

MARINHA DO BRASIL
DIRETORIA DE ENSINO DA MARINHA
CENTRO DE INSTRUÇÃO ALMIRANTE ALEXANDRINO

CURSO DE APERFEIÇOAMENTO AVANÇADO EM
GUERRA ELETRÔNICA

TRABALHO DE CONCLUSÃO DE CURSO

O RÁDIO DEFINIDO POR *SOFTWARE* NA GUERRA ELETRÔNICA: o potencial de
rádios definidos por *software* e de rádios cognitivos contra ações de bloqueio



PRIMEIRO-TENENTE MATHEUS LUIZI NAZAR

Rio de Janeiro
2023

PRIMEIRO-TENENTE MATHEUS LUIZI NAZAR

O RÁDIO DEFINIDO POR *SOFTWARE* NA GUERRA ELETRÔNICA: o potencial de
rádios definidos por *software* e de rádios cognitivos contra ações de bloqueio

Monografia apresentada ao Centro de Instrução
Almirante Alexandrino como requisito parcial à
conclusão do Curso de Aperfeiçoamento Avançado em
Guerra Eletrônica.

Orientadores:

Prof. Guilherme Ribeiro Colen, DSc

Capitão-Tenente Willian Sathler Lino Soares, MSc

CIAA
Rio de Janeiro
2023

PRIMEIRO-TENENTE MATHEUS LUIZI NAZAR

O RÁDIO DEFINIDO POR *SOFTWARE* NA GUERRA ELETRÔNICA: o potencial de
rádios definidos por *software* e de rádios cognitivos contra ações de bloqueio

Monografia apresentada ao Centro de Instrução Almirante Alexandrino como requisito parcial
à conclusão do Curso de Aperfeiçoamento Avançado em Guerra Eletrônica.

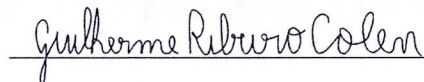
Aprovada em 23/11/2023

Banca Examinadora:

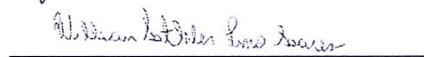
CF Robson Ribeiro Carreira, DSc – CIAA



Prof. Guilherme Ribeiro Colen, DSc – CIAA



CT Willian Sathler Lino Soares, MSc – CASOP



Prof.^a Beatriz Alencar Ribeiro, MSc – CIAA



AGRADECIMENTOS

Agradeço a Deus, pelo dom da vida e pela saúde que me concede para exercer minha profissão dia após dia.

Agradeço à minha esposa, Isabela, pelo amor e suporte contínuos em toda a minha trajetória profissional, bem como nas demais áreas de minha vida.

Agradeço ao Prof. Dr. Guilherme Ribeiro Colen, orientador acadêmico e coordenador do C-ApA-GE, pelas instruções seguras a respeito da organização e das abordagens realizadas neste trabalho.

Agradeço ao Capitão-Tenente Willian Sathler Lino Soares, orientador técnico, pelas orientações fornecidas para a execução deste trabalho, orientações estas que foram extremamente úteis para balizar e delimitar um tema tão abrangente, com diversos assuntos em potencial para exploração.

O RÁDIO DEFINIDO POR SOFTWARE NA GUERRA ELETRÔNICA: o potencial de rádios definidos por software e de rádios cognitivos contra ações de bloqueio

Resumo

As comunicações militares são essenciais para o comando, controle e ações táticas no campo de batalha. No entanto, essas comunicações podem ser alvo de interferências indesejadas e maliciosas, como por exemplo o bloqueio eletrônico. O bloqueio eletrônico é uma técnica que utiliza a irradiação de sinais eletromagnéticos para interromper ou degradar as comunicações, e pode ser empregado para impedir que as forças militares se comuniquem entre si. Para garantir a segurança das comunicações militares em um ambiente com a presença de bloqueio eletrônico, é necessário dispor de medidas eficazes contra estes bloqueios. Possíveis soluções para se contrapor a ele são os rádios definidos por *software* (RDS) e os rádios cognitivos. Os RDS são uma tecnologia que permite alterar a funcionalidade do rádio por meio de *software*, o que permite maior flexibilidade e interoperabilidade. Já os rádios cognitivos são uma evolução aos RDS. Eles possuem a capacidade de perceber o ambiente eletromagnético no qual estão operando e se adaptar a ele para executar comunicações eficazes e seguras.

Palavras- chave: rádio definido por *software*, rádio cognitivo, guerra eletrônica, bloqueio.

LISTA DE FIGURAS

Figura 2.1 – Diagrama em blocos de um sistema de comunicações típico	20
Figura 2.2 – RDS ideal conforme descrito por Mitola	21
Figura 2.3 – Diagrama de um RDS	21
Figura 2.4 – diagrama em blocos de um RDS moderno	22
Figura 2.5 (a) – Processamento no RDS ideal	23
Figura 2.5 (b) – Processamento no RDS real	23
Figura 4.1 – Diferença no uso das bandas de TV analógica e TV digital	26
Figura 4.2 – Aplicação dos rádios cognitivos como SU.....	27
Figura 4.3 – Ilustração sobre o uso dos canais licenciados por SU ao longo do tempo	28
Figura 4.4 – Ilustração da técnica FFHSS.....	30
Figura 4.5 – Ilustração da técnica SFHSS.....	30
Figura 4.6 – Esquema de transmissão e mudança de canal do rádio cognitivo	31
Figura 4.7 – Probabilidade de sucesso do bloqueio de ponto contra rádios cognitivos	32
Figura 4.8 – probabilidade de sucesso do bloqueio de barragem contra rádios cognitivos	33
Figura 4.9 – probabilidade de sucesso do bloqueio inteligente contra rádios cognitivos	35

LISTA DE SIGLAS E ABREVIATURAS

A/D	Analógico-digital
D/A	Digital-analógico
DARPA	<i>Defense Advanced Research Projects Agency</i>
DSSS	<i>Direct Sequence Spread Spectrum</i>
DSP	<i>Digital Signal Processor</i>
EEM	Espectro Eletromagnético
FFHSS	<i>Fast Frequency-Hopping Spread Spectrum</i>
FHSS	<i>Frequency-Hopping Spread Spectrum</i>
FPGA	<i>Field Programmable Gate Arrays</i>
GE-COM	Guerra Eletrônica de Comunicações
GPP	<i>General Purpose Processors</i>
HF	<i>High-Frequency</i>
ICNIA	<i>Integrated Communications, Navigation and Identification Architecture</i>
IEEE	<i>Institute of Electrical and Electronics Engineers</i>
LPI	<i>Low Probability of Interception</i>
LPD	<i>Low Probability of Detection</i>
MAE	Medidas de Ataque Eletrônico
MAE-COM	Medidas de Ataque Eletrônico em Comunicações
MAGE	Medidas de Apoio à Guerra Eletrônica
MAGE-COM	Medidas de Apoio à Guerra Eletrônica em Comunicações
MPE	Medidas de Proteção Eletrônica
MPE-COM	Medidas de Proteção Eletrônica em Comunicações

OTAN	Organização do Tratado do Atlântico Norte
P&D	Pesquisa e Desenvolvimento
PU	<i>Primary User</i>
RDS	Rádio Definido por <i>Software</i>
SATURN	<i>Second Generation Anti-Jam Tactical Ultra-High Frequency Radio</i>
SCA	<i>Software Communication Architecture</i>
SFHSS	<i>Slow Frequency-Hopping Spread Spectrum</i>
SS	<i>Spread Spectrum</i>
SU	<i>Secondary User</i>
TVWS	<i>Television White Spaces</i>
UHF	<i>Ultra-High Frequency</i>
UIT	União Internacional de Telecomunicações
VHF	<i>Very-High Frequency</i>

SUMÁRIO

1 INTRODUÇÃO	10
1.1 Apresentação do Problema	11
1.2 Justificativa e Relevância	12
1.3 Objetivos	13
1.3.1 Objetivo Geral	14
1.3.2 Objetivos Específicos	14
2 REFERENCIAL TEÓRICO	15
2.1 Conceitos iniciais sobre guerra eletrônica	15
2.2 Conceitos básicos sobre bloqueio eletrônico	16
2.2.1 Bloqueio de ponto	16
2.2.2 Bloqueio de barragem	16
2.2.3 Bloqueio de varredura	16
2.2.4 Bloqueio seguidor	17
3 METODOLOGIA	18
3.1 Classificação da Pesquisa	18
3.1.1 Classificação Quanto aos Fins	18
3.1.2 Classificação Quanto aos Meios	18
3.2 Limitações do Método	18
4 SOLUÇÕES DE RÁDIO CONTRA BLOQUEIOS	19
4.1 Rádio Definido por Software	19
4.1.1 Histórico	19
4.1.2 Tecnologia RDS	19
4.1.3 Vantagens e desvantagens do RDS	23
4.1.4 RDS como solução para bloqueio	24
4.2 Rádio Cognitivo	24
4.2.1 TV <i>White Spaces</i>	26
4.2.2 Uso dos rádios cognitivos em aplicações militares	28
4.2.3 Rádios cognitivos empregados contra bloqueio de ponto	32
4.2.4 Rádios cognitivos empregados contra bloqueio de barragem	33

4.2.5 Rádios cognitivos empregados contra bloqueios de varredura e seguidor	34
5 CONCLUSÃO	36
5.1 Considerações Finais	36
5.2 Sugestões para futuros trabalhos	37
REFERÊNCIAS	38
ANEXO	40

1 INTRODUÇÃO

Ao longo da história, a tática militar sempre envolveu o uso de medidas para combater o inimigo e de contramedidas para se proteger de ataques. Atualmente, esta verdade é bastante clara no campo de guerra eletrônica e, mais especificamente, na guerra de comunicações. Técnicas e equipamentos de Medidas de Apoio de Guerra Eletrônica de Comunicações (MAGE-COM) e de Medidas de Ataque Eletrônico em Comunicações (MAE-COM) são utilizadas para, respectivamente, interceptar e negar (ou degradar) o uso do espectro eletromagnético (EEM) por parte do oponente. Enquanto estas técnicas são difíceis de ser implementadas contra sistemas de comunicações cujos meios de transmissão sejam físicos, como o fio elétrico, quando se transmite sinais de comunicações no espaço tais interceptações e ataques se tornam bem mais factíveis (Poisel, 2002).

Comunicações por fios são difíceis de ser implementadas num campo de batalha, e impossíveis caso este campo de batalha seja o mar. Como resultado disso, as comunicações militares devem dispor de métodos eficientes para assegurar o uso do EEM por equipamentos de comunicações. Tais métodos são chamados de Medidas de Proteção Eletrônica (MPE) e englobam criptografia, autenticação de mensagem, modificação dos parâmetros dos sinais transmitidos, entre outros (Poisel, 2002). Todas estas técnicas possuem como objetivo a consecução um dos fatores principais em operações militares, que é a obtenção de superioridade de comunicações, termo utilizado no documento STO-TR-IST-140 da Organização do Tratado do Atlântico Norte (OTAN). Tal superioridade demanda comunicações confiáveis, eficientes e robustas.

