

Fundamentos de Guerra Eletrônica (*Electronic Warfare - EW*). Detecção de ameaças. Sinais LPI (*Low Probability of Intercept*). Localização de emissores de radiação eletromagnética. *Jamming*.

Departamento de Eletrônica e Computação  
Centro de Tecnologia  
ELC1148 – Comunicações Estratégicas  
Prof. Fernando DeCastro



## Conceitos básicos de EW:

A grande maioria dos teatros de operações militares modernos, senão todos, dependem do transporte de informação através de ondas eletromagnéticas (EM) para o comando e controle (C2) das forças táticas. Técnicas de guerra eletrônica (EW – *electronic warfare*) são um meio de explorar e negar às forças inimigas o acesso a tal meio de transporte de informação, ao mesmo tempo que protege o espectro EM para uso por forças amigas (o conceito de espectro de um sinal é discutido em [http://www.fccdecastro.com.br/pdf/SS\\_Aula2\\_12032020.pdf](http://www.fccdecastro.com.br/pdf/SS_Aula2_12032020.pdf)).

EW tem sido um componente de teatros de guerra desde que a propagação de ondas EM começaram a ser usadas de modo prático, especificamente desde o final do século XIX. Na realidade, se comunicações navio-a-navio com sinalização ótica (bandeiras, faróis marítimo, sinalizadores, etc ...) puderem ser incluídas, então EW passa a ser um conceito muito mais antigo.

Uma das situações mais emblemáticas no âmbito de EW, e que demonstra a efetividade das técnicas de EW, é o incidente ocorrido em 2014 no Mar Negro em que um bombardeiro russo Su-24 equipado com um sistema de *jamming* (= bloqueio/neutralização de um dispositivo/sistema por interferência eletromagnética) de última geração, denominado em russo de *Khibiny* ([https://en.wikipedia.org/wiki/Khibiny\\_\(electronic\\_countermeasures\\_system\)](https://en.wikipedia.org/wiki/Khibiny_(electronic_countermeasures_system))), paralisou totalmente o sofisticado sistema de combate Aegis ([https://en.wikipedia.org/wiki/Aegis\\_Combat\\_System](https://en.wikipedia.org/wiki/Aegis_Combat_System)), instalado a bordo do destróier USS Donald Cook, um dos mais bem equipados destróieres da marinha norte americana. Uma breve descrição do incidente é encontrada em <https://www.naval.com.br/blog/2014/04/22/como-um-su-24-russo-paralisou-destroier-americano/>.

Em um teatro de guerra, comunicações através de ondas EM, sejam comunicações *wireless* ou não, interconectam sistemas de informação que podem ser pessoas ou máquinas, ou ambos. Neste contexto, EW consiste em três domínios de suporte mútuo: Suporte eletrônico (ES – *Electronic Support*), ataque eletrônico (EA – *Electronic Attack*) e proteção eletrônica (EP – *Electronic Protection*). Uma visão geral de EW mostrando esses três componentes é ilustrada no diagrama do próximo slide.

Historicamente, no âmbito do EW clássico, temos as seguintes equivalências nas denominações das três componentes ([https://en.wikipedia.org/wiki/Electronic\\_warfare](https://en.wikipedia.org/wiki/Electronic_warfare)):

- *Electronic Support* é o equivalente ao antigamente denominado *Electronic Support Measures* (ESM).
- *Electronic Attack* é o equivalente ao antigamente denominado *Electronic Countermeasures* (ECM) mas modernamente inclui armas anti-radiação (*antiradiation weapons*) e armas de energia dirigida (*directed-energy weapons*).
- *Electronic Protection* é o equivalente ao antigamente denominado *Electronic counter-countermeasures* (ECCM)

# Conceitos básicos de EW:

## Guerra Eletrônica (EW – *Electronic Warfare*)

### Ataque Eletrônico (EA – *Electronic Attack*)

EA consiste nas ações que fazem uso de energia eletromagnética, energia dirigida (*directed energy*) ou armas anti-radiação para atacar o efetivo humano, instalações ou equipamentos com a intenção de degradar, neutralizar ou destruir a capacidade de combate do inimigo.

