmissões dos UP quanto a do US legítimo. Assumimos também que o atacante não ataca quando os UP estão transmitindo.

- Estratégias de Atribuição de Canais

Se o US legítimo adotar um esquema fixo de escolha de canais de controle e de dados, um atacante cognitivo pode capturar tais padrões, distinguir entre os canais de controle e de dados, e atacar apenas os canais de controle ou os de dados, causando, assim, o maior dano possível.

Portanto, o US legítimo precisa realizar a mudança de canal para aliviar o dano potencial devido a uma estratégia fixa de atribuição de canais. Numa estratégia variável de atribuição de canais, os que são usados para transmissão de controle e dados em um intervalo de tempo podem não ser mais utilizados para a mesma finalidade no intervalo seguinte. Com a introdução de aleatoriedade em sua atribuição de canais, o padrão do US Legítimo torna-se mais imprevisível. Então, os atacantes também tem que estrategicamente mudar os canais que eles atacarão em cada intervalo de tempo. Portanto, uma

estratégia variável de atribuição de canal é mais resistente ao ataque de interferência que uma fixo.

3.4.2 ANÁLISE DE DESEMPENHO EM REDES DE RÁDIOS COGNITIVOS

No restante deste capítulo, fazemos uma análise do desempenho de uma RRC. Iniciamos com um sistema mono-canal sem ataques. Em seguida, analisaremos um sistema mono-canal em face de ataque de interferência. Depois, analisaremos um sistema multicanal em face de um ataque de interferência e descrevemos nosso mecanismo anti-interferência proposto. Em seguida, fazemos a análise de um sistema mono-canal em face de ataque de emulação de usuário primário. Depois, analisamos um sistema multicanal em face de um ataque de emulação de usuário primário e descrevemos nosso mecanismo anti-EUP proposto. Por fim, fazemos uma conclusão do capítulo.

3.4.3 SISTEMA MONO-CANAL SEM ATAQUES

Neste cenário, consideramos que as transmissões do UP podem ser previstas. Também é considerado que não há ataques a rede. Neste cenário, obtemos: $i_p = 0$ e

$$\overline{v_r} = F_c * \Sigma M \tag{3.3}$$

Na qual $F_c = (1 - t_u) * b$ e $\Sigma M = \sum_{m=1}^{K} (m * (1 - p_e) * p_m)$.

Como um dos objetivos principais de uma RRC é maximizar sua vazão média, concluímos, portanto, que três parâmetros devem ser considerados na utilização de uma rede de rádios cognitivos sobre uma rede primária: a largura de banda do canal, a relação sinal-ruído média e a taxa de utilização do UP.

3.4.4 SISTEMA MONO-CANAL COM ATAQUE DE INTERFERÊNCIA

Em uma RRC, atacantes podem lançar um ataque de interferência para evitar que a utilização oportunista do espectro seja eficiente. O efeito de um ataque de interferência em um canal de uma RRC é o mesmo que o verificado em redes não cognitivas, ou seja, a redução da RSR do canal sob ataque, o que pode obrigar o US legítimo a empregar uma estratégia de modulação que lhe possibilita transmitir menos dados por símbolo ou mesmo impossibilitar a transmissão, se a RSR for reduzida para um valor menor que o limite inferior da primeira estratégia de modulação.

Como a RSR média do canal será diminuída, as probabilidades de não transmissão, p_0, e de cada estratégia de modulação, p_m, $m \in \{1, 2, ..., K\}$ serão alteradas para p_{0a} e p_{ma}, $m \in \{1, 2, ..., K\}$, cujos valores podem ser calculados utilizando a Equação 3.2, considerando $\overline{\gamma}$ igual a nova RSR média em face do ataque de interferência. Portanto, a vazão da rede será igual a:

$$\overline{v_r} = F_c * \Sigma M_a \tag{3.4}$$

Na qual, $\Sigma M_a = \sum_{m=1}^{K}(m * (1 - p_e) * p_{ma})$. Portanto, a perda da vazão da rede será de:

$$\Delta\overline{v_r} = F_c * (\Sigma M - \Sigma M_a) \tag{3.5}$$

Considerando a utilização de um único canal, o objetivo é manter a RSR média da rede superior ao limite inferior da estratégia de modulação que proporciona maior taxa de transmissão para atenuar os efeitos do ataque. Para atingir este objetivo, uma estratégia é aumentar a potência de transmissão. No entanto, esta contra-medida nem sempre é possível, pois ocasiona o aumento do consumo de energia pelo dispositivo e facilita sua detecção pelos elementos de guerra eletrônica. Outra medida de defesa anti-interferência em um único canal é a utilização de antenas direcionais (NOUBIR, 2004).

3.4.5 SISTEMA MULTICANAL COM ATAQUE DE INTERFERÊNCIA

Neste cenário, para coordenar o acesso e obter uma utilização eficiente do espectro, mensagens de controle precisam ser trocadas entre a estação base secundária e o US Legítimo por meio de canais de controle dedicados. Canais de controle servem como um meio para suportar alto nível de funcionalidade da rede, tais como o controle de acesso, atribuição e mudança de canal e, de relevante para nossa análise, a confirmação de recebimento de dados (LIU, 2011). Portanto, se as mensagens de controle não são recebidas corretamente pelo US legítimo, ele não recebe as confirmações das transmissões dos dados e promove a retransmissão dos mesmos, degradando o desempenho da rede.

Como a funcionalidade da rede depende da recepção correta de mensagens de controle, é mais confiável transmitir as mesmas mensagens de controle em múltiplos canais, técnica conhecida como MIMO (TORLAK, 2012). No entanto, se o US legítimo reserva muitos

canais de controle, o número de canais de dados é pequeno, e a transmissão de dados possível através da utilização do espectro é desnecessariamente baixa. Portanto, uma boa seleção de canais deve ser capaz de equilibrar o risco de não ter as mensagens de controle recebidas com a quantidade de dados que pode ser transmitida. Se a quantidade de dados que o US legítimo possui para transmitir for menor que a que pode ser transmitida em um único canal de dados, ele pode também utilizar a técnica de transmitir os mesmos dados em todos os canais de dados, visando uma maior garantia da entrega.

Consideramos que o número de canais disponíveis para transmissão, todos com a mesma largura de banda, é N_c. Este valor pode variar em cada intervalo de tempo. Consideramos também que o atacante pode interferir em, no máximo, M canais, devido à limitação de seu hardware como, por exemplo, o número de antenas. Assumimos que $M < N_c - 1$, pois, caso contrário, o US legítimo não poderia transmitir devido ao fato de precisar de, pelo menos, 1 canal de controle e de 1 de dados para sua transmissão.

Se o atacante não possuir restrições de energia, ele interfere em M canais, caso contrário, ele interfere em menos de M canais, de acordo com sua quantidade de energia disponível. Como não é objetivo deste trabalho modelar a quantidade de energia do atacante, consideramos que suas $M + 1$ opções são equiprováveis. O objetivo do atacante é causar o máximo dano ao US com a limitada capacidade de interferência.

A opção do US legítimo é indicada pelo número de canais utilizados para controle e para dados. Assim $a^l = (c_c, c_d)$, em que c_c e c_d são, respectivamente, o número de canais de controle e de dados utilizados. Como o US legítimo precisa de, pelo menos, 1 canal de controle e 1 de dados, $1 \leq c_c < N_c$ e $1 \leq c_d < N_c$. Finalmente, como o US legítimo não precisa necessariamente utilizar todos os canais disponíveis, então $c_c + c_d \leq N_c$.

O número de opções disponíveis para o US legítimo, N_{op}, é:

$$N_{op} = \frac{N_c * (N_c - 1)}{2} \tag{3.6}$$

A TAB. 3.3 mostra alguns valores de N_{op}, dado o número de canais disponíveis para transmissão:

A opção escolhida pelo atacante, a^j, é igual a (j), em que j é o número de canais interferidos.

As aplicações mais comumente usadas em sistemas militares, como o sistema C2 e o SISTAC do Exército Brasileiro, possuem como principais requisitos de QoS altas confiabilidade e vazão. Devido ao mencionado anteriormente, definimos dois ganhos para o US

Número de Canais Disponíveis para Transmissão	Número de Opções do US Legítimo
8	28
10	45
20	190
50	1205
100	4950

TAB. 3.3: Número de Opções do US Legítimo dado o de Canais Disponíveis

legítimo no caso de não haver restrições de energia: probabilidade de transmissão, p_{trans}, e esperança de vazão, E_v.

No caso de restrições de energia, definimos como ganhos do US legítimo a probabilidade de transmissão *spectrum-efficient*, p_{trans_se}, cujo valor é igual a razão entre a probabilidade de transmissão e o número de canais utilizados, $\frac{p_{trans}}{c_c + c_d}$, e a esperança de vazão *spectrum-efficient*, E_{v_se}, cujo valor é igual a razão entre a esperança de vazão e o número de canais utilizados, $\frac{E_v}{c_c + c_d}$ (WANG, 2011). Isto se dá porque o objetivo do US legítimo é obter o máximo ganho possível por quantidade de energia utilizado, ou seja, pelo número de canais utilizados na transmissão.

Uma estratégia de escolha de opção para o US legítimo, nomeada, Estratégia de Opção Aleatória para o US Legítimo, consiste em enumerar todas as opções disponíveis para o US legítimo e escolher, com a mesma probabilidade, uma delas. Os ganhos do US legítimo utilizando esta estratégia são verificados, via simulações, em 4.3.4.

Outra estratégia, nomeada, Mecanismos com Base em (WANG, 2011), consiste em primeiro determinar um ganho médio para o US legítimo e enumerar suas opções. Na primeira execução do mecanismo, todas as opções do US legítimo são escolhidas com a mesma probabilidade. Sempre que uma opção do US legítimo é escolhida, calcula-se seu ganho e se o ganho obtido for maior que o ganho médio, aumenta sua probabilidade de escolha, caso contrário, diminui sua probabilidade de escolha. Os ganhos do US legítimo utilizando esta estratégia são verificados, via simulações, em 4.3.5.