Uma das MAE-COM empregadas é o bloqueio (*jamming*), cujo propósito é prevenir que um sinal de comunicação chegue no receptor. O bloqueio das comunicações num cenário de guerra pode acarretar no subemprego da Força, bem como degradar a capacidade de Comando e Controle (Wilgenbusch; Heisig, 2013). Isso significa que a Força deve possuir sistemas de comunicações capazes de ser utilizados eficazmente na presença de um ambiente saturado por bloqueio. Nesta situação, os RDS e os rádios cognitivos – que constituem uma tecnologia sucessora ao RDS – podem se apresentar como uma boa solução.

RDS é um equipamento rádio no qual algumas de suas funções são realizadas por meio de *software* ao invés de *hardware*, o que fornece maior flexibilidade de operação. Essa maior flexibilidade pode significar uma vantagem em comunicações na presença de atores hostis. Já o rádio cognitivo pode ser definido como um RDS que compreende o ambiente

eletromagnético no qual está inserido e, assim, é capaz de se adaptar a este ambiente de modo a realizar comunicações de maneira eficiente e inteligente.

Normalmente, o interesse em rádios cognitivos é voltado para a eficiência no uso do EEM, que é um recurso escasso e limitado, por meio de técnicas de acesso dinâmico ao espectro. No entanto, o uso de rádios cognitivos pode resultar, também, em superioridade de comunicações num ambiente de guerra, não só pelo uso eficiente do EEM, mas também pelo seu potencial em manter comunicações seguras na presença de interferidores inimigos, como os bloqueadores.

Finalmente, não obstante o fato de muitas bibliografias e artigos tratarem os rádios cognitivos como uma tecnologia futura, há relatos de uso destes equipamentos na guerra entre Rússia e Ucrânia (Bisht, 2023). Tais relatos citam este equipamento como sistemas capazes de elevar a proteção contra interferências através da capacitação de se contrapor a bloqueios e outras técnicas de guerra eletrônica empregadas pelos adversários.

1.1 Apresentação do Problema

As informações durante uma batalha são necessárias para coordenação de operações conjuntas, intercâmbio de informações sensíveis ao combate, apoios logísticos, informações sobre condições operativas dos meios, dentre outros motivos. O bloqueio das comunicações, quando realizado com sucesso, impede que os Comandantes de Forças ou Unidades empreguem e controlem os meios a eles subordinados de maneira eficaz. Adicionalmente, a aplicação inteligente do bloqueio pode não ser percebida por um longo período, como por exemplo quando a degradação das comunicações é atribuída a mau funcionamento do equipamento (Wilgenbusch; Heisig, 2013).

O bloqueio é um elemento importante em qualquer plano de negação de comunicações. Seu custo é baixo e a operação é simples (Wilgenbusch; Heisig, 2013). Além disso, ele pode ser utilizado por meio de diferentes técnicas, que serão abordadas ao longo deste trabalho. Desta forma, a ausência de meios para se proteger contra ações de bloqueio é um fator preocupante.

Na contramão do que ocorre com os equipamentos rádios civis, os sistemas militares são muitas vezes antigos, pelo fato de possuírem um longo ciclo de vida e, também, devido ao alto custo de aquisição em grandes quantidades de novos equipamentos. Esses rádios, em grande parte convencionais, possuem limitações nas frequências de operação, poucas opções de potência de transmissão (às vezes há apenas uma potência) e capacidades

restritas de modulação. Estas limitações implicam em pouca flexibilidade de operação (H. Saarnisaari; T. Braysy, 2017).

A Marinha do Brasil ainda depende muito desses rádios convencionais em suas comunicações táticas, o que as torna bastante vulneráveis ao bloqueio. Surge, então, a necessidade de eliminar, ou ao menos mitigar, o problema do bloqueio. A solução para alcançar esta eliminação ou mitigação pode ser encontrada na utilização de rádios mais flexíveis, como o RDS e o rádio cognitivo (que é baseado em RDS).

De fato, o RDS tem sido um desenvolvimento inovador em plataformas rádio, e tem permitido a operação dos equipamentos em bandas de frequência mais amplas, bem como melhoria na capacidade de processamento dos sinais recebidos. Desta forma, estes equipamentos são mais eficazes na detecção e na classificação de ameaças. Estes rádios podem, também, suportar diferentes formas de onda, aumentando sua robustez e flexibilidade, como é o caso do RDS *Falcon III AN/PRC-152A*, da fabricante *Harris* (H. Saarnisaari; T. Braysy, 2017).

1.2 Justificativa e Relevância

A Pesquisa e Desenvolvimento (P&D) em rádios é necessária devido a necessidade de meios de comunicações táticos sofisticados, eficientes e seguros, conforme evidenciado por documentos que balizam o pensamento estratégico das Forças Armadas, como a Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional. Contudo, é importante ressaltar que a P&D é uma alternativa à obtenção de equipamentos no mercado. Sendo assim, é necessário avaliar se há realmente vantagem em se estabelecer P&D em rádios (Filho; Galdino; Moura, 2017).

As desvantagens envolvem o custo elevado, bem como o longo prazo necessário a todo o ciclo de P&D, o que pode tornar este processo inadequado para soluções de curto prazo. No entanto, em se tratando de rádios cognitivos e, conseqüentemente, de RDS, há desvantagens na obtenção de tais equipamentos no mercado internacional. Primeiramente, dada a natureza do equipamento, ao longo da vida útil do equipamento podem ser necessárias atualizações de software, o que pode implicar numa dependência estratégica do fornecedor. Outra desvantagem consiste na ameaça cibernética. Pode ser difícil saber quais softwares existem no equipamento, que podem ter sido intencionalmente instalados pelo fabricante estrangeiro. Adicionalmente, o sistema está sujeito a ataques cibernéticos externos, cujos efeitos podem ser extremamente negativos caso não haja um sistema de defesa cibernética

adequado. Desta forma, conclui-se que o Brasil não pode depender de fornecedores estrangeiros, e produtos nacionais são a melhor opção para atender às necessidades operativas no futuro (Filho; Galdino; Moura, 2017).

O Brasil possui o Programa RDS-Defesa, com coordenação do Exército Brasileiro. Embora a escolha pelo programa tenha focado no RDS, uma evolução natural de P&D neste projeto é a investigação dos rádios cognitivos (Filho; Galdino; Moura, 2017). Há, inclusive, uma portaria deste ano do Chefe do Departamento de Ciência e Tecnologia do Exército, aprovando as necessidades de conhecimentos específicos da linha de ensino militar científico-tecnológico para o ano de 2024 (PORTARIA – DCT/C Ex Nº 007 de 27 de janeiro de 2023), que prevê seis vagas em cursos de Mestrado e Doutorado na área de RDS e rádios cognitivos (Brasil, 2023).

Para o Brasil se manter no estado da arte em comunicações, é necessário acompanhar as evoluções tecnológicas da área. Monteiro (2019) afirma que a tecnologia de radiocomunicações iniciou com comunicações analógicas, seguidas pelas comunicações digitais, ambos implementados em hardware. O passo seguinte às comunicações digitais, e atual estágio de evolução das radiocomunicações, são os RDS, no qual os componentes, outrora implementados em *hardware*, passam a ser implementados em *software*, melhorando as capacidades de interoperabilidade e portabilidade de formas de onda. O RDS serve, também, de plataforma de desenvolvimento para os rádios cognitivos. Assim, a evolução natural será um futuro no qual rádios cognitivos se tornarão protagonistas em termos de tecnologia.

Embora possa não ser factível uma implementação de rádios cognitivos no meio militar em um curto prazo, fomentar este assunto em termos de pesquisa, estudo e desenvolvimento pode trazer benefícios e possibilitar sua implementação em médio ou longo prazo. Desta forma, este trabalho visa trazer para a Marinha conhecimentos sobre essa evolução tecnológica que, como será demonstrado, tem um grande potencial para mitigar bloqueios em comunicações e, desta forma, melhorar a superioridade nas comunicações.

1.3 Objetivos

O objetivo deste trabalho é apresentar sistemas que figurem como soluções de radiocomunicações a fim de manter comunicações seguras e eficazes na presença de um ambiente sujeito a interferências inimigas.

1.3.1 Objetivo Geral

Diante, por um lado, das limitações impostas por interferências maliciosas indesejadas aos equipamentos rádios convencionais e, por outro lado, da necessidade de manter comunicações seguras e confiáveis num ambiente de guerra, o objetivo deste trabalho é apresentar os RDS e os rádios cognitivos como equipamentos capazes de manter comunicações eficazes na presença de determinados tipos de bloqueio, de modo a fomentar e estimular a P&D destes sistemas, que podem ser implementados nos meios navais no médio e no longo prazo.

1.3.2 Objetivos Específicos

- Mostrar que o RDS é um sistema eficaz para manter comunicações na presença de bloqueio, por meio de técnicas de salto em frequência.
- Apresentar o rádio cognitivo como uma tecnologia sucessora ao RDS, capaz de manter comunicações eficazes na presença do bloqueio, através do sensoriamento automático do ambiente eletromagnético no qual está operando, e posterior alteração nos parâmetros de operação do equipamento, também efetuada automaticamente.

2 REFERENCIAL TEÓRICO

Após extensa pesquisa pela bibliografia disponível a respeito de guerra eletrônica, as referências selecionadas para basear este capítulo foram do autor Richard A. Poisel (2002, 2011), por fornecerem uma visão abrangente e completa sobre os principais conceitos necessários a este trabalho.

2.1 Conceitos básicos sobre guerra eletrônica

Guerra Eletrônica (GE) e Guerra Eletrônica de Comunicações (GE-COM): GE pode ser definida como o conjunto de ações militares que visam controlar o espectro eletromagnético, a fim de obter informações sobre o seu uso pelo inimigo, negar seu uso ao inimigo e garantir seu uso pelas próprias forças. GE-COM é o nome que levam essas ações quando elas se referem especificamente a sistemas de comunicações, e não a sensores de um modo geral (Poisel, 2002).

É geralmente aceito que GE possui três componentes distintas: Medidas de Apoio à Guerra Eletrônica (MAGE), Medidas de Ataque Eletrônico (MAE) e Medidas de Proteção Eletrônica (MPE). Da mesma forma que o conceito de GE e GE-COM, quando as atividades de MAGE, MAE e MPE são abordadas exclusivamente no contexto de comunicações, recebem o nome de Medidas de Apoio à Guerra Eletrônica de Comunicações (MAGE-COM), Medidas de Ataque Eletrônico de Comunicações (MAE-COM) e Medidas de Proteção Eletrônica de Comunicações (MPE-COM) (Poisel, 2002).

MAGE-COM é a atividade que consiste em detectar os sinais irradiados de uma fonte inimiga a fim de obter informações sobre o oponente. Trata-se de uma atividade passiva, com o intuito de coletar parâmetros dos sinais interceptados, como frequência de operação e tipo de modulação. Essa atividade permite correlacionar fontes de transmissão com plataformas oponentes, desde que haja um conhecimento de inteligência prévio sobre as características das fontes emissoras do inimigo (Poisel, 2002).

MAE-COM é a atividade que visa negar ou reduzir o uso do EEM pelo inimigo. Isso pode ser realizado por meio de ações como armas de energia direcionada ou bloqueios eletrônicos (Poisel, 2011).

MPE-COM é a atividade cujo objetivo é garantir o uso do EEM por parte de Forças Amigas. Basicamente, visa reduzir a eficácia do oponente em conduzir atividades de MAGE-COM ou MAE-COM (Poisel, 2011).