### Proteção Eletrônica (EP – *Electronic Protection*)

EP consiste nas ações tomadas para proteger o efetivo humano, instalações e equipamentos de quaisquer efeitos do uso amigável ou belicoso do espectro eletromagnético com a intenção de degradar, neutralizar ou destruir a capacidade de combate da(s) facção(ões) amiga(s) engajada(s) no teatro operacional.

### Suporte à Guerra Eletrônica (ES – *Electronic Support*)

ES consiste nas ações tomadas por, ou sob controle direto de, um comandante operacional para buscar, interceptar, identificar, posicionar ou localizar fontes intencionais ou não-intencionais de energia eletromagnética irradiada com o objetivo de imediato reconhecimento de ameaças (*threats*), identificação de alvos (*targeting*), planejamento e condução de operações futuras.

EM *Jamming* (EM – eletromagnético)

EM *Deception* (=engodo via ondas EM)

*Directed Energy*

*Antiradiation Missile*

*Expendables* (=dispensáveis): *flares* (*flare* = dispositivo que produz uma luminosidade intensa, usado especialmente como um sinal ou marcador), *active decoys*, etc ... (*decoy* = dispositivo p/ engodo usado para afastar um inimigo de um alvo mais importante)

*Threat Warning* (= identificação e advertência de ameaças)

*Collection Supporting EW* (= coleta de informação p/ suporte, através de técnicas de EW)

*Direction Finding* (= identificação da direção da fonte de sinais)

*Spectrum Management*  
(= gerenciamento do espectro EM)

*EM Hardening*  
(= ação tomada p/ proteger o efetivo humano, instalações e/ou equipamentos, através de filtragem, atenuação, aterramento (*grounding*), conexão ou blindagem contra efeitos da radiação EM)