3.4.6 MECANISMO ANTI-INTERFERÊNCIA PROPOSTO

Nosso mecanismo proposto primeiro enumera todas as opções disponíveis para o US legítimo. Para cada opção do US legítimo, caso não haja restrições de energia, utilizamos o algoritmo CMGS (CAMILO, 2012a), mostrado a seguir, para calcular a probabilidade

de transmissão, p_{trans}, e a esperança de vazão, E_v, dada a opção do US legítimo. Caso haja restrições de energia no dispositivo, executamos o mesmo procedimento acima e dividimos os valores de p_{trans} e E_v por $(c_c + c_d)$ para encontrarmos, respectivamente, os valores de p_{trans_se} e E_{v_se}.

Então, podemos diretamente escolher a melhor opção para o US legítimo, dado o requisito de QoS da aplicação confiabilidade ou vazão e considerando a existência ou não de restrições de energia.

Algoritmo CMGS: Cálculo da Probabilidade de Transmissão e Esperança de Vazão (CAMILO, 2012a).

$p_{trans} = 0$;
$E_v = 0$;
Para $j = 0$ até M faça
  $\alpha = min\{c_c, j\}$;
  Para $c_j = 0$ até α faça
    $\beta = max\{0, (j - c_j) - (N_c - c_c - c_d)\}$;
    $\gamma = min\{c_d, j - c_j\}$;
    Para $d_j = \beta$ até γ faça
      Se $c_c - c_j > 0$ e $c_d - d_j > 0$ então
        $p^{block}_{c_j\_d_j} = \frac{\binom{c_c}{c_j}\binom{a_d}{d_j}\binom{N_c - c_c - c_d}{j - c_j - d_j}}{\binom{N_c}{j}}$;
        $p_{trans} = p_{trans} + p^{block}_{c_j\_d_j}$;
        $E_v = E_v + p^{block}_{c_j\_d_j} * (c_d - d_j)$;
$p_{trans} = \frac{p_{trans}}{M+1}$;
$E_v = \frac{E_v}{M+1}$;

A complexidade do Algoritmo CMGS é $O(M.N_c^2)$.

A E_v fornecida pelo Algoritmo CMGS, assim como as que são calculadas no Capitulo 4, via simulações, para a Estratégia de Opção Aleatória para o US Legítimo e para o Mecanismos com Base em (WANG, 2011), é a esperança de canais não interferidos. Para calcular o valor da $\overline{v_r}$, multiplicamos este valor pelo resultado da equação 3.3.

Sejam c_j e d_j, respectivamente, o número de canais de controle e de dados. Conse-

quentemente, o número de canais de controle e de dados não interferidos são, respectivamente, $c_c - c_j$ e $c_d - d_j$. Só há transmissão se, pelo menos, um canal de controle e um de dados não forem interferidos, ou seja, $c_c - c_j > 0$ e $c_d - d_j > 0$.

A probabilidade de c_j canais de controle e d_j de dados serem interferidos é:

$$p_{c_j\_d_j}^{block} = \frac{\binom{c_c}{c_j}\binom{c_d}{d_j}\binom{N_c - c_c - c_d}{j - c_j - d_j}}{\binom{N_c}{j}} \tag{3.7}$$

O número de canais de controle interferidos, c_j, varia de 0 a $\alpha = min\{c_c, j\}$. Dado que c_j canais de controle foram interferidos. O número de canais de dados interferidos, d_j, varia de $\beta = max\{0, (j - c_j) - (N_c - c_c - c_d)\}$ a $\gamma = min\{c_d, j - c_j\}$.

Portanto a probabilidade de transmissão é:

$$p_{trans} = \frac{1}{M+1} \sum_{j=0}^{M} \sum_{c_j=0}^{\alpha} \sum_{d_j=\beta}^{\gamma} (p_{c_j\_d_j}^{block}) \tag{3.8}$$

e a esperança de vazão é:

$$E_v = \frac{1}{M+1} \sum_{j=0}^{M} \sum_{c_j=0}^{\alpha} \sum_{d_j=\beta}^{\gamma} (p_{c_j\_d_j}^{block}(cd - d_j)) \tag{3.9}$$

ambas, quando $c_c - c_j > 0$ e $c_d - d_j > 0$.

Há dois casos especiais nesta análise:

- 1. Quando $j = 0$ (primeira interação do algoritmo).

Este caso significa que o atacante opta por não interferir, então os únicos valores para c_j e d_j são 0, consequentemente $p_{c_j\_d_j}^{block} = 1$. Como, temos também $(c_d - d_j) = c_d$, então $p_{trans} = 1$ e $E_v = c_d$. Neste caso, a complexidade do algoritmo CMGS é $O(1)$.

- 2. Quando $c_c + c_d = N_c$.

Neste caso, o US Legítimo está utilizando todos os canais disponíveis para transmissão, temos que todos os canais que foram interferidos estão sendo utilizado como canais de controle ou de dados, consequentemente: $j = c_j + d_j$ e c_j varia de 0 a j.

Considerando c_j canais de controle interferidos, $d_j = j - c_j$, então:

$$p_{c_j\_d_j}^{block} = \frac{\binom{c_c}{c_j}\binom{N-c_c}{j-c_j}}{\binom{N_c}{j}} \tag{3.10}$$

Consequentemente:

$$p_{trans} = \frac{1}{M+1}\sum_{j=0}^{M}\sum_{c_j=0}^{\alpha}(p_{c_j\_d_j}^{block}) \tag{3.11}$$

$$E_v = \frac{1}{M+1}\sum_{j=0}^{M}\sum_{c_j=0}^{\alpha}(p_{c_j\_d_j}^{block}(c_c + c_j - j)) \tag{3.12}$$

Neste caso, a complexidade do algoritmo CMGS é $O(M.N_c)$.

Em um cenário com grande número de canais disponíveis para transmissão, dado o reduzido tempo de *slot*, pode ser inviável o cálculo dos ganhos do US legítimo e, consequentemente, da melhor opção. Neste caso, as melhores opções, dados o número de canais disponíveis para transmissão e o número máximo de canais que atacante pode interferir, podem ser calculados anteriormente e colocados na memória do dispositivo.

Em 4.3.3, calculamos, utilizando o Algoritmo CMGS e os parâmetros dados, os ganhos do US legítimo utilizando nosso mecanismo proposto, visando obter os ganhos da opções do US legítimo. Depois, executamos simulações deste mecanismo para validar os resultados obtidos analiticamente.

3.4.7 SISTEMA MONO-CANAL COM ATAQUE DE EMULAÇÃO DE USUÁRIO PRIMÁRIO

Neste sistema, consideramos que a taxa de transmissão do UP é igual a t_p. A taxa de ataques do atacante é igual a t_a, ou seja, em cada intervalo de tempo, caso o UP não esteja transmitindo, o atacante executará uma EUP com uma probabilidade de t_a. O valor de t_a varia de acordo com limitações de energia do US atacante, com sua estratégia de persuasão e com a necessidade de eficiência deste ataque.

Considerando as informações expostas no parágrafo anterior, o fator F_c da equação 3.3, passa a ser $F_c = (1 - (t_u + t_a - t_u * t_a)) * b$. Portanto, a perda da vazão da rede é de:

$$((1 - t_u) * t_a * b) * \Sigma M \tag{3.13}$$

Em 4.4.1, realizamos experimentos numéricos para calcular a perda da vazão da rede no cenário proposto.

Caso t_a tenha valores próximo de 1, o US atacante tem seu ataque mais facilmente detectado, porém terá mais eficiência no ataque. Caso t_a tenha valores próximos de 0, acontece o oposto.

3.4.8 SISTEMA MULTICANAL COM ATAQUE DE EMULAÇÃO DE USUÁRIO PRIMÁRIO

Neste sistema, utilizaremos todas as considerações usadas em 3.4.7. Consideramos ainda que há N_c canais disponíveis para transmissão e que o US legítimo transmite em, no máximo, N_t canais, devido a uma limitação do dispositivo como, por exemplo, o número de antenas ou a quantidade de energia disponível, sendo $N_t \leq N_c$. No entanto, o US legítimo monitora todos os canais para verificar a presença ou não do UP e somente transmite caso o UP não esteja transmitindo no canal e no momento em questão.

O atacante executa a EUP em M canais com a mesma probabilidade t_a.

Consideramos que o tempo necessário para que o US legítimo detecte a presença ou não de uma transmissão do UP, seja esta uma transmissão legítima ou uma emulação executada pelo US atacante, é desprezível.

Uma primeira estratégia, denominada Estratégia de Ocupação Espectral Fixa, é considerar que o US legítimo utiliza sempre os mesmos canais para transmitir mensagens de controle e dados, por exemplo: canal 1 para transmitir mensagens de controle e canais de 2 a N_t para transmitir dados. Nesta abordagem, por possuir capacidade cognitiva, o US atacante detecta o padrão de comportamento do US legítimo e executa suas emulações nos canais de 1 a N_t e sempre ataca o canal de controle, canal 1 neste caso, visando aumentar a eficiência do ataque. Consequentemente, o US legítimo transmite nos canais não atacados com probabilidade $1 - t_u$ e nos canais atacados com probabilidade de $1 - (1 + t_a) * t_u$. Os ganhos do US legítimo utilizando esta estratégia são verificados, via simulações, em 4.4.3.

A estratégia denominada Estratégia com base em (CHEN, 2009) consiste em transmitir nos canais nos quais não foi detectada a transmissão do UP, seja uma transmissão legítima ou uma emulação do US atacante. Os ganhos do US legítimo utilizando esta estratégia são verificados, via simulações, em 4.4.5.