2.2 Conceitos básicos sobre bloqueio eletrônico

Conforme citado, o bloqueio integra as ações de MAE-COM. Um bloqueador pode utilizar diferentes estratégias, cada uma com suas vantagens e limitações. Uma importante peculiaridade do bloqueio eletrônico em comunicações é que o bloqueio é sempre dirigido ao receptor, nunca ao transmissor. A bibliografia sugere quatro tipos principais de bloqueio empregados em comunicações: bloqueio de ponto, bloqueio de barragem, bloqueio de varredura e bloqueio seguidor (Poisel, 2002), (Poisel, 2011).

2.2.1 Bloqueio de ponto

O bloqueio de ponto emprega toda a potência do bloqueador em um único canal de comunicações. Essa alta densidade de energia implica na vantagem de que, se o canal correto for selecionado, o bloqueio pode ser bastante eficaz para negar as comunicações entre transmissor e receptor. No entanto, algumas técnicas de comunicações, como a mudança rápida de frequência, podem tornar este tipo de bloqueio ineficaz.

2.2.2 Bloqueio de barragem

O bloqueio de barragem transmite ruído em toda a banda do espectro de frequência que se espera que seja utilizado pelo transmissor, ou seja, ele possui a vantagem de ser dirigido simultaneamente a muitos canais. No entanto, como a potência é espalhada em todo o espectro, a densidade de potência pode ser bem reduzida. Essa redução na densidade de potência pode resultar em um bloqueio não eficaz para negar as comunicações entre o transmissor e o receptor, mas pode reduzir a distância na qual essas comunicações são efetivas, por meio do aumento do nível de ruído no receptor.

2.2.3 Bloqueio de varredura

O bloqueio de varredura mistura alguns conceitos dos bloqueios de ponto e de barragem. Assim como no bloqueio de ponto, a energia é toda empregada em um único canal, ou numa banda estreita de frequência. No entanto, ao longo do tempo, o sinal bloqueador varre diversos canais ou diversas pequenas bandas de frequência, e isso pode ser realizado num curto período de tempo.

2.2.4 Bloqueio seguidor

O bloqueio seguidor possui a característica de tentar localizar (ou seguir) o salto em frequência do transmissor, de modo a poder bloquear a frequência que está sendo utilizada pelo transmissor em determinado instante. O bloqueio ocorre com toda a energia direcionada em um canal apenas. Sua implementação é de alta complexidade.

3 METODOLOGIA

3.1 Classificação da Pesquisa

3.1.1 Quanto aos fins

Este trabalho é classificado, quanto aos fins, em exploratório, pois se baseia em extensa pesquisa bibliográfica a livros e artigos a respeito do tema, a fim de explorar um assunto ainda não muito difundido na Marinha do Brasil.

3.1.2 Quanto aos meios

Quanto aos meios, este trabalho é classificado como de pesquisa bibliográfica, tendo em vista que o meio principal de pesquisa são diversos artigos científicos, bem como algumas bibliografias vastamente utilizadas no meio acadêmico referentes ao tema.

3.2 Limitações do Método

Embora haja artigos interessantes sobre a aplicação civil dos rádios cognitivos, as publicações de pesquisas a respeito deste sistema no meio militar ainda são escassas. Adicionalmente, por serem equipamentos de tecnologia complexa, não há *datasheet* disponível em fonte aberta de equipamentos militares de rádios cognitivos, tornando difícil obter conhecimento dos parâmetros de funcionamento exatos deste sistema, o que se constitui numa importante informação necessária para realizar simulações.

Outras limitações são a escassez de resultados reais ou de simulações da eficácia de redes de rádios cognitivos na presença de todos os tipos de bloqueio definidos no item 2.2. Sendo assim, para analisar a eficácia dos rádios cognitivos contra os bloqueios de varredura e seguidor, foram utilizados dados bibliográficos teóricos, bem como resultados de uma simulação com um tipo de bloqueio parecido.

4 SOLUÇÕES DE RÁDIO CONTRA BLOQUEIOS

4.1 Rádio Definido por *Software*

4.1.1 Histórico

A década de 90 foi um marco na transição dos rádios implementados em hardware para rádios implementados em software. O *Integrated Communications, Navigation and Identification Architecture* (ICNIA), dos Estados Unidos da América, foi um sistema que integrava componentes para comunicações, navegação e identificação de aeronaves. Esses componentes eram compostos por módulos substituíveis. Assim, este foi o primeiro sistema a possuir algumas das funcionalidades do RDS que é conhecido hoje (Dabcevic, 2015).

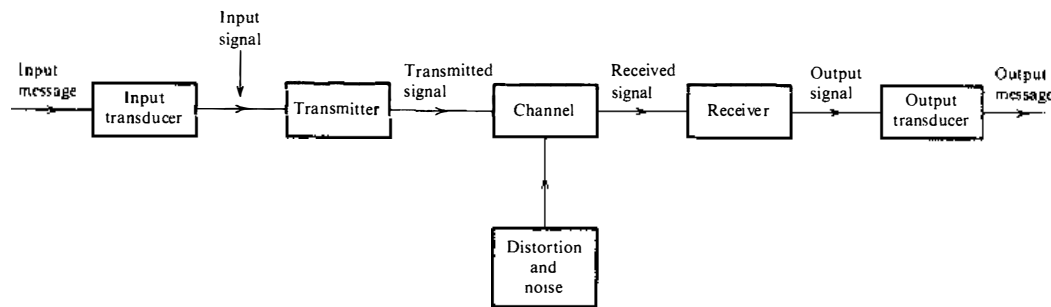
O termo RDS foi introduzido pela primeira vez por Joseph Mitola, em 1991, e foi considerado como um equipamento capaz de possuir interoperabilidade com vários serviços de comunicações e suas respectivas faixas de frequência. Pela alteração de seu algoritmo de funcionamento, o equipamento é capaz de se reconfigurar automaticamente para o sinal apropriado (Mitola, 2003).

O *SpeakEasy* e o *SpeakEasy II* foram projetos do Departamento de Defesa dos EUA com o objetivo de desenvolver um sistema de comunicações utilizando RDS. Estes projetos convergiram para o *Joint Tactical Radio System* (JTRS), um projeto que visava integrar os equipamentos rádio militares dos EUA em RDS. O projeto foi descontinuado, mas deixou como legado o *Software Communication Architecture* (SCA), uma arquitetura aberta que é utilizado no projeto de RDS militares (Dabcevic, 2015).

4.1.2 Tecnologia RDS

Para se chegar ao entendimento do funcionamento de um RDS, é necessário conhecer a estrutura de equipamentos rádio convencionais. Há diferentes sistemas de comunicações existentes. De acordo com Lathi; Zhi Ding (2010), a melhor maneira de entender um sistema de comunicações é estudando um diagrama de blocos que, embora genérico, seja comum a praticamente todos os sistemas. A partir desse conhecimento básico, consegue-se analisar novos e diferentes equipamentos. Um sistema de comunicações típico com suas funcionalidades, está mostrado na Figura 2.1.

Figura 2.1: diagrama em blocos de um sistema de comunicações típico.



Fonte: Lathi; Zhi Ding, 2010

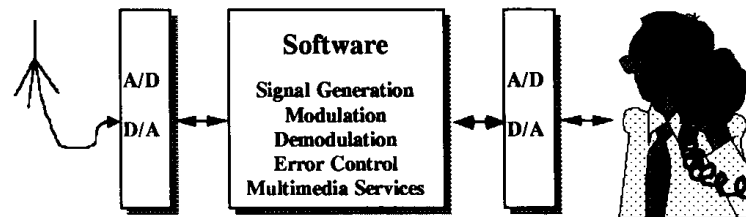
Mensagem de entrada (*input message*): é uma mensagem que se deseja que seja transmitida. Se essa mensagem não for elétrica (por exemplo, a voz humana), ela é convertida pelo transdutor de entrada (*input transceiver*) para o formato de um sinal elétrico em forma de onda. Este sinal é o sinal de entrada (*input signal*) ou sinal em banda-base.

O transmissor (*transmitter*) é responsável por transmitir o sinal. No entanto, normalmente, o sinal não é transmitido em banda-base. Ele é sujeito a manipulações de modo a ser transmitido da maneira mais eficiente. Assim, o transmissor pode ser constituído de conversor analógico-digital (A/D), codificador e modulador. O sinal será transmitido pelo canal de comunicações (*channel*). Neste trabalho, o canal de comunicações é o espaço livre.

O sinal transmitido chega ao receptor (*receiver*), que é responsável por realizar o caminho inverso das modificações realizadas no transmissor, bem como remover as distorções e ruídos presentes no canal de comunicações. Para isso, o receptor pode ser constituído de demoduladores, decodificadores e conversor digital-analógico (D/A). Este sinal, novamente em banda-base, chega ao transdutor de saída (*output transducer*), onde é convertido para sua forma original, a mesma da mensagem de entrada.

Um RDS é um sistema no qual alguns dos componentes apresentados acima são implementados por um software. Mitola considerou o diagrama da Figura 2.2 como um RDS ideal. Os conversores A/D e D/A próximos à antena e ao usuário permitem que as funções de transmissão, recepção, geração do sinal, modulação, demodulação, codificação, decodificação e controle sejam realizados em software (Mitola, 2003).

Figura 2.2: RDS ideal conforme descrito por Mitola.

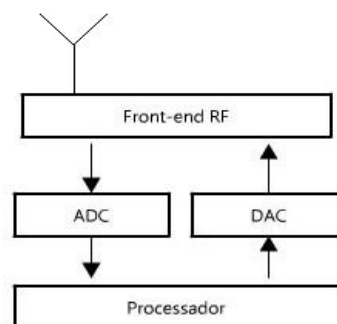


Fonte: Mitola, 2003

A implementação em *software* dos componentes rádio tornam o RDS um equipamento mais flexível, se comparado à implementação via *hardware*. A evolução dos sistemas rádio e as necessidades cada vez maiores de sistemas de comunicações seguros, adaptáveis às condicionantes operacionais e que possam ser reconfigurados para emprego em diferentes cenários de comunicações, resultaram no surgimento do RDS (Filho; Galdino; Moura, 2017).

Um RDS ideal teria todos os modos de RF definidos em *software*, ou seja, ele consistiria apenas de antena, conversores A/D e D/A, e um processador programável. Desta forma, ele seria muito parecido com o proposto por Mitola, e eliminaria praticamente todo o *hardware*, restando apenas os conversores A/D e D/A. O conversor A/D, neste caso, seria utilizado para amostrar o sinal de rádio da antena. Lopes (2013) afirma que não existem conversores A/D capazes de amostrar toda a faixa de frequências utilizada e, por isso, em um RDS, é necessário haver algum grau de implementação em *hardware*, compondo aquilo que é chamado de *front-end* de RF, que tem como função converter o sinal de interesse (em frequências mais altas) para uma frequência intermediária (mais baixa). Assim, um RDS teria uma configuração parecida com a da Figura 2.3.