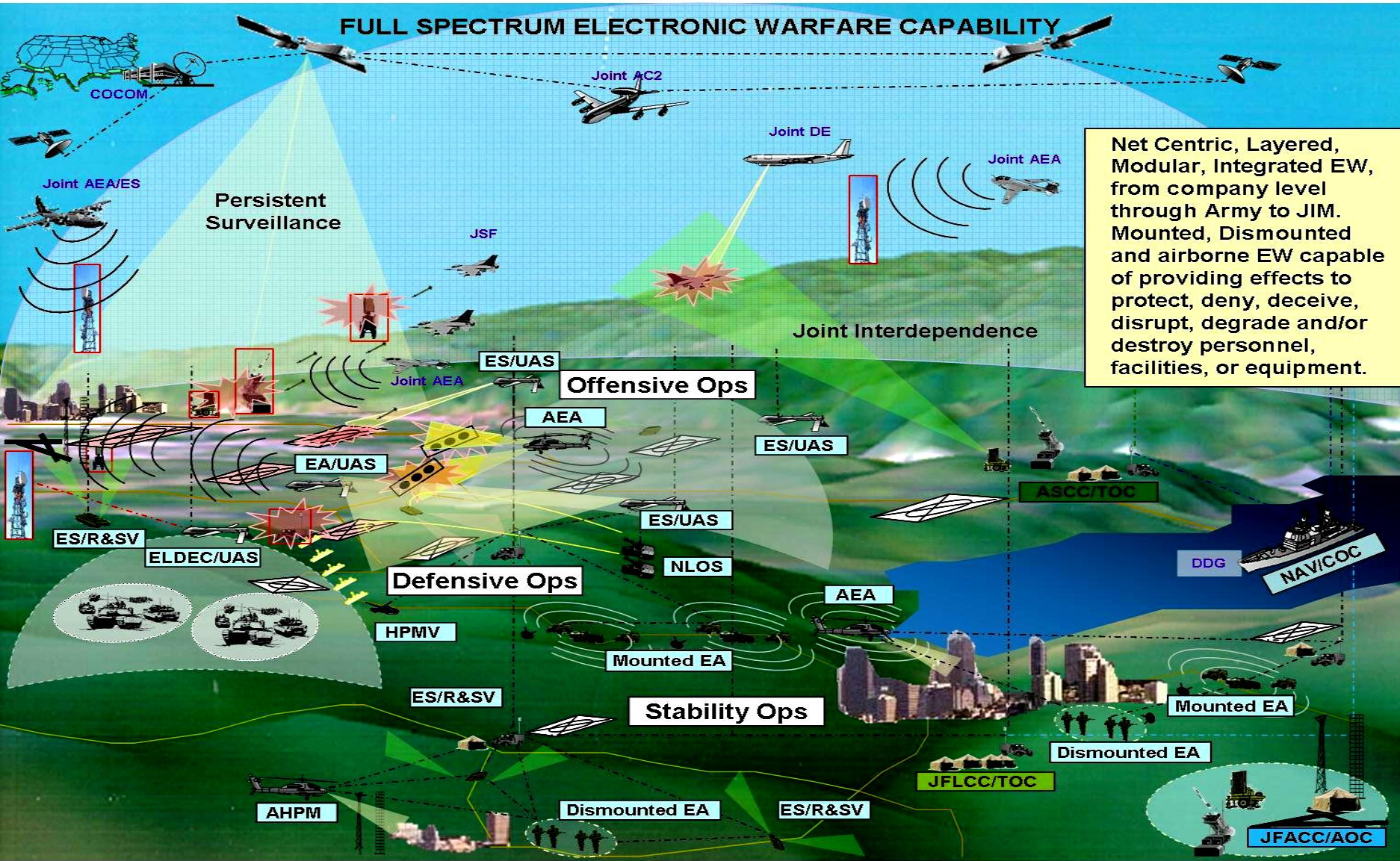
*Emission Control*  
(= controle da emissão de radiação EM por dispositivos e sistemas p/ evitar detecção pelo inimigo)



# Conceitos básicos – possível teatro de operações de EW:

## FULL SPECTRUM ELECTRONIC WARFARE CAPABILITY

Net Centric, Layered, Modular, Integrated EW, from company level through Army to JIM. Mounted, Dismounted and airborne EW capable of providing effects to protect, deny, deceive, disrupt, degrade and/or destroy personnel, facilities, or equipment.



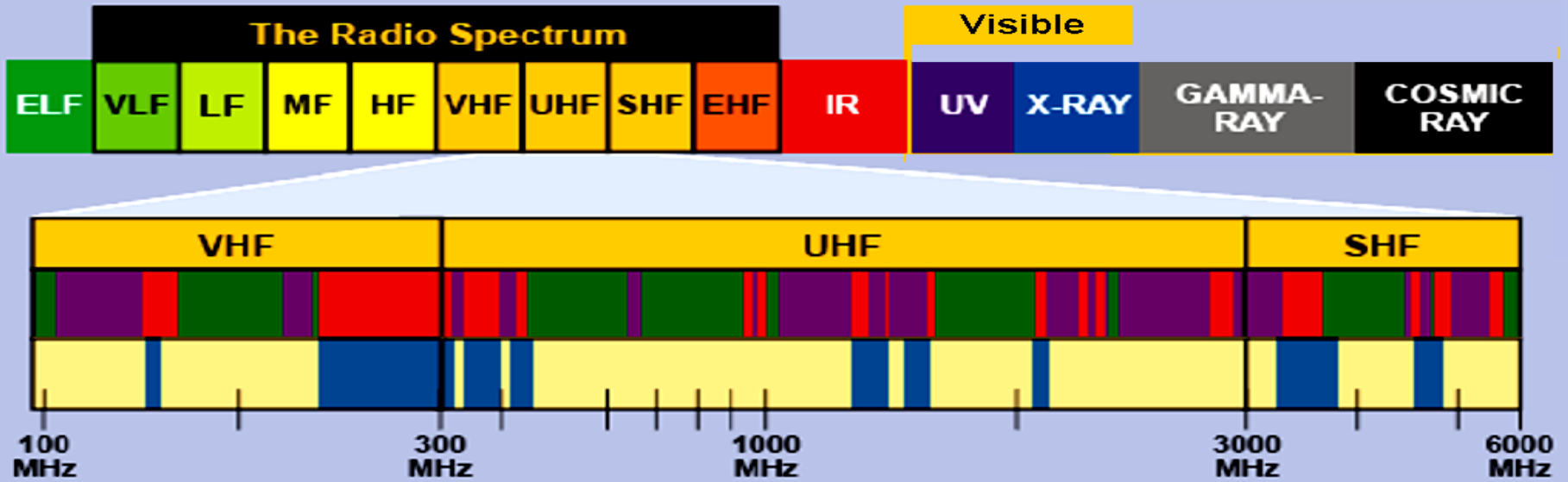
AEA – Airborne Electronic Attack  
 AHPM – Airborne High Power Microwave  
 AOC – Air Operations Center  
 ASCC – Army Service Component Command  
 COC – Command Operations Center  
 DDG – Guided Missile Destroyer