3.4.9 MECANISMO ANTI-EMULAÇÃO DE USUÁRIO PRIMÁRIO PROPOSTO

Definimos a taxa de utilização do canal, t_c, como a razão entre o número de intervalos de tempo no qual detecta-se a transmissão do UP, seja uma transmissão legítima ou uma emulação do US atacante, e o número de intervalos de tempo considerado.

Objetivando a detecção de um ataque de EUP, nosso mecanismo considera ataque quando:

$$t_c \geq (1 + \alpha) * t_u \tag{3.14}$$

Como $t_c = t_u + (1 - t_u) * t_a$, se for conhecido o valor de t_a, podemos estimar o intervalo para α como:

$$0 \leq \alpha \leq \frac{(1 - t_u) * t_a}{t_u} \tag{3.15}$$

No entanto, na maioria das situações reais, t_a não é conhecido e precisa-se arbitrar o valor de α. Executamos simulações em 4.4.1, com alguns valores de α no cenário descrito.

Com a finalidade de mitigar o ataque de EUP, nosso mecanismo proposto também transmite nos canais nos quais não foi detectada a transmissão do UP, seja uma transmissão legítima ou uma emulação do US atacante. Para um melhor aproveitamento do espectro eletromagnético, nosso mecanismo utiliza para transmissão de mensagens de controle o canal com menor RSR dentre os canais citados neste parágrafo e que permitam transmissão, ou seja, o valor de sua RSR está acima do limite superior do intervalo de não transmissão, em outras palavras, $\gamma > v_1$, conforme definido em 3.4.3.

Caso haja, pelo menos, $N_t - 1$ canais que permitam transmissão nos quais não é detectada transmissões do UP e que não é usado para transmitir mensagens de controle, nosso mecanismo escolhe para transmitir dados os $N_t - 1$ canais de maior RSR dentre os canais citados anteriormente. Do contrário, nosso mecanismo utiliza todos os canais, ainda disponíveis, para transmitir dados. Os ganhos do US legítimo utilizando esta estratégia são verificados, via simulações, em 4.4.4.

3.5 RESUMO

Neste capítulo, descrevemos a arquitetura de RC com segurança espectral e estudamos algumas estratégias de mitigação de ataques de interferência e de emulação de usuário

primário. Também propomos mecanismos para mitigação dos citados ataques. No próximo capítulo fazemos experimentos numéricos e simulações para verificar o desempenho dos mecanismos propostos e dos mencionados neste capítulo.

4 RESULTADOS

Neste capítulo, apresentamos os resultados dos experimentos numéricos e simulações realizados com os mecanismos anti-interferência e anti-EUP propostos e de algumas estratégias de mitigação de ataques de interferência e emulação de usuário primário. Mostramos também as comparações de desempenho das abordagens anti-interferência e anti-EUP discutidas.

4.1 INTRODUÇÃO

Nos experimentos numéricos e simulações realizados neste capítulo, utilizamos $b = 2MHz$ e $t_p = 0,5$. Utilizamos cinco estratégias de modulação, ou seja, $K = 5$. As estratégias de modulação, seus intervalos de RSR, em dB, e número de bits por símbolos são mostrados na TAB. 4.1. Estes valores foram utilizados baseado nos valores experimentais citados em (MOURA, 2011), objetivando uma taxa de erro, p_e, igual a 10^{-2}. Não há perda de generalização e outros valores podes ser escolhidos.

Estratégia de Modulação	Intervalo da RSR (dB)	Número de Bits por Símbolo
Não transmite	[0,0000; 7,4062)	0
BPSK	[7,4062; 9,2711)	1
4 QAM	[9,2711; 15,2856)	2
8 QAM	[15,2856; 16,6485)	3
16 QAM	[16,6485; 20,8606)	4
32 QAM	[20,8606; $+\infty$)	5

TAB. 4.1: Estratégias de modulação, Intervalos da RSR e Número de Bits por Símbolo

4.2 SISTEMA MONO-CANAL SEM ATAQUE

Em um primeiro experimento, consideramos um sistema mono-canal sem ataques. Utilizando os valores citados em 4.1 e as equações 3.2 e 3.3, obtemos os valores da $\overline{v_r}$ para várias $\overline{\gamma}$ que são mostrados na TAB. 4.2:

Concluímos pela TAB. 4.2 que, até o limite inferior do intervalo da RSR da estratégia de modulação que proporciona maior taxa de transmissão, um canal com uma RSR média

$\overline{\gamma}$ (dB)	$\overline{v_r}$ (Mbps)
5	$0,077$
10	$2,064$
15	$4,451$
20	$4,897$
25	$4,945$
30	$4,949$
≥ 35	$4,950$

TAB. 4.2: Valores da $\overline{v_r}$ para várias $\overline{\gamma}$

maior proporciona um ganho considerável na $\overline{v_r}$. Após este limite, o aumento da $\overline{v_r}$ para um canal com uma RSR média maior é inexpressivo.

4.3 CENÁRIOS COM ATAQUE DE INTERFERÊNCIA

Nesta seção, consideramos os cenários com ataque de interferência. Primeiro estudamos um sistema mono-canal e depois passamos para um sistema multicanal.

4.3.1 SISTEMA MONO-CANAL COM ATAQUE DE INTERFERÊNCIA

Consideramos um cenário com uma RSR média antes do ataque igual a 35 dB, o que possibilitava uma vazão média de $4,95$ Mb, conforme a TAB. 4.2. Utilizando novamente os valores citados em 4.1 e as equações 3.2 e 3.3, obtemos os valores das perdas da $\overline{v_r}$, para ataques de interferência que reduzem os valores da RSR média para 5, 10, 15, 20, 25 e 30 dB, mostradas na TAB. 4.3.

Novo valor da $\overline{\gamma}$ (dB)	Novo valor da $\overline{v_r}$ (Mbps)	Perda da (%) $\overline{v_r}$
5	$0,077$	$98,44$
10	$2,064$	$58,29$
15	$4,451$	$10,09$
20	$4,897$	$1,08$
25	$4,945$	$0,11$
30	$4,949$	$0,01$

TAB. 4.3: Valores da Perda da $\overline{v_r}$ para várias $\overline{\gamma}$

Concluímos, pela TAB. 4.3, que diminuições na RSR média que:

- mantém este valor dentro do intervalo de RSR da estratégia de modulação que

proporciona maior taxa de transmissão, $\overline{\gamma} = 30$, por exemplo, tem uma perda inexpressiva no valor da vazão média;

- coloca este valor abaixo do intervalo de RSR da estratégia de modulação que proporciona maior taxa de transmissão, $\overline{\gamma} = 15$, por exemplo, tem uma perda considerável no valor da vazão média; e

- coloca este valor abaixo do limite inferior da RSR da estratégia de modulação que proporciona menor taxa de transmissão, $\overline{\gamma} = 5$, por exemplo, tem uma perda muito grande no valor da vazão média, praticamente anulando este valor.

4.3.2 SISTEMA MULTICANAL COM ATAQUE DE INTERFERÊNCIA

Nos experimentos numéricos e simulações desta seção, utilizamos $N_c = 8$ e $M = 4$. Consideramos que todos os N_c canais disponíveis para transmissão possuem a mesma largura de banda. Definimos o ganho do US legítimo nas 4 situações enumeradas a seguir:

- 1. o requisito de QoS da aplicação é confiabilidade e não há restrição de energia.

- 2. o requisito de QoS da aplicação é vazão e não há restrição de energia.

- 3. o requisito de QoS da aplicação é confiabilidade e há restrição de energia.

- 4. o requisito de QoS da aplicação é vazão e não há restrição de energia.

Primeiro, calculamos os valores utilizando o Mecanismo Anti-Interferência Proposto. Depois, calculamos os ganhos do US legítimo utilizando a Estratégia de Opção Aleatória para o US Legítimo. Em seguida, fizemos os mesmo procedimentos utilizando o Mecanismo com Base em (WANG, 2011). Por fim, fizemos a comparação entre as três estratégias.

Considerando nosso cenário proposto, há 28 possíveis opções para o US legítimo. Como o atacante pode interferir em no máximo 4 canais e que as mesmas mensagens de controle são transferidas em todos os canais de controle, se o US legítimo utiliza 5 canais de controle, pelo menos 1 não será interferido. Portanto, não há razão para usar mais que 5 canais de controle. Assim, as opções $(6, 1)$, ou seja, 6 canais de controle e um de dados, $(6, 2)$ e $(7, 1)$ não são razoáveis. No entanto, todas as possíveis opções do US legítimo foram testadas, com o objetivo de comparação dos seus ganhos.

4.3.3 SISTEMA MULTICANAL COM ATAQUE DE INTERFERÊNCIA UTILIZANDO MECANISMOS ANTI-INTERFERÊNCIA PROPOSTO

Neste experimento, o objetivo é calcular a melhor opção para o US Legítimo em cada um dos 4 casos citados em 4.3.2, implementamos uma versão em C++ do Algoritmo CMGS com os parâmetros mencionados anteriormente. Os gráficos com os resultados das probabilidade de transmissão, esperança de vazão, em número de canais não interferidos, probabilidade de transmissão *spectrum-efficient* e esperança de vazão *spectrum-efficient*, também em número de canais não interferidos, são mostrados, respectivamente, nas FIG. 4.1, 4.2, 4.3 e 4.4.