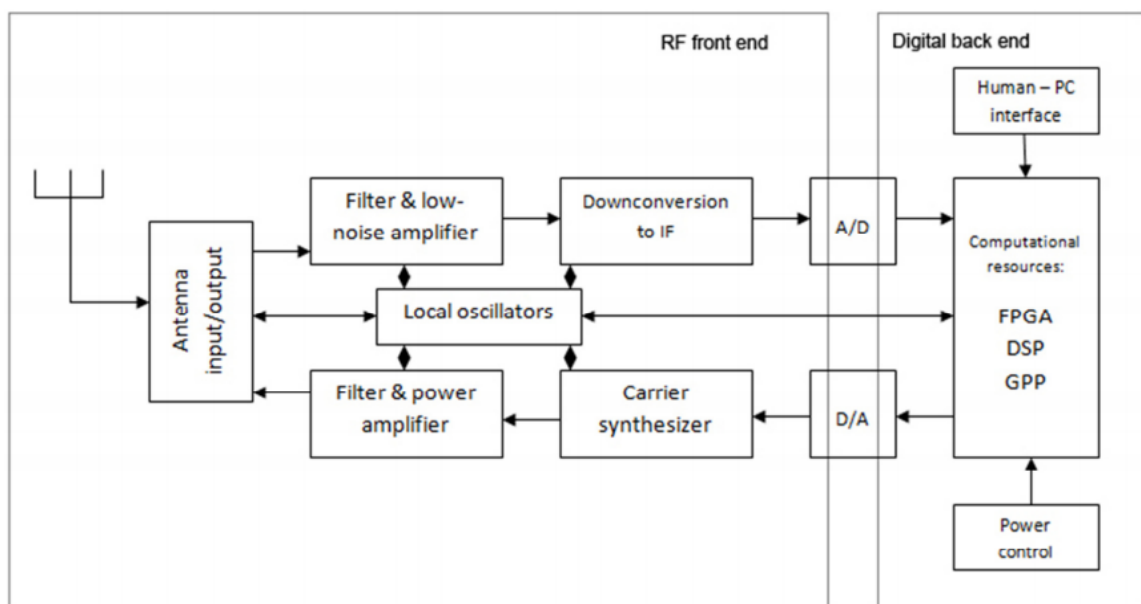
Figura 2.3: diagrama de um RDS.



Fonte: Garcia Reis, 2012

Tem-se, até aqui, o entendimento dos passos a serem realizados para reduzir a frequência do sinal recebido a uma frequência intermediária. Esses passos podem ser exemplificados da seguinte forma: consideremos um sinal de voz que será transmitido por um transceptor de radiocomunicações qualquer e será recebido por um RDS. O sinal de voz por si só possui uma banda-base, que é a faixa de frequências que contém o sinal da voz. Essa informação de voz precisa modular uma onda portadora, de frequência muito maior, para poder ser transmitida como onda eletromagnética no espaço livre. O sinal recebido pelo RDS é o da onda portadora modulada, em alta frequência. O *front-end* de RF é responsável por reduzir esse sinal para uma frequência menor, que é a frequência intermediária. Esse sinal, na frequência intermediária, será convertido em sinal digital e será passado para o processador, que é a camada em software do RDS. Assim, o processamento é feito pelos recursos computacionais como *General Purpose Processors* (GPP), *Digital Signal Processor* (DSP) e *Field Programmable Gate Arrays* (FPGA), ou uma combinação deles. Esses recursos computacionais são responsáveis pela etapa de frequência intermediária para banda-base (*digital down converter*) e vice-versa (*digital up converter*). A Figura 2.4 mostra de maneira mais detalhada o diagrama de um RDS moderno. Pode-se perceber que o *front-end* de RF consiste de antena, amplificadores, filtros, osciladores locais e conversores A/D e D/A (Dabcevic, 2015).

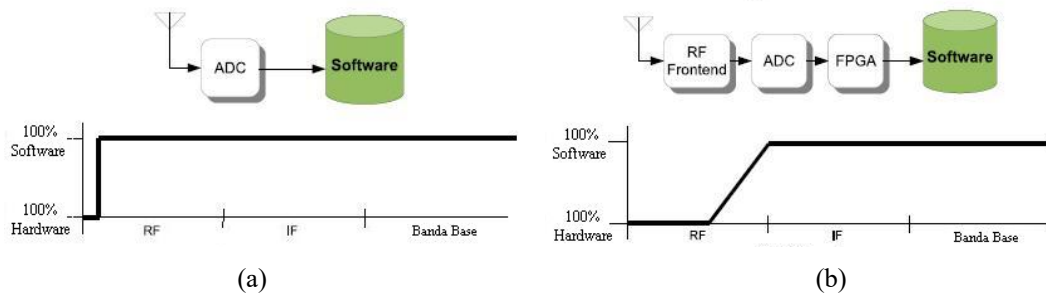
Figura 2.4: diagrama em blocos de um RDS moderno.



Fonte: Dabcevic, 2015

Lopes (2013) fornece uma ilustração bastante elucidativa sobre a diferença entre o RDS ideal e o RDS real. Percebe-se que na Figura 2.5 (a), representativa do RDS ideal, todas as funções são realizadas por *software*, diferente do RDS real, mostrado na Figura 2.5 (b), em que a conversão do sinal de RF para frequência intermediária é realizada por *hardware*.

Figura 2.5: processamento no RDS ideal (a) e processamento no RDS real (b).



Fonte: Lopes, 2013

4.1.3 Vantagens e desvantagens do RDS

O RDS é um meio pelo qual se pode estabelecer padrões de comunicações. O rádio tradicional só pode ser modificado por intervenção física em seus componentes, enquanto que o RDS permite que suas propriedades como frequência da portadora, largura de banda do sinal e modulação sejam definidas por *software*. Desta forma, o RDS permite reprogramação dos seus parâmetros, adoção de novas funcionalidades, possibilidade de o *software* ser reutilizado entre os rádios, maior facilidade de desenvolvimento que um ambiente de *software* possui e redução da complexidade do *hardware* dos sistemas rádio, ficando este limitado somente à implementação do *front-end* de RF (Garcia Reis, 2012), (Lopes, 2013).

Além dessa flexibilidade, outros benefícios do RDS são o fato de serem mais robustos a variações de temperatura e degradação de seus componentes pelo tempo, já que o processamento não mais está correlacionado à precisão dos componentes analógicos do rádio (Garcia Reis, 2012).

As desvantagens consistem em maior complexidade devido à necessidade do *front-end* de RF operar em faixa de frequências maior que a de um rádio convencional, de modo a permitir ao RDS manter sua flexibilidade de alteração de parâmetros de transmissão por *software*, bem como aos perigos relacionados a ataques cibernéticos (Lopes, 2013), (Marques, 2018).

4.1.4 RDS como solução para bloqueio

O RDS, como explicado, pode ser programado para operar com diferentes parâmetros ao longo do tempo. Essa mudança nos parâmetros inclui a variação da frequência de operação, da potência ou do tipo de modulação, por exemplo.

Em comunicações táticas militares, as frequências utilizadas estão principalmente nas faixas de HF, VHF e UHF. Principalmente nas frequências de VHF e UHF, uma das MPE-COM que são empregadas para garantir comunicações seguras é o salto em frequência, que consiste em alterar continuamente os canais de operação dentre os diversos disponíveis, ocupando cada canal por um período bem curto de tempo, na ordem de milissegundos (Filippo Neri, 2018).

Uma notícia vinculada no *site* oficial da Força Aérea dos Estados Unidos da América fornece informações sobre avanços tecnológicos nas comunicações militares deste país. Uma equipe da Base Aérea de Hanscom tem trabalhado para fornecer um sistema de comunicações anti-bloqueio, denominado *Second Generation Anti-Jam Tactical Ultra-High Frequency Radio* (SATURN). O SATURN é um RDS, que substituirá um atual sistema *HAVE QUICK II*. Este sistema é capaz de operar com segurança mesmo na presença de um ambiente saturado por bloqueio, a fim de permitir comunicações eficazes com forças aliadas da OTAN. Desta forma, este sistema provê não só a capacidade de MPE-COM contra o bloqueio, mas também a interoperabilidade. A capacidade anti-bloqueio é provida por meio de saltos rápidos em frequência, bem como através de técnicas de modulação digital (“SATURN radio connects U.S. forces to allies”, 2020). Há alguns RDS no mercado que incorporam técnicas MPE de salto em frequência contra bloqueio, inclusive já compatíveis com o SATURN, como é o caso dos modelos M3AR e MR6000A da fabricante *Rohde & Schwarz* (Rohde & Schwarz, 2017). Desta forma, uma das capacidades do RDS em se contrapor ao bloqueio resulta da capacidade de salto rápido em frequência, capacidade essa que já pode ser encontrada em RDS disponíveis no mercado. Um *datasheet* que fala sobre as capacidades anti-bloqueio do M3AR está anexo a este trabalho.

4.2 Rádio Cognitivo

Não há uma definição unânime sobre os rádios cognitivos. As definições podem variar por questões semânticas, ou de acordo com a aplicação que se deseja realizar do equipamento.

Rádio cognitivo é definido pela União Internacional de Telecomunicações (UIT) como um sistema rádio empregando tecnologias que permitam ao sistema obter conhecimento sobre o ambiente operacional e geográfico ao seu redor, políticas estabelecidas e seu estado interno, de modo que dinamicamente e autonomamente ajuste seus parâmetros de operação de acordo com o conhecimento obtido, visando alcançar objetivos pré-determinados e aprender com os resultados obtidos (ITU, 2009).

O *Institute of Electrical and Electronics Engineers* (IEEE) traz uma definição de rádio cognitivo como um transceptor projetado para detectar, de maneira inteligente, o segmento do EEM em rádio que está em uso, de modo a cambiar de frequência a fim de utilizar outra parte do segmento, que não esteja em uso no momento, realizando essa tarefa de maneira rápida, sem interferir com as comunicações de usuários autorizados (Dabcevic, 2015).

Dabcevic (2015) sintetiza as diversas definições da seguinte maneira: rádios cognitivos são RDS, com capacidade adicional de perceber o ambiente de RF em que está inserido e, assim, reconfigurar seus parâmetros de operação automaticamente. Também podem ser equipados com antenas inteligentes, capacidade de geolocalização, dentre outras funcionalidades.

Apesar das diferentes definições, há princípios que estão presentes em praticamente todas elas, e que são o foco das aplicações deste sistema: capacidade cognitiva e capacidade de reconfiguração (Dabcevic, 2015), (Lopes, 2013), (Diogo, 2022).

A capacidade cognitiva de um rádio cognitivo é a habilidade de adquirir, processar e usar informações sobre seu ambiente operacional, geográfico, políticas estabelecidas e estado interno para tomar decisões sobre como operar de forma eficiente e eficaz. Com esta capacidade, partes do EEM não utilizados em determinado momento podem ser identificadas e utilizadas (Diogo, 2022), (Lopes, 2013).

A capacidade de reconfiguração viabiliza que, através do conhecimento obtido pela capacidade cognitiva, haja uma reprogramação, de forma dinâmica e autônoma, dos parâmetros operacionais do equipamento, de modo a realizar as comunicações da maneira mais eficiente (Diogo, 2022), (Lopes, 2013).

Sendo assim, pode-se dizer que o objetivo final do RC é obter o melhor espectro disponível por meio da capacidade cognitiva e da reconfiguração (Dabcevic, 2015).

4.2.1 TV *White Spaces* (TVWS)

A aplicação dos rádios cognitivos em GE-COM se dá graças às capacidades mencionadas de inteligência e reconfiguração automática dos parâmetros. Esses dois conceitos são vitais nos rádios cognitivos, e são utilizados no desenvolvimento de ações de bloqueio e anti-bloqueio (Dabcevic, 2015). Contudo, antes de se analisar a aplicação militar deste equipamento, cabe explicar uma outra aplicação, que pode ser tanto em comunicações civis quanto militares, e que já está sendo regulamentada em alguns países.