DE – Directed Energy  
 EA – Electronic Attack  
 ELDEC – Electronic Deception  
 ES – Electronic Warfare Support  
 HPMV – High Power Microwave Vehicle  
 JFACC – Joint Force Air Component Commander

JFLCC – Joint Force Land Component Commander  
 JSF – Joint Strike Fighter  
 NAV – Navy  
 NLOS – Non Line of Sight  
 R&SV – Reconnaissance and Surveillance Vehicle  
 UAS – Unmanned Aerial System



## THE ELECTROMAGNETIC SPECTRUM (EMS)



The top bar shows how the electromagnetic spectrum is divided into various regions, and indicates that portion referred to as the Radio Spectrum. The lower bar illustrates the division of Federal, non-Federal, and shared bands for a critical part of the Radio Spectrum. Also shown are selected military uses that would be impacted by reallocating spectrum for competing uses.

EHF	extremely high frequency	MF	medium frequency
ELF	extremely low frequency	MHz	megahertz
GHz	gigahertz	SHF	super-high frequency
HF	high frequency	UHF	ultrahigh frequency
IR	infrared	UV	ultraviolet
LF	low frequency	VHF	very high frequency
		VLF	very low frequency

## Conceitos básicos – os três domínios de suporte mútuo em EW:

### Suporte Eletrônico (ES)

O suporte eletrônico consiste nas operações e ações de detecção do ambiente eletromagnético (EM) com a finalidade de detectar e identificar alvos de interesse, principalmente em apoio ao ataque eletrônico (EA), mas também útil para estabelecer e manter a ordem eletrônica da batalha (EOB – *electronic order of battle*). Estabelecer o EOB significa identificar os emissores de sinais em uma área de interesse, determinando sua localização geográfica e sua região de mobilidade, caracterizando seus sinais e, quando possível, determinando seu papel na ordem organizacional mais ampla de batalha (= SIGINT – *signals intelligence*). A base de dados de EOB é usualmente plotada em um mapa tático, conforme mostrado no próximo slide.

### Ataque Eletrônico (EA)

O ataque eletrônico consiste de um amplo conjunto de ações possíveis, desde a destruição física de um equipamento ou de sua capacidade operacional de modo que ele não seja mais utilizável sem reparo ou substituição, até simplesmente atrasar a troca de informações entre dois pontos, possivelmente por *jamming* do receptor de uma rede de comunicações *wireless*.