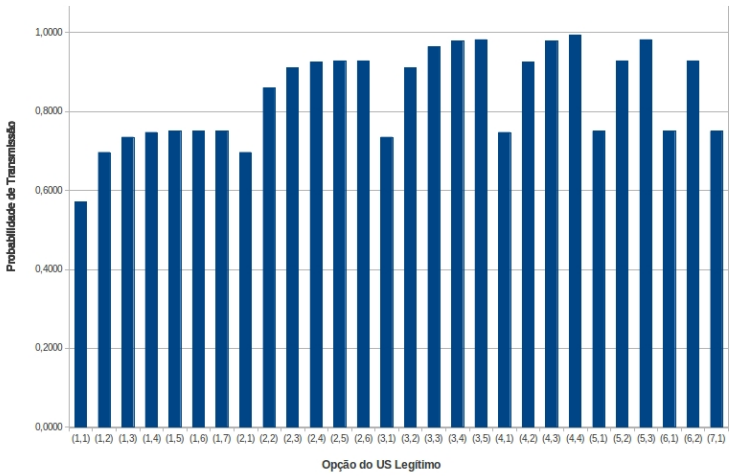

FIG. 4.1: Probabilidade de Transmissão das Opções do US

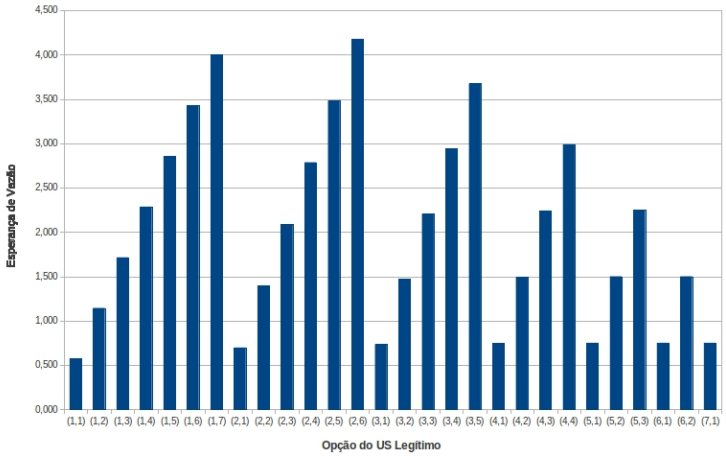

FIG. 4.2: Esperança de Vazão das Opções do US

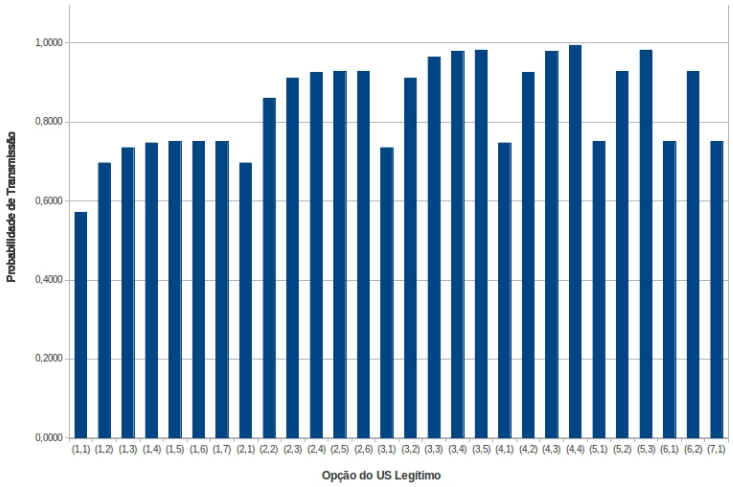

FIG. 4.3: Probabilidade de Transmissão Spectrum-Efficient das Opções do US

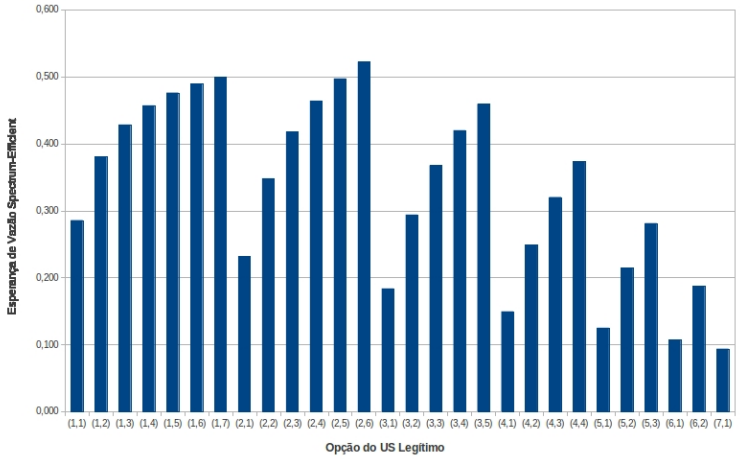

FIG. 4.4: Esperança de Vazão Spectrum-Efficient das Opções do US

Podemos concluir pelos resultados obtidos que dado um dispositivo sem restrição de energia e que executa uma aplicação de vídeo em demanda, que tem como requisito de QoS alta vazão, ou seja, alta quantidade de dados transmitidos por unidade de tempo, deve optar por 2 canais de controle e 6 de dados, opção que lhe proporciona a maior esperança de vazão, cujo valor é igual a $4,179$. Já uma aplicação de correio eletrônico, que tem como requisito de QoS alta confiabilidade, ou seja, probabilidade de entrega de pacotes sem alterações no seu conteúdo, deve optar por 4 canais de controle e 4 de dados, pois esta opção lhe proporciona a maior probabilidade de transmissão, cujo valor é igual a $0,994$.

A título de exemplo do poder de análise obtido a partir do algoritmo CMGS, tem-

se que, dado um dispositivo com restrição de energia e que executa uma aplicação de vídeo em demanda, deve optar por 2 canais de controle e 6 de dados, pois assim obtém a maior esperança de vazão *spectrum-efficient*, cujo valor é igual a $0,522$. Por outro lado, nesta mesma situação, uma aplicação de correio eletrônico, deve optar por 1 canal de controle e 1 de dados, opção que lhe proporciona a maior probabilidade de transmissão *spectrum-efficient*, cujo valor é igual a $0,286$.

Por fim, uma aplicação com requisito de vazão de, pelo menos, 3 canais não interferidos, confiabilidade de, pelo menos, $0,8$ e com capacidade de utilizar no máximo 7 canais, deve optar por 2 canais de controle e 5 de dados, pois esta é a única opção que atende tais requisitos.

Com o objetivo de validar os valores das p_{trans}, E_v, p_{trans_se} e E_{v_se}, calculados utilizando o algoritmo CMGS, executamos simulações do cenário proposto. Implementamos uma versão em C++ do algoritmo CMS1, mostrado a seguir, com o objetivo de realizar as simulações.

Algoritmo CMS1: Simulador do Mecanismo Anti-Interferência Proposto.

$SomaTransmissao = 0$;

$SomaE_v = 0$;

c_c = números de canais utilizados para transmitir mensagens de controle;

c_d = números de canais utilizados para transmitir dados;

Para $i = 0$ até *tempo_simulacao* faça

US legítimo sorteia canais nos quais transmite mensagens de controle;

US legítimo sorteia canais nos quais transmite dados;

US atacante escolhe o número de canais a interferir;

US atacante sorteia canais nos quais interfere;

Calcular c_{c_ni} = número de canais de controle não interferidos;

Calcular c_{d_ni} = número de canais de dados não interferidos;

Se $c_{c\_ni} > 0$ então

$SomaTransmissao = SomaTransmissao + 1$;

$SomaE_v = SomaE_v + c_{d\_ni}$;

$$P_{trans} = \frac{SomaTransmissao}{tempo\_simulacao};$$

$$E_v = \frac{SomaE_v}{tempo\_simulacao};$$

Os valores das p_{trans} e E_v das simulações, os valores analíticos e a diferença percentual entre os valores de cada opção do US legítimo são mostrados, respectivamente, nas TAB. 7.1 e 7.2, em anexo a este trabalho. O tempo de simulação considerado é igual a 10^6 períodos de tempo.

Observa-se que os valores obtidos nas simulações encontram-se em um intervalo de confiança de 95%. Observa-se também que o módulo da diferença entre os valores das simulações e os analíticos foi sempre menor ou igual a 0,12%, o que mostra a validação dos resultados analíticos. Como os valores das p_{trans_se} e E_{v_se} são derivados, respectivamente, dos valores das p_{trans} e E_v, estes também são validados com as simulações acima mencionadas.

4.3.4 SISTEMA MULTICANAL COM ATAQUE DE INTERFERÊNCIA UTILIZANDO ESTRATÉGIA DE OPÇÃO ALEATÓRIA PARA O US LEGÍTIMO

Com o objetivo de verificar os valores da p_{trans}, E_v, p_{trans_se} e E_{v_se}, utilizando a Estratégia de Opção Aleatória para o US Legítimo, executamos simulações desta estratégia. Implementamos uma versão em C++ do Algoritmo CMS2, mostrado a seguir, com o objetivo de realizar as simulações.

Algoritmo CMS2: Simulador da Estratégia de Opção Aleatória para o US Legítimo.