O EEM é um recurso limitado, e com o avanço tecnológico e o aumento da quantidade de serviços que utilizam este recurso, a demanda por faixas de frequência é cada vez maior. Assim, o seu uso deve ser feito de forma eficiente (Diogo, 2022). A digitalização dos canais de televisão no Brasil, por exemplo, foi uma ocorrência que otimizou o uso do EEM. Um canal de TV analógico possui uma largura de banda de 6 MHz. Esta mesma largura de banda pode ser dividida para 3 a 10 canais digitais (Avendaño; Espindola; Montañez, 2020), conforme ilustrado na Figura 4.1, em que a largura de banda foi dividida para 4 canais digitais.

Figura 4.1: diferença no uso das bandas de TV analógica e TV digital.



Fonte: Diogo, 2022

A crescente demanda por faixas de frequência no espectro das comunicações sem fio inspirou pesquisas para a utilização dinâmica dessas faixas. Essas pesquisas demonstram que o rádio cognitivo pode ser uma ferramenta eficaz no uso eficiente do EEM (Dong, 2018).

Neste contexto, temos os usuários primários (PU) e os usuários secundários (SU). PU são os usuários licenciados que possuem autorização para uso das diferentes bandas da faixa do EEM considerada, ou seja, são os usuários aos quais a agência reguladora do país em questão alocou determinada banda. O PU pode ser, por exemplo, uma emissora de TV, que está licenciada para operar um determinado canal. O SU é um usuário que pode ser licenciado, e que deseja fazer uso de bandas ou canais concedidos aos PU, sem, no entanto, interferir nos serviços deste usuário (Diogo, 2022) (Dong, 2018).

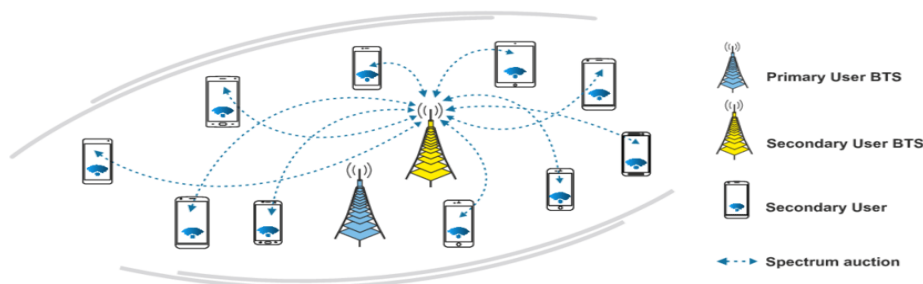
Os rádios cognitivos, devido a sua capacidade de utilizar o EEM de maneira inteligente, bem como de reconfigurar seus parâmetros de operação, podem ser utilizados

pelos SU, alocando a estes usuários um “espaço em branco” do espectro, ou seja, um canal concedido a um PU, mas que não esteja sendo utilizado no momento considerado ou em determinada região. Pela sua habilidade em reconhecer o ambiente eletromagnético no qual está operando, o rádio cognitivo é capaz de analisar determinada faixa de frequência, determinais canais que não estejam sendo utilizados no momento, utilizar um desses canais e, caso este canal comece a ser utilizada pelo PU, o rádio automaticamente migra para outro que não esteja em uso, de modo que não haja perdas de comunicação. Assim, ele é capaz de manter comunicações sem impactar o uso dos canais pelos PU e, desta forma, o EEM é utilizado de maneira mais eficiente (Diogo, 2022).

De acordo com Avendaño; Espindola; Montañez (2020), TVWS é um conceito baseado no padrão IEEE 802.22, que engloba a ideia de SU utilizarem canais ociosos dos PU de canais de TV, a fim de viabilizar o acesso à internet, especialmente em áreas rurais. O padrão IEEE 802.22 estabelece como é possível levar sinal de banda larga sem fio para localizações remotas, na faixa de frequência do serviço de televisão em VHF e UHF, instalando-se rádios cognitivos como SU que utilizarão os canais alocados para os PU, sem interferir no serviço destes (Diogo, 2022). A Colômbia foi o primeiro país da América do Sul a regulamentar o uso da tecnologia TVWS, em 2017, por meio do padrão IEEE 802.22. A principal vantagem do TVWS em VHF e UHF se dá devido a melhores condições de propagação, incremento no alcance e robustez quando comparado às frequências mais altas (Avendaño; Espindola; Montañez, 2020).

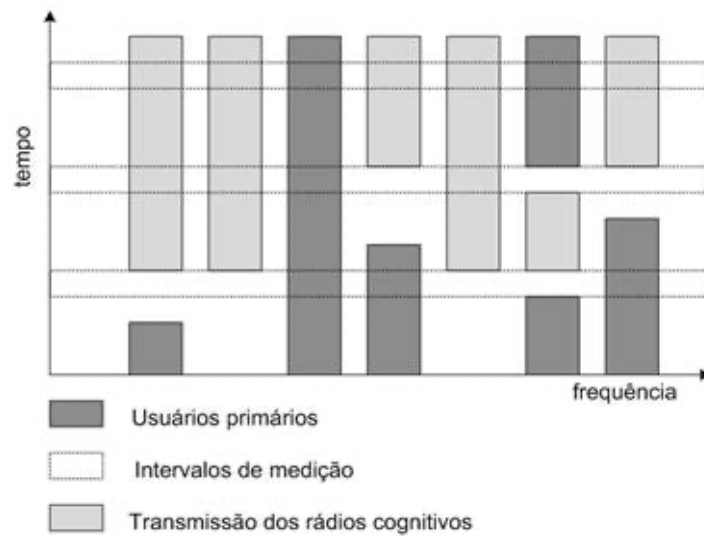
A Figura 4.2 esquematiza uma estação base de SU (*secondary user BTS*) utilizando a mesma frequência do PU, já que este não está em uso, para efetuar comunicações com os dispositivos SU. Já a Figura 4.3 mostra um SU utilizando os canais ociosos dos PU ao longo do tempo.

Figura 4.2: aplicação dos rádios cognitivos como SU.



Fonte: GAZDA et al., 2017

Figura 4.3: ilustração sobre o uso dos canais licenciados por SU ao longo do tempo.



Fonte: Vogel, 2019

4.2.2 Uso dos rádios cognitivos em aplicações militares

Foi mostrado que a utilização de rádios cognitivos permite a utilização mais eficiente do EEM, e uma das aplicações militares destes equipamentos é o próprio conceito de TVWS, que permite o aproveitamento de canais de TV digital ociosos para uso por comunicações em banda larga. No entanto, os rádios cognitivos também podem possuir vantagens na GE-COM. As duas características principais dos rádios cognitivos abordadas neste trabalho, que são a inteligência e a reconfiguração automática dos parâmetros, são utilizadas no desenvolvimento de ações de bloqueio e anti-bloqueio. Embora o conceito de bloqueio seja bastante antigo, os problemas relacionados a sistemas de bloqueio e anti-bloqueio permanecem longe de ter solução, conforme a corrida entre os dois continua a se desenvolver continuamente (Dabcevic, 2015).

Os rádios cognitivos permitem diversas aplicações, como interoperabilidade, acesso dinâmico ao EEM e, especificamente em comunicações militares, soluções avançadas na GE-COM. Esta última aplicação implica em manter comunicações confiáveis entre meios de uma mesma Força, ou também prevenir o inimigo de fazer o mesmo, e pode significar em vantagem tática num teatro de operações. Assim, a interoperabilidade e a capacidade de reconfiguração automática provida por um rádio cognitivo são de especial interesse no campo de GE-COM (Dabcevic, 2015).

Como visto, os rádios cognitivos utilizados como SU podem utilizar um canal de um PU enquanto este não esteja utilizando o canal. No entanto, ao perceber a atividade do PU, o SU altera seu canal de operação. Este conceito pode ser aplicado, também, seguindo os

mesmos princípios, em MPE-COM, como uma técnica de comunicações anti-bloqueio. O rádio cognitivo continuaria fazendo o papel de SU. Contudo, neste caso, o papel de PU é assumido pelo dispositivo de bloqueio. Assim, o rádio cognitivo, ao detectar a presença de um dispositivo de bloqueio (que não mais é um usuário licenciado, e sim uma interferência indesejada), altera seus parâmetros de operação, no intuito não mais de não interferir com o PU, e sim para não ser interferido (ou bloqueado) por ele.

É importante ressaltar que, de acordo com Poisel (2011), técnicas de comunicações anti-bloqueio se referem à habilidade de combater um bloqueio. Entretanto, estar totalmente imune aos efeitos do bloqueio em comunicações sem fio é um objetivo irrealista. Nas condições apropriadas, todos os sistemas de RF podem ser bloqueados. Dessa forma, deve-se procurar conseguir mitigar ao máximo as interferências indesejadas, mesmo que a condição ideal (não sofrer absolutamente nenhuma interferência do bloqueio) não seja atendida. Uma das tecnologias utilizadas para se contrapor ao bloqueio é a tecnologia *spread spectrum* (SS).

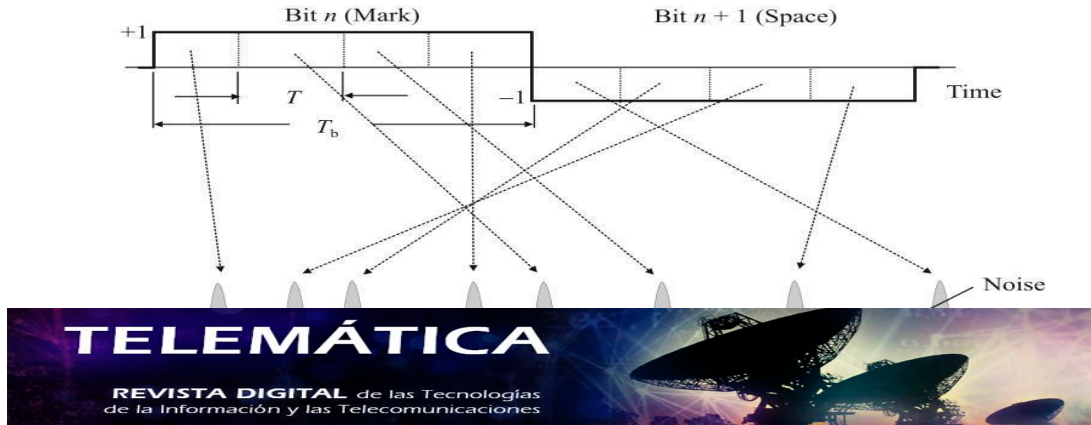
As capacidades do rádio cognitivo permitem que ele seja utilizado para monitorar as bandas de frequência de interesse em conjunto com técnicas de *Frequency-Hopping Spread Spectrum* (FHSS), de modo a identificar espaços em branco nos canais, ou seja, canais não utilizados. FHSS é uma das técnicas que, juntamente com o *Direct Sequence Spread Spectrum* (DSSS), constituem as duas técnicas mais tradicionais de comunicações contra bloqueios. A técnica DSSS é uma técnica *Low Probability of Detection* (LPD), ou seja, com baixa probabilidade de detecção, cujo objetivo é que um receptor tenha dificuldade em determinar até mesmo se há sinal presente. Já o FHSS é uma técnica de *Low Probability of Interception* (LPI), ou seja, embora o receptor consiga detectar a presença do sinal, ele é difícil de ser interceptado. As técnicas anti-bloqueio são as mesmas utilizadas para sinais LPD e LPI (Poisel, 2011).