Os elementos constituintes das ações no âmbito de EA são:

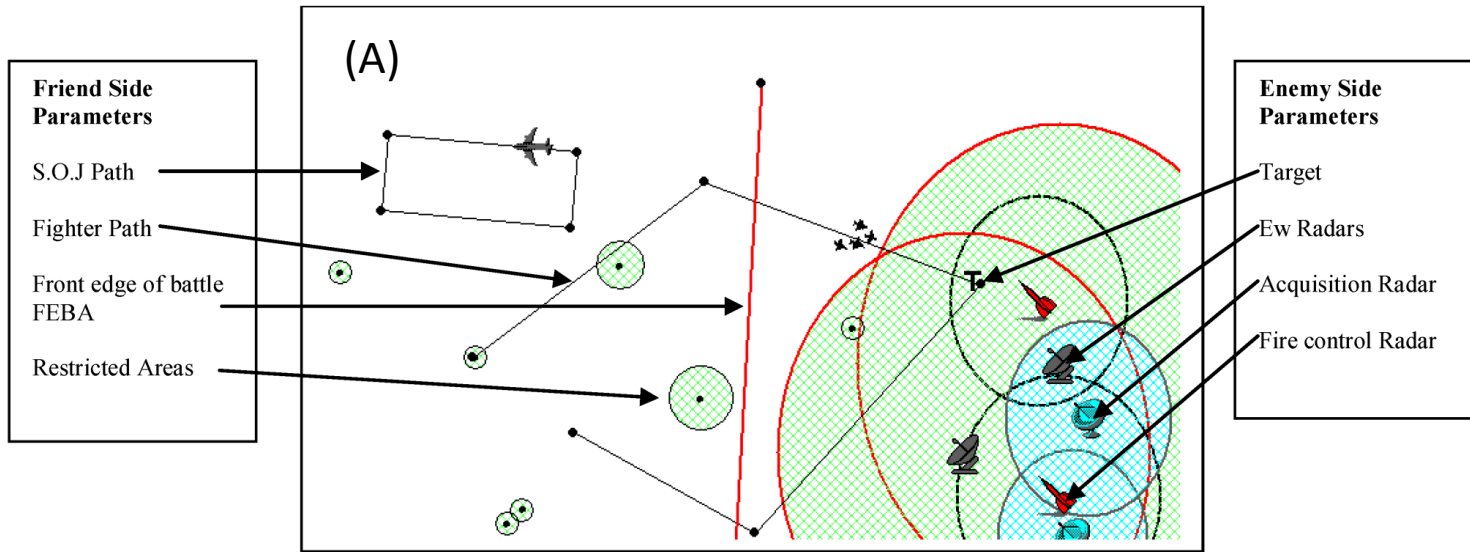
- Destruição: Conforme mencionado no parágrafo inicial que define EA.
- Desviar e distrair: Desvio da atenção e de recursos de um alvo. Ocultar outros ataques ou atrasar sua descoberta. Organizar ataques falsos para distrair o inimigo enquanto outros ataques estão ocorrendo de forma muito mais sutil.
- Distorcer: Distorcer o conteúdo físico e/ou de informações em um alvo. Distorcer o encaminhamento das ações do alvo. Gestão da percepção – distorcer a percepção do alvo através de operações psicológicas (PsyOps).
- Controle: Alimentar informações incorretas (por exemplo, imitar um sinal conhecido tão bem que o receptor não consegue distinguir o sinal falso do sinal real). Uso de várias técnicas para mascarar a identidade da parte penetrante em uma rede ou sistema.
- Atraso: Conforme mencionado no parágrafo inicial que define EA.