$SomaTransmissao = 0$;
$SomaTransmissao_{se} = 0$;
$SomaE_v = 0$;
$SomaE_{v\_se} = 0$;
Para $i = 0$ até *tempo_simulacao* faça
    US legítimo sorte sua opção (com mesma probabilidade de escolha);
    c_c = números de canais utilizados para transmitir mensagens de controle;
    c_d = números de canais utilizados para transmitir dados;
    US legítimo sorteia canais nos quais transmite mensagens de controle;
    US legítimo sorteia canais nos quais transmite dados;
    US atacante escolhe o número de canais a interferir;

US atacante sorteia canais nos quais interfere;

Calcular c_{c_ni} = número de canais de controle não interferidos;

Calcular c_{d_ni} = número de canais de dados não interferidos;

Se $c_{c\_ni} > 0$ então

$SomaTransmissao = SomaTransmissao + 1$;

$SomaTransmissao_{se} = SomaTransmissao_{se} + \frac{1}{c_c + c_d}$;

$SomaE_v = SomaE_v + c_{d\_ni}$;

$SomaE_{v\_se} = SomaE_{v\_se} + \frac{c_{d\_ni}}{c_c + c_d}$;

$$P_{trans} = \frac{SomaTransmissao}{tempo\_simulacao};$$

$$P_{trans\_se} = \frac{SomaTransmissao_{se}}{tempo\_simulacao};$$

$$E_v = \frac{SomaE_v}{tempo\_simulacao};$$

$$E_{v\_se} = \frac{SomaE_{v\_se}}{tempo\_simulacao};$$

Os valores das p_{trans}, p_{trans_se}, E_v e E_{v_se} são mostrados na TAB. 4.4,

Ganho	Valor
p_{trans}	$0,841$
p_{trans_se}	$0,152$
E_v	$2,020$
E_{v_se}	$0,333$

TAB. 4.4: Ganhos Utilizando a Estratégia de Opção Aleatória para o US Legítimo

Observa-se que os valores obtidos nas simulações encontram-se em um intervalo de confiança de 95%. O tempo de simulação considerado é igual a 10^6 períodos de tempo.

4.3.5 SISTEMA MULTICANAL COM ATAQUE DE INTERFERÊNCIA UTILIZANDO MECANISMOS COM BASE EM (WANG, 2011)

Com o objetivo de verificar os valores da p_{trans}, E_v, p_{trans_se} e E_{v_se}, utilizando o Mecanismo com base em (WANG, 2011), executamos simulações desta estratégia. Implementamos

uma versão em C++ do Algoritmo CMS3, mostrado a seguir, com o objetivo de realizar as simulações.

Algoritmo CMS3: Simulador do Mecanismo com Base em (WANG, 2011).

$SomaGanho = 0$;
$MedGanho = GanhoMaximo/2$;
Para todos as Opções do US Legítimo
    probabilidade de escolha da Opção = K;
Para $i = 0$ até *tempo_simulacao* faça
    US legítimo sorte sua opção;
     (de acordo com a probabilidade de escolha de cada opção);
    c_c = números de canais utilizados para transmitir mensagens de controle;
    c_d = números de canais utilizados para transmitir dados;
    US legítimo sorteia canais nos quais transmite mensagens de controle;
    US legítimo sorteia canais nos quais transmite dados;
    US atacante escolhe o número de canais a interferir;
    US atacante sorteia canais nos quais interfere;
    Calcular c_{c_ni} = número de canais de controle não interferidos;
    Calcular c_{d_ni} = número de canais de dados não interferidos;
    Calcular *ganho* (semelhante ao algoritmo CMS1);
    $SomaGanho = SomaGanho + ganho$;
    Se $ganho \geq MedGanho$;
        Aumentar a probabilidade de escolha da opção proporcionalmente à
         $ganho - MedGanho$;
    Senão
        Diminuir a probabilidade de escolha da opção proporcionalmente à
         $MedGanho - Ganho$;
$MediaGanho = SomaGanho/tempo\_simulacao$;

Implementamos uma versão deste algoritmo para cada um dos quatros ganhos descritos anteriormente: p_{trans}, p_{trans_se}, E_v e E_{v_se}. No caso de p_{trans}, o $GanhoMaximo$ considerado é 1, considerando que há transmissão no período de tempo. No caso de p_{trans_se}, o $GanhoMaximo$ considerado é $\frac{1}{2}$, quando há transmissão no período de tempo

utilizando 2 canais, um para mensagens de controle e um para dados. No caso de E_v, o $GanhoMaximo$ considerado é $Nc-1$. No caso de E_{v_se}, o $GanhoMaximo$ considerado é $\frac{Nc-1}{Nc}$. Os valores da p_{trans}, p_{trans_se}, E_v e E_{v_se} são mostrados na TAB. 4.5.

Ganho	Tempo de Simulação 10^4	Tempo de Simulação 10^5	Tempo de Simulação 10^6
p_{trans}	$0,852$	$0,877$	$0,902$
p_{trans_se}	$0,187$	$0,212$	$0,223$
E_v	$3,477$	$3,993$	$4,109$
E_{v_se}	$0,438$	$0,494$	$0,511$

TAB. 4.5: Ganhos Utilizando o Mecanismo com Base em (WANG, 2011)

Observa-se que os valores obtidos nas simulações encontram-se em um intervalo de confiança de 95%. Os ganhos utilizando este mecanismo variam de acordo com o tempo de simulação. Devido a este fato, consideramos tempos de simulação iguais a 10^4, 10^5 e 10^6 períodos de tempo.

4.3.6 COMPARAÇÃO DAS ESTRATÉGIAS ANTI-INTERFERÊNCIA

Os valores dos ganhos do US legítimo utilizando as três estratégias abordadas são mostrados na TAB. 4.6.

Ganho	Mecanismo Proposto	Estratégia Aleatória	Mecanismo (WANG, 2011)
p_{trans}	$0,994$	$0,841$	$0,852$ / $0,877$ / $0,902$
p_{trans_se}	$0,286$	$0,152$	$0,187$ / $0,212$ / $0,223$
E_v	$4,179$	$2,020$	$3,477$ / $3,993$ / $4,109$
E_{v_se}	$0,522$	$0,333$	$0,438$ / $0,494$ / $0,511$

TAB. 4.6: Ganhos do US Legítimo Utilizando as Três Estratégias Abordadas

Concluímos que o Mecanismo Anti-Interferência Proposto possibilita valores das p_{trans}, p_{trans_se}, E_v e E_{v_se}, respectivamente, 18,21%, 87,59%, 106,88% e 56,76% maiores que os da Estratégia de Opção Aleatória para o US Legítimo.

Comparado com o Mecanismo com Base em (WANG, 2011), em um cenário no qual o número de canais disponíveis para transmissão varia em média a cada 10^4 períodos de tempo (10s, quando $T_f = 10^{-3}$s), o Mecanismo Anti-Interferência Proposto possibilita valores da p_{trans}, p_{trans_se}, E_v e E_{v_se}, respectivamente, 16,73%, 52,70%, 20,19% e 19,18% maiores. Em um cenário no qual o número de canais disponíveis para transmissão varia

em média a cada 10^5 períodos de tempo, os ganhos obtidos com o Mecanismo Anti-Interferência Proposto são, respectivamente, 13,32%, 34,51%, 4,66% e 5,67% maiores. Em um cenário no qual o número de canais disponíveis para transmissão varia em média a cada 10^6 períodos de tempo, os ganhos obtidos com o Mecanismo Anti-Interferência Proposto são, respectivamente, 10,28%, 28,29%, 1,70% e 2,15% maiores.

4.4 CENÁRIOS COM ATAQUE DE EMULAÇÃO DE USUÁRIO PRIMÁRIO

Nesta seção, consideramos os cenários com ataque de emulação de usuário primário. Primeiro estudamos um sistema mono-canal e depois passamos para um sistema multicanal.

Nos experimento desta seção, consideramos os seguintes parâmetros: $t_p = 0.5$ e $t_a = 0.5$.

4.4.1 SISTEMA MONO-CANAL COM ATAQUE DE EMULAÇÃO DE USUÁRIO PRIMÁRIO

Utilizando os valores do cenário descrito anteriormente, a RSR média da rede de 25 dB e com base na equação 3.13, calculamos os valores da perda da vazão da rede com alguns valores de t_a. Esse valores são mostrados na TAB. 4.7

t_a	Novo valor da $\overline{v_r}$ (Mbps)	Perda da $\overline{v_r}$ (%)
$0,1$	$4,450$	10
$0,2$	$3,956$	20
$0,3$	$3,461$	35
$0,4$	$2,967$	40
$0,5$	$2,472$	50
$0,9$	$0,494$	90

TAB. 4.7: Valores da Perda da $\overline{v_r}$ para várias t_a

Uma conclusão óbvia é que quanto maior for a t_a, maior será a perda da $\overline{v_r}$.

Considerando o cenário descrito anteriormente e com base na equação 3.14, executamos simulações da detecção deste ataque.

Utilizando a equação 3.15, para determinar α, temos que $0 \leq \alpha \leq 0.1$.

Com $\alpha = 0,1$, há a detecção de 98% do canais atacados e não há notificações de ataques em canais não atacados. Quando $\alpha = 0,001$, há a detecção de 100% do canais atacados,

porém 62% dos canais não atacados são notificados como atacados. Considerando $\alpha = 1,1$, há a detecção de 72% do canais atacados e não há notificações de ataques em canais não atacados. Sendo $\alpha = 1,5$, não há detecção ataque nem notificações de ataques em canais não atacados.

Concluímos que a arbitragem do valor de α é de fundamental importância para a detecção de ataque de EUP por nosso mecanismo. Uma sugestão para melhorar esse desempenho é a utilização de técnicas multi-critérios como, por exemplo, a proposta por (SOTO, 2012).

4.4.2 SISTEMA MULTICANAL COM ATAQUE DE EMULAÇÃO DE USUÁRIO PRIMÁRIO

Nos experimento desta seção, consideramos também os seguintes parâmetros: $N_c = 16$, $N_t = 8$ e $M = 4$.

Com o objetivo de verificar os valores da p_{trans}, E_v, p_{trans_se} e E_{v_se}, utilizando as três estratégias citadas em 3.4.8 e 3.4.9, executamos simulações utilizando o Algoritmo CMS4, mostrado a seguir.