O DSSS espalha o sinal ao longo de uma banda extensa, de tal modo que toda a banda é ocupada instantaneamente. Isso faz com que a energia em cada pequena banda de frequência é bem pequena. Muitas vezes os receptores de comunicações podem confundir o sinal como ruído ambiente, devido a tão baixa energia e, assim, é necessária alguma técnica especial para o processamento do sinal.

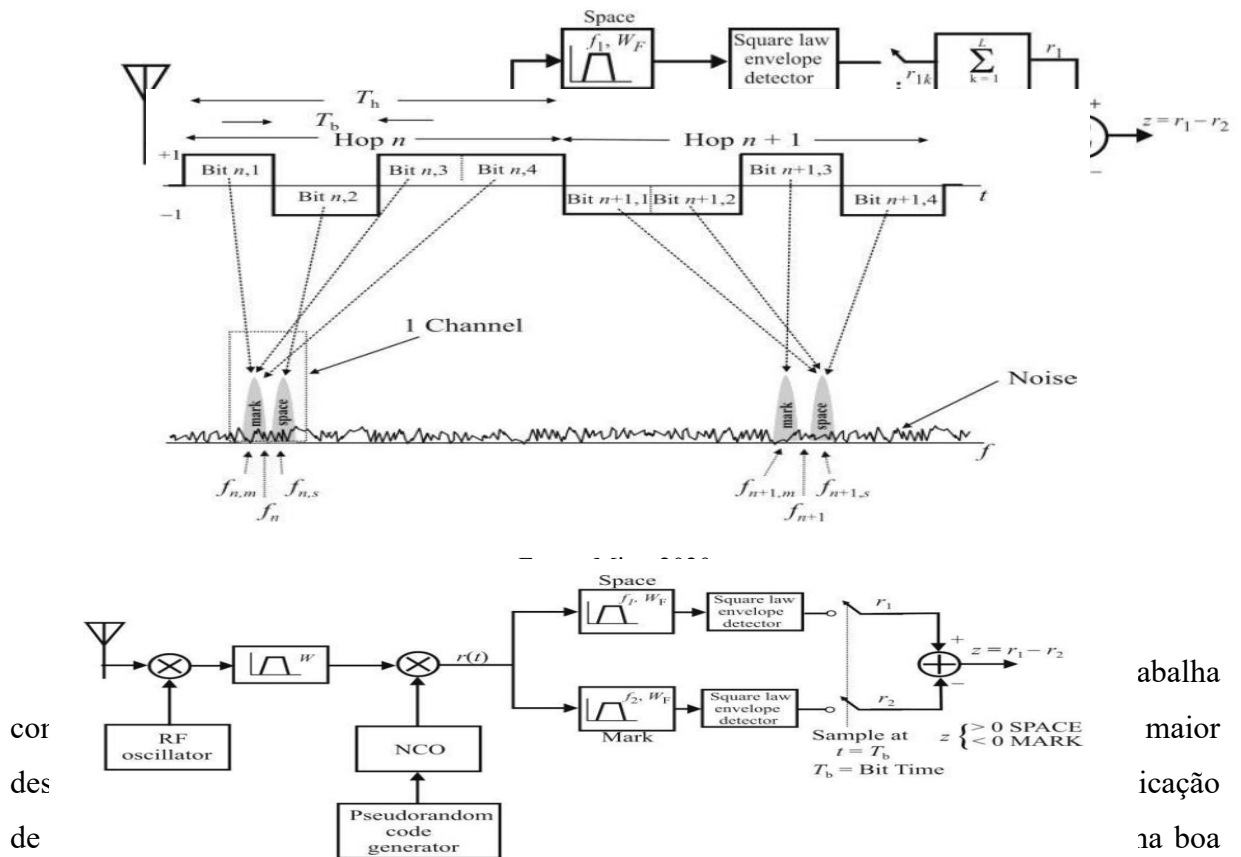
Na tecnologia FHSS, diferentemente do DSSS, o sinal ocupa apenas um canal, normalmente em faixa estreita, em cada momento. Nas comunicações em VHF, essa faixa é normalmente 25 kHz. Nas frequências mais baixas em VHF, há mais ou menos 2400 canais de 25 kHz de banda disponíveis. A vantagem do FHSS é a diversidade de frequência. O FHSS

é subdividido em *Fast Frequency-Hopping Spread Spectrum* (FFHSS) e *Slow Frequency-Hopping Spread Spectrum* (SFHSS), conforme ilustrado nas Figuras 4.4 e 4.5.

Figura 4.4: ilustração da técnica FFHSS.



Fonte: Mier, 2020



cor
des
de

abalha
maior
icação
na boa

solução para promover eficiência do uso do EEM, bem como perceber canais não utilizados pelos PU. Estes objetivos podem ser alcançados com técnica FFHSS (Mier, 2020).

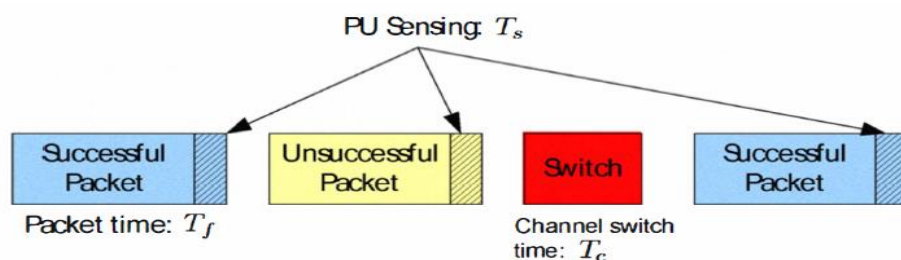
A priori, o bloqueador não sabe em qual canal o rádio cognitivo opera. Quanto mais canais são bloqueados simultaneamente, mais provavelmente o canal sendo utilizado pelo rádio cognitivo poderá ser bloqueado, no entanto, menos potência de bloqueio haverá em

cada canal. Quanto menos canais são bloqueados, menos provavelmente o canal sendo utilizado pelo rádio cognitivo será bloqueado, mas com mais potência, o que aumenta a eficácia da interferência caso o canal correto esteja sendo utilizado pelo bloqueador. Por isso, na prática, o número de canais bloqueados simultaneamente não pode ser muito grande (Mier, 2020). Esses aspectos devem ser considerados na escolha do tipo de bloqueio a ser empregado. Além desse aspecto, a escolha do método de bloqueio escolhido também depende da capacidade do equipamento a ser utilizado. O bloqueio seguidor, por exemplo, é mais complexo que os demais, o que pode acarretar na inviabilidade de seu emprego, mesmo que em determinada situação particular ele possa ser julgado como o mais conveniente. Assim, é necessário levar em consideração as capacidades dos rádios cognitivos de se contraporem aos diferentes tipos de bloqueios já definidos, já que qualquer um deles pode ser empregado num cenário de guerra.

A eficácia dos rádios cognitivos contra diferentes tipos de bloqueios foi estudada por Mier (2020). Ele realizou simulações e estudos de dois tipos de rádios cognitivos diferentes: um rádio baseado no sistema comercial IEEE 802.22 (TVWS), denominado sistema C1, bem como um rádio do sistema militar XG da *Defense Advanced Research Projects Agency* (DARPA), denominado sistema C2. Ambos os sistemas são baseados no esquema de transmissão ilustrado na Figura 4.6. Esta figura mostra que a transmissão do pacote de dados é efetuada durante o período do tempo T_f . Após essa transmissão, é efetuado um sensoramento pelo rádio cognitivo durante um intervalo de tempo T_s . Caso o canal não esteja bloqueado, o rádio realiza outra transmissão mesmo canal durante o mesmo intervalo



Figura 4.6: esquema de transmissão e mudança de canal do rádio cognitivo.

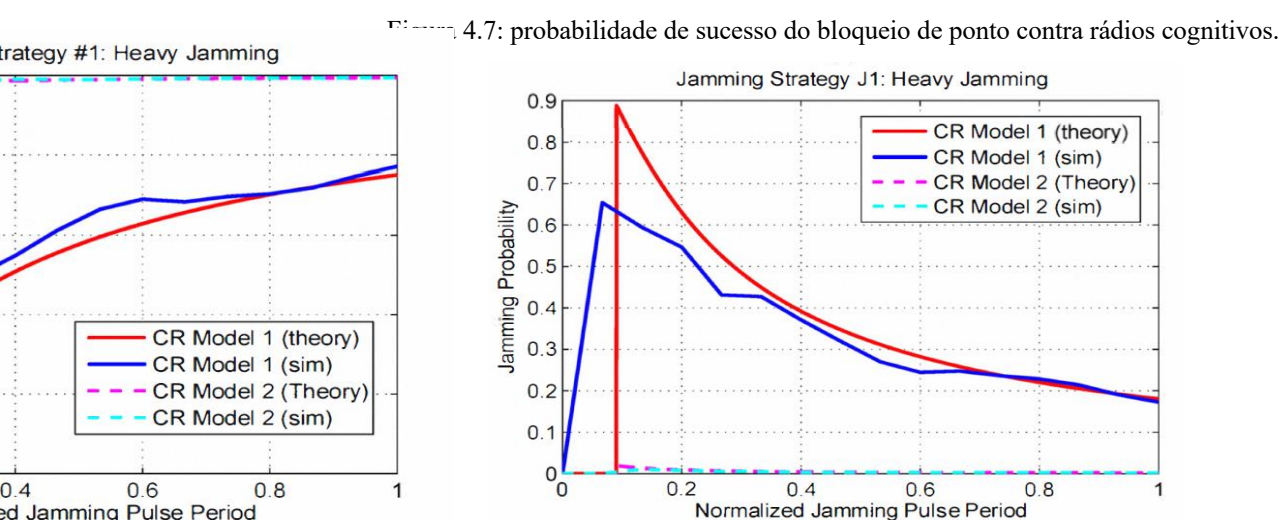


Fonte: Mier, 2020

A diferença principal entre os sistemas C1 e C2 está na quantidade de canais disponíveis e nos intervalos de tempo T_f , T_c . O sistema C1, comercial, possui poucos canais disponíveis e altos valores de T_f e T_c . Já o sistema militar C2 possui muitos canais disponíveis e baixos valores de T_f e T_c .

4.2.3 Rádios cognitivos empregados contra bloqueio de ponto

Contra bloqueio de ponto, com alto valor de potência em um único canal, Mier (2020) demonstra que, quando utilizando um número de canais alto, a tecnologia do rádio cognitivo pode mitigar de maneira eficaz os bloqueadores, já que a probabilidade de bloqueio é praticamente zero, tanto para a curva teórica, quanto para a simulada. Isso pode ser visto na Figura 4.7.



Fonte: Mier, 2020

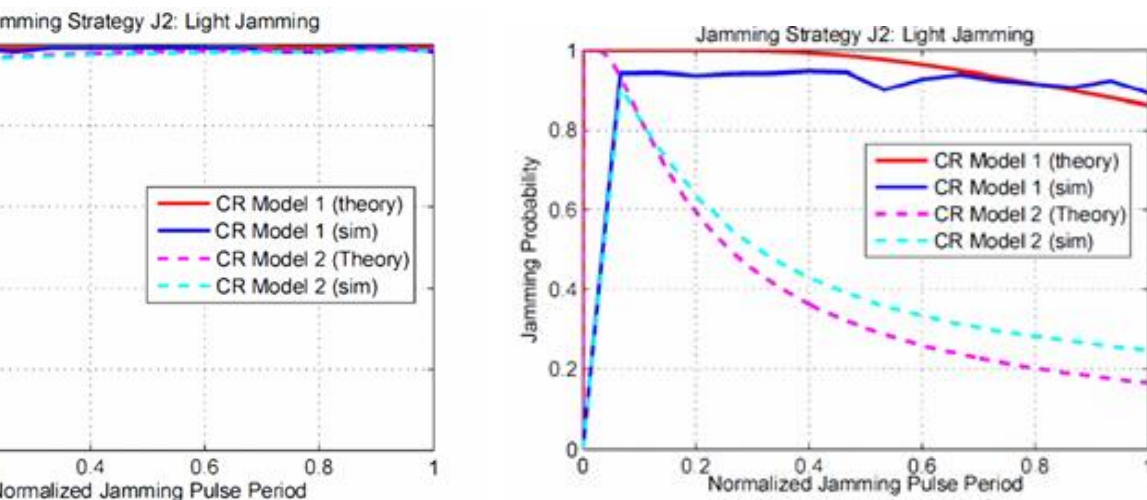
No caso apresentado, um sistema militar (sistema C2), com muitos canais de operação, e intervalos de tempo de transmissão e de comutação de canais pequenos, praticamente não sofre bloqueio. Para qualquer período de pulso de bloqueio normalizado, a probabilidade do bloqueio é praticamente zero. Já para os rádios cognitivos comerciais, o bloqueio pode ou não ser eficaz, a depender do período de pulso do bloqueio. Sendo assim, os rádios cognitivos militares conseguiriam manter comunicações eficazes e na presença de bloqueio de ponto. Mesmo que o bloqueador interfira no canal correto, o enlace dos rádios cognitivos efetuará a alteração do canal de operação e, como o bloqueador, normalmente, não pode seguir perfeitamente a troca de canais do rádio cognitivo, assume-se que esta próxima transmissão seja exitosa (Mier, 2020).

Desta forma, as técnicas de FHSS possuem boa eficácia contra bloqueio de ponto, sendo mais eficazes quanto mais canais estiverem disponíveis para a operação e quanto mais rápida for a comutação dos canais.

4.2.4 Rádios cognitivos empregados contra bloqueio de barragem

No caso dos bloqueios de barragem, diferente do bloqueio de ponto, a eficácia do bloqueio não é medida em termos da capacidade do bloqueador em emitir um sinal mais potente que o rádio cognitivo transmissor, de modo a impedir que o receptor obtenha as mensagens do transmissor. Mier (2020) propõe que o bloqueador emitiria um sinal fraco, mas que fosse capaz de fazer o rádio cognitivo perceber sua presença no ambiente do EEM. Sendo assim, durante o intervalo de tempo T_s em que o rádio cognitivo faz o sensoriamento do ambiente, ele perceberia a utilização do canal pelo bloqueador e, assim, seria obrigado a realizar a comutação do canal. Isso significa que os pacotes de dados transmitidos podem, sim, chegar ao receptor de maneira eficaz, já que o bloqueador não é potente o suficiente para mascarar o sinal do transmissor. No entanto, o rádio cognitivo, ao realizar o sensoriamento, perceberia que há um “PU” utilizando o canal e, assim, realizaria a comutação do canal. Após a comutação, ocorreria a retransmissão do mesmo pacote de dados que havia sido transmitido no canal anterior. A Figura 4.8 ilustra a eficácia do bloqueio de barragem contra rádios cognitivos.

Figura 4.8: probabilidade de sucesso do bloqueio de barragem contra rádios cognitivos.



Fonte: Mier, 2020

Na análise da Figura 4.8, pode-se perceber que uma maior quantidade de canais implica em menor eficiência do bloqueio, a depender do período de pulso do bloqueio. Por

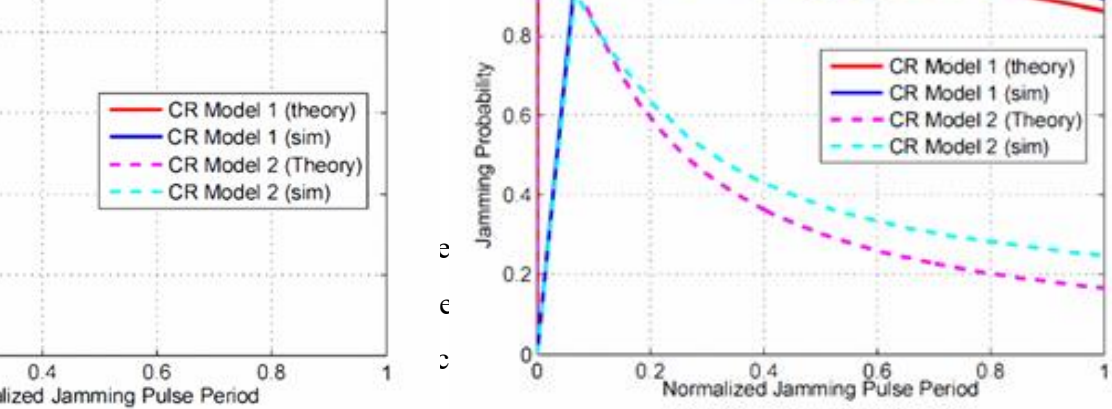
mais que o bloqueio de barragem implique uma interferência numa grande faixa de frequências, um sistema militar como o sistema C2, com muitos canais disponíveis, pode fazer com que nem todos os canais sejam cobertos pelo bloqueio de barragem. No entanto, o interesse do bloqueador é obrigar o enlace dos rádios cognitivos a comutarem o canal. De acordo com Mier (2020), quanto maior o período de pulso de bloqueio, menos probabilidade o sistema C2 terá de ser bloqueado. Uma exemplificação disso é a seguinte: como foi dito, neste caso de bloqueio, o que importa é bloquear o período T_s de sensoriamento do rádio cognitivo. O bloqueador de barragem pode bloquear M canais simultaneamente. Se o período de bloqueio valer T_s segundos, então o bloqueador interferirá em M canais. Se o período de bloqueio valer a metade de T_s segundos, então o bloqueador interferirá em $2M$ canais. Assim, quanto maior o período de pulso do bloqueio, melhor a capacidade do sistema C2 em se contrapor ao bloqueio de barragem.

4.2.5 Rádios cognitivos empregados contra bloqueios de varredura e seguidor

Embora não abordada por Mier, a eficácia do bloqueio de varredura contra saltos em frequência depende do conhecimento da faixa de frequências em que o salto está ocorrendo, bem como da rapidez da varredura relativamente à rapidez do salto em frequência por parte do transmissor (Poisel, 2011).

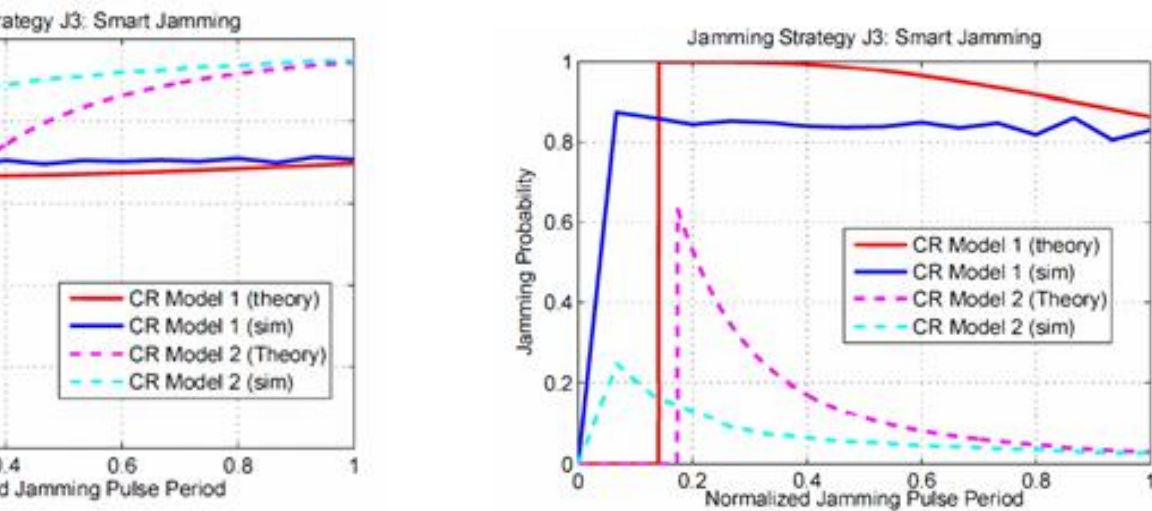
O bloqueio seguidor que possua varredura em extensa faixa de frequência e capacidades de resposta interferente maior que o período de salto do FHSS pode ser eficaz contra esta tecnologia. No entanto, cabe ressaltar que o conceito de bloqueio seguidor é uma realidade implicitamente análoga à realidade dos rádios cognitivos com características de conhecimento do espectro, aprendizado e atuação (Mier, 2020). Já Poisel (2011) diz que o bloqueio seguidor pode ser ineficaz contra FFHSS e eficaz contra SFHSS. Desta forma, a análise das bibliografias sobre o assunto deixa aberta a possibilidade tanto da eficácia como da ineficácia do FHSS contra este tipo de bloqueio. Assim, conclui-se que, especificamente no caso dos bloqueios seguidores, a eficácia dos rádios cognitivos como um equipamento anti-bloqueio vai depender dos parâmetros de ambos os sistemas. Desta forma, a velocidade com que o rádio cognitivo altera seu canal de operação é essencial para a sua capacidade anti-bloqueio e, por isso, a tecnologia FFHSS assume grande importância para esta finalidade.

Mier (2020) fez uma terceira simulação de eficácia do rádio cognitivo contra bloqueio, sobre um tipo de bloqueio que ele denominou como bloqueio inteligente. Pela análise deste bloqueio conforme relatado pelo autor, este tipo é bem semelhante ao bloqueio



entanto, adicionalmente, este bloqueio tem a intenção de impedir o protocolo de enlace realizado pelos rádios cognitivos. Quando isso ocorre, o tempo para a comutação do canal que, de acordo com a Figura 4.6 era T_c , agora será T_w , um valor consideravelmente maior que T_c . A intenção é, então, bloquear o começo do procedimento de comutação do canal, de modo a evitar novos enlaces. A Figura 4.9 mostra os resultados da probabilidade de bloqueio dos sistemas C1 e C2 na presença deste bloqueio inteligente.

Figura 4.9: probabilidade de sucesso do bloqueio inteligente contra rádios cognitivos.



Fonte: Mier, 2020

Este tipo de bloqueio foi o que apresentou melhor performance contra os rádios cognitivos. Mesmo com sistema militar C2, caso o adequado período de pulso de bloqueio seja selecionado, a performance do equipamento rádio pode ser consideravelmente reduzida.