Algoritmo CMS4: Cálculo dos Ganhos do US Legítimo em Face de Ataque de EUP

$SomaGanho = 0$;
Para $j = 0$ até $tempo\_simulacao$ faça
    Para $i = 1$ até M faça
        Sortear canal i para ataque;
    Para $k = 1$ até N_c faça
        Sortear intervalo de RSR do canal k;
        Sortear se o UP transmite ou não no canal k;
        Se o UP não transmite no canal e se o canal foi sorteado para ataque
            Sortear se há ou não ataque no canal k;
    US legítimo define canal nos quais transmite mensagens de controle;
    US legítimo define canais nos quais transmite dados;
    Calcular ganho;
    $SomaGanho = SomaGanho + ganho$;
$MediaGanho = SomaGanho/tempo\_simulacao$;

Considerando este cenário, primeiro, calculamos os valores utilizando a Estratégia de Ocupação Espectral Fixa. Depois, calculamos os ganhos do US legítimo utilizando o Mecanismo Anti-EUP Proposto. Em seguida, fizemos os mesmo procedimentos utilizando o Mecanismo com Base em (CHEN, 2009). Por fim, fizemos a comparação entre as três estratégias.

4.4.3 SISTEMA MULTICANAL COM ATAQUE DE EMULAÇÃO DE USUÁRIO PRIMÁRIO UTILIZANDO A ESTRATÉGIA DE OCUPAÇÃO ESPECTRAL FIXA

Com o objetivo de verificar os valores da p_{trans}, E_v, p_{trans_se} e E_{v_se}, utilizando a estratégia fixa, citada em 3.4.8, implementamos uma versão em C++ do Algoritmo CMS4 para realizar as simulações. Os valores da p_{trans}, p_{trans_se}, E_v e E_{v_se} são mostrados na TAB. 4.8.

Ganho	Valor
p_{trans}	$0,394$
p_{trans_se}	$0,102$
E_v	$5,766$
E_{v_se}	$1,312$

TAB. 4.8: Ganhos do US Legítimo Utilizando a Estratégia de Ocupação Espectral Fixa

Observa-se que os valores obtidos nas simulações encontram-se em um intervalo de confiança de 95%.

4.4.4 CENÁRIO MULTICANAL COM ATAQUE DE EMULAÇÃO DE USUÁRIO PRIMÁRIO UTILIZANDO O MECANISMO ANTI-EUP PROPOSTO

Com o objetivo de verificar os valores da p_{trans}, E_v, p_{trans_se} e E_{v_se}, utilizando o mecanismo anti-EUP proposto, citado em 3.4.9, implementamos uma versão em C++ do Algoritmo CMS4 para realizar as simulações. Os valores das p_{trans}, p_{trans_se}, E_v e E_{v_se} são mostrados na TAB. 4.9.

Observa-se que os valores obtidos nas simulações encontram-se em um intervalo de confiança de 95%.

Ganho	Valor
p_{trans}	$0,999$
p_{trans_se}	$0,154$
E_v	$28,820$
E_{v_se}	$4,144$

TAB. 4.9: Ganhos do US Legítimo Utilizando o Mecanismo Anti-EUP Proposto

4.4.5 CENÁRIO MULTICANAL COM ATAQUE DE EMULAÇÃO DE USUÁRIO PRIMÁRIO UTILIZANDO O MECANISMO COM BASE EM (CHEN, 2009)

Com o objetivo de verificar os valores da p_{trans}, E_v, p_{trans_se} e E_{v_se}, utilizando o mecanismos com base em (CHEN, 2009), citado em 3.4.8, implementamos uma versão em C++ do Algoritmo CMS4 para realizar as simulações. Os valores da p_{trans}, p_{trans_se}, E_v e E_{v_se} são mostrados na TAB. 4.10.

Ganho	Valor
p_{trans}	$0,999$
p_{trans_se}	$0,150$
E_v	$26,977$
E_{v_se}	$3,819$

TAB. 4.10: Ganhos do US Legítimo Utilizando o Mecanismo com base em (CHEN, 2009)

Observa-se que os valores obtidos nas simulações encontram-se em um intervalo de confiança de 95%.

4.4.6 COMPARAÇÃO DAS ESTRATÉGIAS ANTI-EUP

Os valores dos ganhos do US Legítimo utilizando as três estratégias abordadas são mostrados na TAB. 4.11.

Ganho	Mecanismo Proposto	Estratégia de Ocupação Espectral Fixa	Mecanismo com base em (CHEN, 2009)
p_{trans}	$0,999$	$0,394$	$0,999$
p_{trans_se}	$0,154$	$0,102$	$0,150$
E_v	$28,820$	$5,766$	$26,977$
E_{v_se}	$4,144$	$1,312$	$3,819$

TAB. 4.11: Ganhos do US Legítimo Utilizando as Três Estratégias Discutidas

Concluímos que o Mecanismo Anti-EUP Proposto possibilita valores da p_{trans}, p_{trans_se}, E_v e E_{v_se}, respectivamente, 153,55%, 50,98%, 399,83% e 215,85% maiores que os da Estratégia de Ocupação Espectral Fixa.

Comparado com o Mecanismo Proposto por (CHEN, 2009), o Mecanismo Anti-EUP Proposto possibilita o mesmo valor da p_{trans} e valores das p_{trans}, E_v e E_{v_se}, respectivamente, 2,67%, 6,83% e 8,51% maiores.

4.5 RESUMO

Neste capítulo, apresentamos os resultados obtidos, no qual, mostramos os experimentos numéricos e simulações realizados com os mecanismos anti-interferência e anti-EUP, bem como a comparação do desempenho dos nossos mecanismos proposto com outras abordagens. No próximo capítulo, apresentamos as conclusões do trabalho, indicando as contribuições da dissertação, bem como as oportunidades de trabalhos futuros.

5 CONSIDERAÇÕES FINAIS

5.1 CONCLUSÕES

Os mecanismos estudados para defesa anti-interferência e anti PUEA são validados considerando os mecanismos isolados das fases do ciclo cognitivo, em lugar de uma abordagem integrada. Com o desenvolvimento de mecanismos de defesa em RRC, surge a necessidade de arquiteturas validadas e integradas para RC que contemplem mecanismos de segurança.

Os trabalhos presentes na literatura possuem duas limitações principais: a insensibilidade dos modelos à diferença de requisitos de QoS e a adoção de um modelo com restrição de energia e que não contempla outras aplicações.

Os pontos em aberto identificados neste trabalho são:

- Arquitetura de RC;
- Mecanismos anti-interferência e
- Mecanismos anti-EUP.

A primeira, com base em (CAMILO, 2012b), é a arquitetura CMPS para RC que contempla a segurança espectral. Assim, mecanismos de defesa podem ser validados. Como proposta, a arquitetura CMPS apresenta o componente de Segurança Espectral como aprimoramento do ciclo cognitivo descrito em (AKYILDIZ, 2006) e considerando os quatro conjunto de informações de entrada principais listados por (DOYLE, 2009): informações do ambiente rádio, informações dos requisitos de QoS da aplicação, informações dos recursos disponíveis para o dispositivos e informações da política regulatório do uso do espectro.

A segunda é um mecanismo anti-interferência em RRC que, com base em (CAMILO, 2012a), calcula a melhor ocupação espectral para o usuário secundário, introduz a aleatoriedade na escolha de canais e transmite as mensagens de controle e os dados de maneira redundante em múltiplos canais. Neste fase, estudamos os efeitos do ataque de interferência em redes de rádios cognitivos. Avaliamos os efeitos dos perfis de ocupação es-

pectral do usuário primário e do atacante, bem como de parâmetros da camada física na confiabilidade e na vazão média da rede.

Por fim, a terceira proposta é um mecanismo de mitigação de ataque de EUP em RRC que introduz a aleatoriedade e utiliza informações da camada física para a escolha de canais. Neste fase, estudamos os efeitos do ataque de emulação de usuário primário em redes de rádios cognitivos. Avaliamos os efeitos dos perfis de ocupação espectral do usuário primário e do atacante, bem como de parâmetros da camada física na vazão média da rede.

Isto posto, esta dissertação apresenta as seguintes conclusões:

- Arquitetura de RC

Objetivando o estudo dos mecanismos de segurança para RRC de maneira integrada ao ciclo cognitivo e que seja sensível aos quatro tipos de informações listados por (DOYLE, 2009), há a necessidade de uma arquitetura para RC que contemple o componente de Segurança Espectral, como aprimoramento do ciclo cognitivo descrito em (AKYILDIZ, 2006), e que considere os quatro conjunto de informações de entrada citados.

- Mecanismo Anti-interferência Proposto

Três parâmetros devem ser considerados na utilização de uma rede de rádios cognitivos sobre uma rede primária: a largura de banda do canal, a relação sinal-ruído média e a taxa de utilização do UP.

Considerando um sistema mono-canal, concluímos que até o limite inferior do intervalo da RSR da estratégia de modulação que proporciona maior taxa de transmissão, um canal com uma RSR média maior proporciona um ganho considerável na vazão média da rede. Após este limite, o aumento da vazão média da rede para um canal com uma RSR média maior é inexpressivo. Sob um ataque de interferência, manter o valor da RSR média no intervalo da estratégia de modulação que proporciona maior taxa de transmissão, é de fundamental importância para o desempenho da rede, para atingir este objetivo, O US legítimo pode adotar as estratégias de aumentar a potência de transmissão ou de utilizar antenas direcionais.

O Mecanismo Anti-Interferência Proposto possibilita valores da p_{trans}, p_{trans_se}, E_v e E_{v_se}, respectivamente, 18,21%, 87,59%, 106,88% e 56,76% maiores que os da Estratégia de Opção Aleatória para o US Legítimo.

Comparado com o Mecanismo com Base em (WANG, 2011), em um cenário no qual o número de canais disponíveis para transmissão varia em média a cada 10^4 períodos de tempo (10s, quando $T_f = 10^{-3}$s), o Mecanismo Anti-Interferência Proposto possibilita valores da p_{trans}, p_{trans_se}, E_v e E_{v_se}, respectivamente, 16,73%, 52,70%, 20,19% e 19,18% maiores. Em um cenário no qual o número de canais disponíveis para transmissão varia em média a cada 10^5 períodos de tempo, os ganhos obtidos do Mecanismo Anti-Interferência Proposto são, respectivamente, 13,32%, 34,51%, 4,66% e 5,67% maiores. Em um cenário no qual o número de canais disponíveis para transmissão varia em média a cada 10^6 períodos de tempo, os ganhos do Mecanismo Anti-Interferência Proposto são, respectivamente, 10,28%, 28,29%, 1,70% e 2,15% maiores.

- Mecanismo Anti-Emulação de Usuário Primário

Uma conclusão óbvia é que quanto maior for a taxa de ataque, maior será a perda da vazão média da rede.

Se for conhecido o valor da taxa de ataque, podemos, calculando a taxa de utilização real do UP, detectar ataques de EUP com precisão. No entanto, na maioria das situações reais, a taxa de ataque não é conhecida. Neste caso, uma sugestão para melhorar a precisão da detecção deste ataque é a utilização de técnicas multi-critérios como, por exemplo, a proposta por (SOTO, 2012).

Concluímos que o Mecanismo Anti-EUP Proposto possibilita valores da p_{trans}, p_{trans_se}, E_v e E_{v_se}, respectivamente, 153,55%, 50,98%, 399,83% e 215,85% maiores que os da Estratégia de Ocupação Espectral Fixa.

Comparado com o Mecanismo Proposto por (CHEN, 2009), o Mecanismo Anti-EUP Proposto possibilita o mesmo valor da p_{trans} e valores das p_{trans_se}, E_v e E_{v_se}, respectivamente, 2,67%, 6,83% e 8,51% maiores.

5.2 PERSPECTIVAS PARA TRABALHOS FUTUROS

O estudo feito neste trabalho deixa alguns desafios futuros. Neste trabalho, consideramos que a potência utilizada em todos os canais é a mesma, consequentemente, o consumo de energia é proporcional ao número de canais. Esta consideração é pouco realista. Um desafio é fazer as análises elaboradas neste artigo considerando consumos energéticos diferentes por canal.

Outra consideração pouco realista deste trabalho é a de que o tempo necessário para que o US legítimo detecte a presença ou não de uma transmissão do UP, seja esta uma transmissão legítima ou uma emulação executada pelo US atacante, é desprezível. Considerar a influência do tempo de detecção da transmissão do UP no desempenhos do mecanismos de mitigação de ataque é um trabalho futuro promissor.

Outra contribuição importante é propor o ganho do US legítimo considerando que a aplicação que está sendo executada possui mais de um requisito de QoS, pois algumas aplicações, tal como transferência de arquivos, tem a característica da combinação de restrições independentes.

Por fim, outro desafio é a proposta de mecanismos semelhantes ao descrito neste trabalho para mitigar ou reduzir os efeitos de outros ataques em redes de rádios cognitivos, tais como a falsificação de dados do espectro monitorado.

5.3 PUBLICAÇÕES

Esta seção descreve os trabalhos publicados e submetidos diretamente relacionados a esta dissertação.

- Arquitetura de rede de rádios cognitivos utilizando redes de petri de alto nível. Camilo, M. J., Pinheiro, W. A., Moura, D. F. C. e Salles, R. M.
  II Workshop em Redes de Acesso em Banda Larga, Brasil, Mai 2012.

- Anti-jamming defense mechanism in cognitive radios networks. Camilo, M. J., Moura, D. F. C., Galdino, J. e Salles, R. M.
  IEEE MILCOM'12, EUA, Nov 2012.

- Análise de Desempenho em Redes de Rádios Cognitivos Militares. Camilo, M. J., Moura, D. F. C. e Salles, R. M.
  Submetido ao Simpósio Brasileiro de Redes de Computadores, Brasil, Mai 2013.

6 REFERÊNCIAS BIBLIOGRÁFICAS

AKYILDIZ, I. F., LEE, W., VURAN, M. C. e MOHANTY, S. Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey. Em *Computer Networks Journal*, volume 50, págs. 2127–2159, 2006.

AKYILDIZ, I. F., LEE, W., VURAN, M. C. e MOHANTY, S. A survey on spectrum management in cognitive radio networks. Em *IEEE Communications Magazine*, volume 46, págs. 40–48, 2008.

ANAND, S., JIN, Z. e SUBBALAKSHMI, K. An analytical model for primary user emulation attacks in cognitive radio networks. Em *IEEE Symposium on New Frontiers in Dynamic Spectrum Access networks (DySPAN)*, págs. 1–6, 2008.

ANATEL. Divisão do espectro no brasil, último acesso: Setembro de 2012. http://www.anatel.gov.br/portal/exibirportalinternet.do. 2012.

ARIANANDA, D., LAKHSMANAN, M. e NIKOO, H. A survey on spectrum sensing techniques for cognitive radio. Em *International Workshop on Cognitive Radio and Advanced Spectrum Management (CogArt)*, págs. 74–79, 2009.

BROWN, L. *A Radar History of World War II.* Taylor & Francis, 1999.

CABRIC, D., MISHRA, S. M. e BRODERSEN, R. W. Implementation issues in spectrum sensing for cognitive radios. Em *Proc. 38th Asilomar Conference on Signals, Systems and Computers 2004*, págs. 772–776, 2004.

CAMILO, M. J., MOURA, D. F. C., GALDINO, J. e SALLES, R. M. Anti-jamming defense mechanism in cognitive radios networks. Em *2012 Military Communications Conference (MILCOM 2012)*, 2012a.

CAMILO, M. J., PINHEIRO, W. A., MOURA, D. F. C. e SALLES, R. M. Arquitetura de rede de rádios cognitivos utilizando redes de petri de alto nível. Em *II Workshop em Redes de Acesso em Banda Larga*, págs. 89–102, 2012b.

CANBERK, B., AKYILDIZ, I. F. e OKTUG, S. A qos-aware framework for available spectrum characterization and decision in cognitive radio networks. Em *21th IEEE International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC)*, págs. 1533–1538, 2010.

CHEN, C., CHENG, H. e YAO, I. D. Cooperative spectrum sensing in cognitive radio networks in the presence of the primary use emulation attack. Em *IEEE Wireless Communications*, págs. 2135–2141, 2011a.

CHEN, K. C., PENG, Y. J., PRASAD, N. e LIANG, Y. C. Cognitive radio network architecture: part i: general structure. Em *2nd International Conference on Ubiquitous Information Management and Communication*, págs. 114–119, 2008a.

CHEN, R. e PARK, J. Ensuring trustworthy spectrum sensing in cognitive radio networks. Em *IEEE Workshop in Networking Technologies for Software Defined Radio Networks*, págs. 110–119, 2006.

CHEN, R., PARK, J. e BIAN, K. Robust distributed spectrum sensing in cognitive radio networks. Em *IEEE 27th Conference on Computer Communications (INFOCOM)*, págs. 31–35, 2008b.

CHEN, R., PARK, J. M., HOU, Y. T. e REED, J. H. Toward secure distributed spectrum sensing in cognitive radio networks. Em *IEEE Communications Magazine, Special Issue on Cognitive Radio Communications*, págs. 50–55, 2008c.

CHEN, R., PARK, J. M. e REED, J. H. Defense against primary emulation attacks in cognitive radio networks. Em *IEEE Journal on Selcted Areas in Communications*, págs. 25–37, 2008d.

CHEN, S., ZENG, K. e MOHAPATRA, P. Hearing is believing: Deteting mobile primary user emulation attack in white space. Em *IEEE Conference on Computer Communications (INFOCOM)*, págs. 36–40, 2011b.

CHEN, Z., COOKLEVAND, T., CHEN, C. e POMALAZA-RAEZ, C. Modeling primary user emulation attacks and defenses in cognitive radio networks. Em *IEEE International Performance Computing and Communications Conference (IPCCC)*, págs. 208–215, 2009.

DOYLE, L. E. *Essentials of Cognitive Radio*. Cambridge University Press, 2009.

DUBEY, R. e SHARMA, S. Distributed shared spectrum techniques for cognitive wireless radio networks. Em *International Conference on Computational Intelligence and Communication Networks (CICN)*, págs. 259–264, 2010.

FCC. Spectrum policy task force report. Number 02.2135, 2002.

FCC. Notice of inquiry and notice of proposed rulemaking. Em *ET Docket*, number 03.237, 2003.

GE, Y., SUN, Y., LU, S. e DUTKIEWICZ, E. Adsd: An automatic distributed spectrum decison method in cognitive radio networks. Em *First International Conference on Future Information Networks (ICFIN)*, págs. 253–258, 2009.

HALLDORSON, M. M., HALPERN, J. Y., LI, L. e MIRROKNI, V. S. On spectrum sharing games. Em *Proc. ACM on Principles of distributed computing*, págs. 213–222, 2004.

HAYKIN, S. Cognitive radio: brain-empowered wireless communications. Em *IEEE Journal on Selected Areas in Communications*, volume 23, págs. 201–210, 2005.

HU, J. e WELLMAN, M. P. Multiagent reinforcement learning: Theoretical framework and an algorithm. Em *Proc. 15th International Conference on Machine Learning*, págs. 242–250, 1998.

ISHIBASHI, B., BOUABDALLAH, N. e BOUTABA, R. Qos performance analysis of cognitive radio-based virtual wireless networks. Em *IEEE Conference on Computer Communications (IFOCOM)*, págs. 2423–2431, 2008.

JIN, Z., ANAND, S. e SUBBALAKSHMI, K. Detecting primary user emulation attacks in dynamic spectrum access networks. Em *IEEE International Conference on Communications (ICC)*, págs. 2749–2753, 2009a.

JIN, Z., ANAND, S. e SUBBALAKSHMI, K. Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis esting. Em *Mobiling Computing and Communications Review (SIGMOBILE)*, págs. 74–85, 2009b.