5 CONCLUSÃO

A capacidade do RDS de alterar seus parâmetros de operação como frequência, tipo de modulação e potência de maneira flexível torna este equipamento uma solução para se manter comunicações seguras na presença de bloqueio eletrônico. De fato, há no mercado empresas especializadas em equipamentos militares contendo, em seu portfólio de produtos, RDS com capacidade de MPE-COM anti-bloqueio, através da técnica FHSS. Estas técnicas de FHSS são bastante úteis para se contrapor ao bloqueio, como indicam as tendências tecnológicas dos produtos mais novos de empresas renomadas em equipamentos militares como a *Rohde & Schwarz*, bem como os recentes desenvolvimentos em sistemas rádio do Departamento de Defesa dos Estados Unidos da América, o projeto SATURN.

O rádio cognitivo, como uma evolução do RDS, possui a mesma flexibilidade, com a capacidade adicional de realizar o sensoriamento do ambiente eletromagnético de maneira inteligente. De modo geral, quanto maior a quantidade de canais de comunicações e quanto mais rápida for a comutação entre esses canais, mais eficaz será a comunicação. Assim, as técnicas de FHSS e, em especial, a técnica FFHSS figuram como importantes medidas de MPE-COM. Como o conceito por trás dos rádios cognitivos militares envolve as técnicas de FFHSS, estes equipamentos têm o potencial de figurar como um equipamento com alta capacidade anti-bloqueio.

5.1 Considerações Finais

Contra bloqueio de ponto, os rádios cognitivos apresentaram excelente eficácia, com probabilidade de bloqueio tendendo a zero. É importante ressaltar, no entanto, que quanto mais rápida for a comutação dos canais, e quanto maior a quantidade de canais, mais eficaz será a comunicação.

Contra bloqueios de barragem, pode-se estabelecer um protocolo no enlace entre receptor e transmissor, de modo que mesmo na presença do bloqueio, caso o pacote de dados do transmissor chegue íntegro ao receptor, então a comutação de canal não deve ser compulsoriamente realizada. Neste caso, ao se eliminar a necessidade de comutação dos canais, considerando a baixa densidade de potência do bloqueio de barragem, os rádios cognitivos podem ser eficazes na manutenção das comunicações mesmo na presença do bloqueio.

Contra bloqueios de varredura e seguidor, o rádio cognitivo pode, sim, apresentar eficácia nas comunicações mesmo na presença do bloqueio. No entanto, deve ser dada uma

grande atenção nas capacidades do equipamento no que diz respeito às suas características técnicas, como número de canais, rapidez de comutação e faixa de frequência de operação. Quanto melhores essas características técnicas forem com relação às características do equipamento bloqueador, maior a probabilidade de se manter comunicações eficazes na presença do bloqueio.

5.2 Sugestões para Futuros Trabalhos

Recomenda-se, como sugestão de trabalho futuro, uma análise da eficácia de outras técnicas anti-bloqueio contra o bloqueio seguidor, em especial a técnica híbrida que combina o DSSS com o FHSS.

Considerando o extenso litoral brasileiro, bem como as grandes áreas da Amazônia Azul e da Amazônia Verde, pode ser interessante um estudo sobre o impacto, nos sistemas de monitoramento destas áreas, do emprego dos rádios cognitivos no uso mais eficiente do EEM através do conceito de TVWS que permite a utilização de banda larga em áreas remotas.

REFERÊNCIAS

AVENDAÑO, E.; ESPINDOLA, J. E.; MONTAÑEZ, O. J. Study of tv white spaces in the context of cognitive radio for the deployment of WiFi in rural zones of the colombian army. **Espacios**, v. 41, n. 50, p. 171–182, 30 dez. 2020.

BISHT, I. S. **Russia Equips Su-57 Jets With AI-Based Secure Communication Suite**. Disponível em: <https://www.thedefensepost.com/2023/08/10/russia-su-57-jet/#google_vignette>. Acesso em: 15 set. 2023.

BRASIL. Departamento de Ciência e Tecnologia do Exército. Portaria nº 007, de 27 de janeiro de 2023. Aprova as Necessidades de Conhecimentos Específicos da Linha de Ensino Militar Científico- Tecnológico para o ano de 2024, do Plano de Cursos e Estágios Gerais no Exército Brasileiro (PCE – EB), do Plano de Cursos e Estágios em Estabelecimentos de Ensino Civis Nacionais (PCE – EECN) e do Plano de Cursos e Estágios em Nações Amigas (PCENA). Disponível em: http://www.sgex.eb.mil.br/sg8/006_outras_publicacoes/04_planos/port_n_007_dct_27jan2023.html, acesso em: 2 out. 2023.

DABCEVIC, Kresimir. **Intelligent jamming and anti-jamming techniques using Cognitive Radios**. 2015. (PhD Programme in Computational Intelligence) - University of Genoa, Genoa, 2015.

DIOGO, Olívia Peixoto. **Análise e perspectiva da utilização do TVWS no Brasil**. Dissertação (Pós-Graduação em Engenharia Elétrica e de Telecomunicações) - Universidade Federal Fluminense, Niterói, 2022.

DONG, Qi et al. **A survey on simulation tools and testbeds for cognitive radio networks study**. ArXiv abs/1808.09858, 2018. Disponível em: <<https://arxiv.org/abs/1808.09858>>. Acesso em: 08 set. 2023.

FILHO, H. V. P.; GALDINO, J. F.; MOURA, D. F. C. Pesquisa e Desenvolvimento de Produtos de Defesa: Reflexões e Fatos sobre o Projeto Rádio Definido por Software do Ministério da Defesa à luz do Modelo de Inovação em Tríplex Hélice. **Revista Militar de Ciência e Tecnologia**, Rio de Janeiro, v. 34, n. 1, p. 6-19, 2017.

FILIPPO NERI. **Introduction to electronic defense systems**. Boston: Artech House, 2018.

GARCIA REIS, A. L. et al. Introduction to the Software-defined Radio Approach. **IEEE Latin America Transactions**, v. 10, n. 1, p. 1156–1161, jan. 2012.

GAZDA, J. et al. AGENT-BASED MODEL OF THE SPECTRUM AUCTIONS WITH SENSING IMPERFECTIONS IN DYNAMIC SPECTRUM ACCESS NETWORKS. **Computing and Informatics**, v. 36, p. 1041–1062, 2017.

ITU. **Definitions of Software Defined Radio (SDR) and Cognitive Radio System (CRS) SM Series Spectrum management**. Disponível em: <https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-SM.2152-2009-PDF-E.pdf>. Acesso em: 10 ago. 2023.

LATHI, B. P.; ZHI DING. **Modern digital and analog communication systems**. New York: Oxford University Press, 2010.

LOPES, Fábio Rogério Born. **MÉTODO DE SUPRESSÃO ESPECTRAL DO SINAL OFDM EMPREGANDO BANDA DE GUARDA COM PORTADORAS DE CANCELAMENTO**. Dissertação (Pós-Graduação em Engenharia de Telecomunicações) - Universidade Federal Fluminense, Niterói, 2013.

MARQUES, Alexandre de Macedo. **LIMITAÇÕES IMPOSTAS PELA NATUREZA ÀS COMUNICAÇÕES E O USO DOS RÁDIOS DEFINIDOS POR SOFTWARE COMO UMA SOLUÇÃO PARA AS COMUNICAÇÕES NAVAIS**. Monografia (Curso de Aperfeiçoamento Avançado em Guerra Eletrônica) – Centro de Instrução Almirante Wandenkolk, Rio de Janeiro, 2018.

MIER, R. G. EL RADIO COGNITIVO EN LA GUERRA ELECTRÓNICA. **Revista Telemática**, v. 19, n. 3, p. 23–37, set. 2020.

MITOLA, J. Software radios-survey, critical evaluation and future directions. 2 jan. 2003.

MONTEIRO, M. **APROPRIAÇÃO DO ESFORÇO DE INOVAÇÃO TECNOLÓGICA NO EXÉRCITO BRASILEIRO: O CASO DO RÁDIO DEFINIDO POR SOFTWARE**. Dissertação – Instituto Nacional da Propriedade Industrial

OTAN. Cognitive Radio Networks: Efficient Solutions for Routing, Topology Control, Data Transport, and Network Management. EUA. 2019. **STO-TR-IST-140**.

POISEL, Richard A. **Introduction to Communication Electronic Warfare Systems**. Boston: Artech House, 2002.

POISEL, R. **Modern communications jamming principles and techniques**. Boston: Artech House, Piscataway, New Jersey, 2011.

ROHDE & SCHWARZ. R&S M3AR Software Defined Radios VHF/UHF transceiver family for airborne communications. Disponível em: <https://www.rohde-schwarz.com/us/products/aerospace-defense-security/software-defined-radios-options/rs-m3ar-software-defined-radios_63493-9147.html>. Acesso em: 15 out. 2023.

SATURN radio connects U.S. forces to allies. Disponível em: <<https://www.af.mil/News/Article-Display/Article/2384413/saturn-radio-connects-us-forces-to-allies/>>. Acesso em: 23 set. 2023.

VOGEL, M. M. **Padrão IEEE 802.22 – I: Rádios Cognitivos**. Disponível em: <https://www.teleco.com.br/tutoriais/tutorialieee1/pagina_2.asp>. Acesso em: 10 out. 2023.

WILGENBUSCH, R. C.; HEISIG, A. **Command and Control Vulnerabilities to Communications Jamming**. 1 jan. 2013

ANEXO

Datasheet do equipamento M3AR da Rohde & Schwarz

R&S®M3AR Software Defined Radios At a glance

The software defined, multiband-capable airborne transceivers of the R&S®M3AR family feature a modular design and state-of-the-art technology. This leads to high MTBF values and a long life. The compact and lightweight transceivers offer high performance, making them suitable for operation in all types of aircraft, including unmanned aerial vehicles. Different waveforms are available, which can be installed at any time to provide interoperability in a variety of operational scenarios.

The R&S®M3AR family is the product of decades of experience, especially in the design and development of airborne radio equipment and software defined radio technology. The R&S®M3AR multiband, multimode, multirole radio is the solution of choice for the reliable transmission of mission-critical information, whether for jet or propeller aircraft, helicopters or unmanned aerial vehicles.

Rohde & Schwarz satisfies the most demanding requirements of a multitude of airborne platforms. The R&S®M3AR transceivers are in operation around the world and feature high reliability even under extreme environmental conditions. The outstanding MTBF values ensure low maintenance effort and high availability.

A variety of optional EPM (ECCM) methods are available. For instance, the R&S®SECOS frequency hopping method with integrated encryption can be installed in parallel with HAVE QUICK I/II.

The R&S®M3AR family consists of the R&S®MR6000A in an ARINC 600 housing and the R&S®MR6000R/ R&S®MR6000L, both of which are ARC-164 form and fit compatible. The R&S®MR6000L is equipped with a local control panel while the R&S®MR6000R is remotely controlled. All R&S®M3AR radios can be remotely controlled via the MIL-STD-1553B data bus, as well as by the R&S®GB6500 control unit. The R&S®MR6000R or R&S®MR6000L can serve as a form, fit and function (F3) replacement for legacy AN/ARC-164 radios.

Key facts

- Frequency range from 30 MHz to 400 MHz
- Compact and lightweight with high transmit power (up to 20 W in AM mode and up to 30 W in FM mode)
- EPM (ECCM): HAVE QUICK I/II, SATURN, R&S®SECOS
- Approved for jet and propeller aircraft as well as helicopters and unmanned aerial vehicles
- Embedded NATO or R&S®SECOS encryption
- Suitable for communications with military and civil air traffic control (e.g. 8.33 kHz channel spacing or offset carrier receive operation)