JIN, Z., ANAND, S. e SUBBALAKSHMI, K. Robust spectrum decision protocol against primary user emulation attacks in dynamic spectrum access networks. Em *IEEE Global Telecommunications Conference (GLOBECOM)*, págs. 1–5, 2010.

KAPLAN, M. e BUZLUCA, F. A dynamic spectrum decision scheme for heterogeneous cognitive radio networks. Em *24th International Symposium on Computer and Information Sciences (ISCIS)*, págs. 697–702, 2009.

LEE, W. e AKYILDIZ, I. F. A spectrum decision framework for cognitive radio networks. Em *IEEE Transactions on Mobile Computing*, págs. 161–174, 2011.

LI, H. e HAN, Z. Dogfight in spectrum: Combating primary user emulation attacks in cogntive radio systems, part i: Know channel statistics. Em *IEEE Transactions on Wireless Communications*, págs. 3566–3577, 2010.

LI, L. e CADEAU, C. Anti-jamming strategy for cognitive radio network. Em *IEEE International Conference on Communications (ICC), 2011*, págs. 6–15, 2011.

LINDEN, R. *Algoritmos Genéticos*. Brasport, 2006.

LIU, K. J. R. e WANG, B. *Cognitive Radio Networking and Security*. Cambridge University Press, 2011.

MACKENZIE, A. B. e SILVA, L. A. D. *Game Theory for Wireless Engineers*. Morgan & Clayupool, 2006.

MIN, A., KIM, K. H. e SHIN, K. Robust cooperative sensing via state estimation in cognitive radio networks. Em *IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, págs. 185–196, 2011.

MITOLA, J. *Cognitive Radio: Model-Based Competence for Software Radios*. PhD thesis, Dept.of Teleinformatics, KTH, 1999.

MOURA, D. F. C. e SALLES, R. M. *Cooperação entre camadas para adaptação de modulação em redes militares sem fio*. Instituo Militar de Engenharia, 2011.

NEEL, J. J. Issues in fielding large scale cognitive radio networks in hostile environments. Em *International Software Radio Conference 2010*, 2010.

NIYATO, D. e HOSSAIN, E. Market-equilibrium, competitive, and cooperative pricing for spectrum sharing in cognitive radio networks: Analysis and comparison. Em *IEEE Transactions on Wireless Communications*, págs. 4273–4283, 2018.

NOUBIR, G. On connectivity in ad hoc network under jamming using directional antennas and mobility. Em *International Conference on Wired/Wireless Internet Communications*, págs. 186–200, 2004.

PARVIN, S., HUSSAIN, F. K., HUSSAIN, O. K., HAN, S., TIAN, B. e CHANG, E. Cognitive radio network security: A survey. Em *Journal of Network and Computer Applications*, 2012.

REED, J. e BOSTIAN, W. Understanding the issues in software defined cognitive radio. Em *IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN) 2005*, págs. 611–614, 2005.

SADEGHI, P., KENNEDY, R. A., RAPAJIC, P. B. e SHAMS, R. Finite-state markov modeling of fading channels. Em *IEEE Signal Processing Magazine, vol. 25, no. 5*, págs. 57–80, 2008.

SAHAI, A., HOVEN, N. e TANDRA, R. Some fundamental limits in cognitive radio. Em *Allerton Conference on Communication, Control and Computing*, 2004.

SALLES, R. M., MOURA, D. F. C., CARVALHO, J. M. A. e SILVA, M. R. Novas perspectivas tecnológicas para o emprego das comunicações no exército brasileiro. Em *Revista Militar de Ciência e Tecnologia*, págs. 68–80, 2008.

SKLAR, B. Rayleigh fading channels in mobile digital communication systems, part 1: Characterization. Em *IEEE Communications Magazine*, volume 35, págs. 90–100, 1997.

SODAGARI, S. e CLANCY, T. C. *Anti-jamming strategy for channel acces in cognitive radio network*. Department of Electrical and Computer Engineering - Virginia Tech - Arlington, 2011.

SOTO, J. C. H. e LIMA, M. N. *Um Esquema de Múltiplos Critérios para Análise Cooperativa da Presença de Ataques EUP em Redes Ad Hoc de Rádio Cognitivo*. Universidade Federal do Paraná, 2012.

SU, H., WANG, Q., REN, K. e XING, K. Jamming-resilient dynamic spectrum access for cognitive radio networks. Em *IEEE International Conference on Communications (ICC), 2011*, págs. 1–5, 2011.

TANDRA, R. e SAHAI, A. Fundamental limits on detection in low snr under noise uncertainty. Em *WirelessCom*, volume 9, págs. 464–469, 2005.

TANEMBAUM, A. S. *Redes de Computadores, 4a Edição*. Editora Campus, 2003.

TANG, H. Some physical layer issues of wide-band cognitive radio system. Em *IEEE Symposium on New Frontiers in Dynamic Spectrum Access networks (DySPAN)*, págs. 151–159, 2005.

TORLAK, M. e DUMAN, T. Mimo communication theory, algorithms, and prototyping. Em *20th Signal Processing and Communications Applications Conference*, 2012.

WANG, B., JI, Z., LIU, K. J. R. e CLANCY, C. Primary-prioritized markov approach for efficient and fair dynamic spectrum allocation. Em *IEEE Transaction on Wireless Communications*, volume 8, págs. 1854–1865, 2009.

WANG, B., WU, Y. e LIU, K. J. R. Game theory for cognitive radio networks: an overview. Em *Computer Networks*, volume 54, págs. 2537–2561, 2010.

WANG, B., WU, Y., LIU, K. J. R. e CLANCY, T. C. An anti-jamming stochastic game for cognitive radio networks. Em *IEEE Journal on Selected Areas in Communications*, volume 29, págs. 877–889, 2011.

WERRELL, K. P. *Air War Victorious: The Gulf War vs. Vietnam*. Parameter, 1992.

WILD, B. e RAMCHANDRAN, K. Detecting primary receivers for cognitive radio applications. Em *IEEE Symposium on New Frontiers in Dynamic Spectrum Access networks (DySPAN)*, págs. 124–130, 2005.

XING, Y., CHANDRAMOULI, R., MANGOLD, S. e SHANKAR, S. Dynamic spectrum access in open spectrum wireless networks. Em *IEEE Journal on Selected Areas in Communications*, volume 24, págs. 626–637, 2006.

YUCEK, T. e ARSLAN, H. A survey of spectrum sensing algorithms for cognitive radio applications. Em *IEEE Communications Surveys Tutorials*, págs. 116–130, 2009.

7 ANEXOS

7.1 RESULTADOS DAS SIMULAÇÕES DO MECANISMO PROPOSTO

Opção do US Legítimo	E_v (Valor das Simulações)	E_v (Valor Analítico)	Diferença (%)
(1,1)	0,572	0,5714	0,04
(1,2)	0,696	0,6964	-0,02
(1,3)	0,735	0,7350	0,05
(1,4)	0,747	0,7471	-0,05
(1,5)	0,749	0,7500	-0,11
(1,6)	0,750	0,7500	0,02
(1,7)	0,750	0,7500	-0,01
(2,1)	0,697	0,6964	0,04
(2,2)	0,861	0,8600	0,07
(2,3)	0,911	0,9107	0,05
(2,4)	0,926	0,9257	0,03
(2,5)	0,929	0,9286	0,01
(2,6)	0,929	0,9286	0,01
(3,1)	0,734	0,7350	-0,07
(3,2)	0,911	0,9107	-0,01
(3,3)	0,964	0,9643	0,02
(3,4)	0,979	0,9793	0,00
(3,5)	0,982	0,9821	0,00
(4,1)	0,747	0,7471	-0,04
(4,2)	0,925	0,9257	-0,03
(4,3)	0,979	0,9793	-0,01
(4,4)	0,994	0,9943	0,01
(5,1)	0,749	0,7500	-0,07
(5,2)	0,929	0,9286	0,03
(5,3)	0,982	0,9821	0,01
(6,1)	0,750	0,7500	0,00
(6,2)	0,929	0,9286	0,00
(7,1)	0,750	0,7500	-0,04

TAB. 7.1: Comparação dos Valores da p_{trans} das Simulções com os Valores Analíticos

Opção do US Legítimo	E_v (Valor das Simulações)	E_v (Valor Analítico)	Diferença (%)
(1,1)	0,572	0,571	0,04
(1,2)	1,143	1,143	0,05
(1,3)	1,716	1,714	0,10
(1,4)	2,286	2,286	0,01
(1,5)	2,854	2,857	-0,12
(1,6)	3,429	3,429	0,00
(1,7)	3,999	4,000	-0,02
(2,1)	0,697	0,696	0,04
(2,2)	1,394	1,393	0,08
(2,3)	2,091	2,089	0,10
(2,4)	2,787	2,786	0,06
(2,5)	3,482	3,482	-0,01
(2,6)	4,179	4,179	0,01
(3,1)	0,734	0,735	-0,07
(3,2)	1,471	1,470	0,04
(3,3)	2,206	2,205	0,02
(3,4)	2,940	2,940	0,01
(3,5)	3,675	3,675	0,01
(4,1)	0,747	0,747	-0,04
(4,2)	1,494	1,494	-0,03
(4,3)	2,243	2,241	0,05
(4,4)	2,988	2,989	0,00
(5,1)	0,749	0,750	-0,07
(5,2)	1,500	1,500	-0,02
(5,3)	2,250	2,250	0,02
(6,1)	0,750	0,750	0,00
(6,2)	1,501	1,500	0,06
(7,1)	0,750	0,750	-0,04

TAB. 7.2: Comparação dos Valores da E_v das Simulções com os Valores Analíticos

Observa-se que os valores obtidos nas simulações encontram-se em um intervalo de confiança de 95%.