### Proteção Eletrônica (EP)

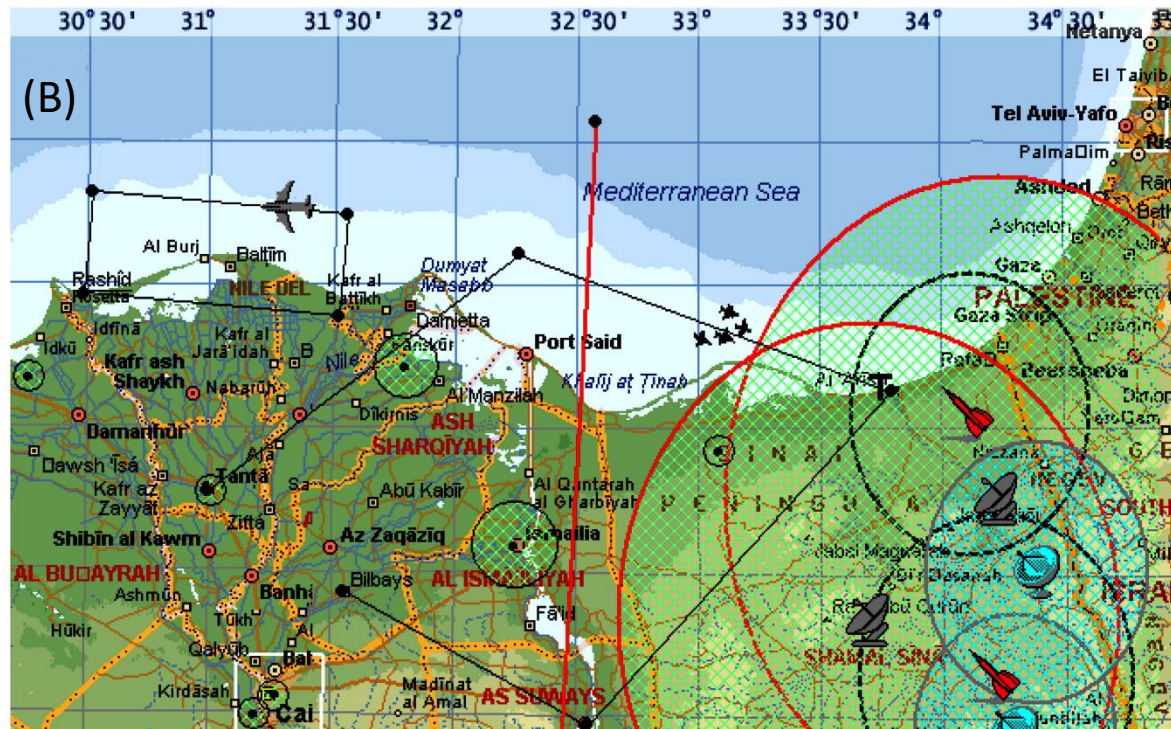
Proteção eletrônica consiste nas ações e atividades que impedem e/ou minimizam um adversário de conduzir ações de EA contra forças amigas. Exemplos de EP são criptografia do fluxo de informação e comunicações em *spread-spectrum*.



## Conceitos básicos – EOB (*Electronic Order of Battle*):



(A) é o EOB extraído do mapa táctico geral em (B)



## Conceitos básicos – efeitos a serem implementados em um teatro de operações de EW:

Qualquer teatro de operações de EW é estabelecido para fundamentalmente garantir e manter o uso do espectro eletromagnético (EMS – *electromagnetic spectrum*) para forças amigas e para negar ao inimigo uma vantagem real ou percebida neste contexto. EW pode ser aplicado de plataformas operacionais tripuladas e não-tripuladas no ar, em terra, no mar e/ou no espaço. Operações de EW são empregadas para alcançar os efeitos desejados de: controle, detecção, negação, engodo, interrupção/degradação, destruição e proteção.

Os efeitos de um cenário de operações de EW envolvem vários níveis de controle. Embora controlar o uso do EMS por meio da aplicação adequada de técnicas de EW seja vantajoso, quando as operações não são devidamente coordenadas e integradas, pode-se obter resultados inesperados, afetando adversamente as forças por meio de conflito equivocado entre facções amigas (=fratricídio) ou até eliminar alvos de alto valor para inteligência. Por exemplo, usar *jamming* em um momento inoportuno pode expor uma equipe de reconhecimento que não havia sido detectada pelo inimigo, interferindo no uso do EMS por essa equipe. As ações em um cenário de operações de EW permitem que os comandantes implementem os seguintes efeitos:

**(1) Controle:** O controle do EMS é alcançado por uma eficaz gestão/coordenação de sistemas de facções amigas enquanto se opõe aos sistemas adversários. EA limita o uso do EMS pelo adversário, EP assegura o uso do EMS para forças amigas e ES permite estimativas precisas de parte do comandante da situação na área operacional. Todos os três devem ser cuidadosamente integrados para serem eficazes. Além disso, os comandantes devem garantir a integração máxima entre EW, comunicações, ISR (*Intelligence, Surveillance and Reconnaissance* - inteligência, vigilância e reconhecimento) e outras capacidades de IO (*Information Operations* - operações de informação).

**(2) Detecção:** Detecção consiste no monitoramento ativo e passivo do campo de batalha para ameaças EM. Exemplos de ameaças EM são mísseis guiados por radio frequência (RF), dispositivos de vigilância/sinalização/orientação EO (*Electro-Optical* - eletro óptico), LASER, IR (*Infrared* - infravermelho) e UV (*ultraviolet* – ultravioleta). Esta definição reconhece que a ameaça real pode ser o adversário que está deliberadamente perpetrando a interferência EM, mas é o monitoramento do EMS que habilita as forças amigas detectarem o adversário. Monitoramento do EMS para detecção de ameaças é o primeiro passo essencial em EW para uma exploração e avaliação eficaz do cenário operacional, visando o planejamento defensivo e proteção das facções amigas engajadas no teatro de guerra. As forças amigas devem ter a capacidade de detectar e caracterizar a interferência como interferência EM hostil (*jamming*) ou não hostil (intencional ou não).



## Conceitos básicos – efeitos a serem implementados em um teatro de operações de EW:

**(3) Negação:** A negação (*denial*) consiste em controlar as informações que um adversário recebe por meio do EMS e impedir a aquisição de informações precisas sobre as forças amigas. A negação pode ser feita por técnicas tradicionais de *jamming*, contra-medidas através de *expendables* (*flares, decoys, etc ...*) ou medidas destrutivas. Eventualmente outros recursos de negação podem ser utilizados, como, por exemplo, o *denial of service* (negação de serviço) aplicado diretamente a sistemas informatizados

([https://pt.wikipedia.org/wiki/Ataque\\_de\\_nega%C3%A7%C3%A3o\\_de\\_servi%C3%A7o](https://pt.wikipedia.org/wiki/Ataque_de_nega%C3%A7%C3%A3o_de_servi%C3%A7o)).

**(4) Engodo:** Engodo (*deception*) consiste em confundir ou enganar um adversário através de informação falsa irradiada/re-irradiada através de ondas EM (e/ou acústicas), ou através de informação falsa gerada por absorção ou reflexão de ondas EM (e/ou acústicas). Através do uso do EMS (ou do espectro acústico), técnicas de engodo manipulam o ciclo de decisão do adversário, tornando difícil estabelecer uma percepção precisa da realidade objetiva. Por exemplo, durante a 2ª guerra mundial técnicas de engodo foram largamente utilizadas pelo exército alemão contra as forças aliadas (ver [https://en.wikipedia.org/wiki/German\\_Radio\\_Intelligence\\_Operations\\_during\\_World\\_War\\_II](https://en.wikipedia.org/wiki/German_Radio_Intelligence_Operations_during_World_War_II)).

**(5) Disrupção / Degradação:** Técnicas de disrupção e degradação interferem no uso do EMS pelo inimigo, inabilitando sua cadeia de comando e controle (C2) e, portanto, limitando suas capacidades de combate. Isso é obtido através de *jamming*, engodo e intrusão eletrônica. Estes três aspectos aumentam a letalidade dos ataques às forças hostis e agem como multiplicadores de força, aumentando a incerteza do adversário, enquanto reduz a incerteza para as forças amigas. As técnicas avançadas de EA oferecem oportunidade de interromper ou degradar de forma não destrutiva a infraestrutura adversária.

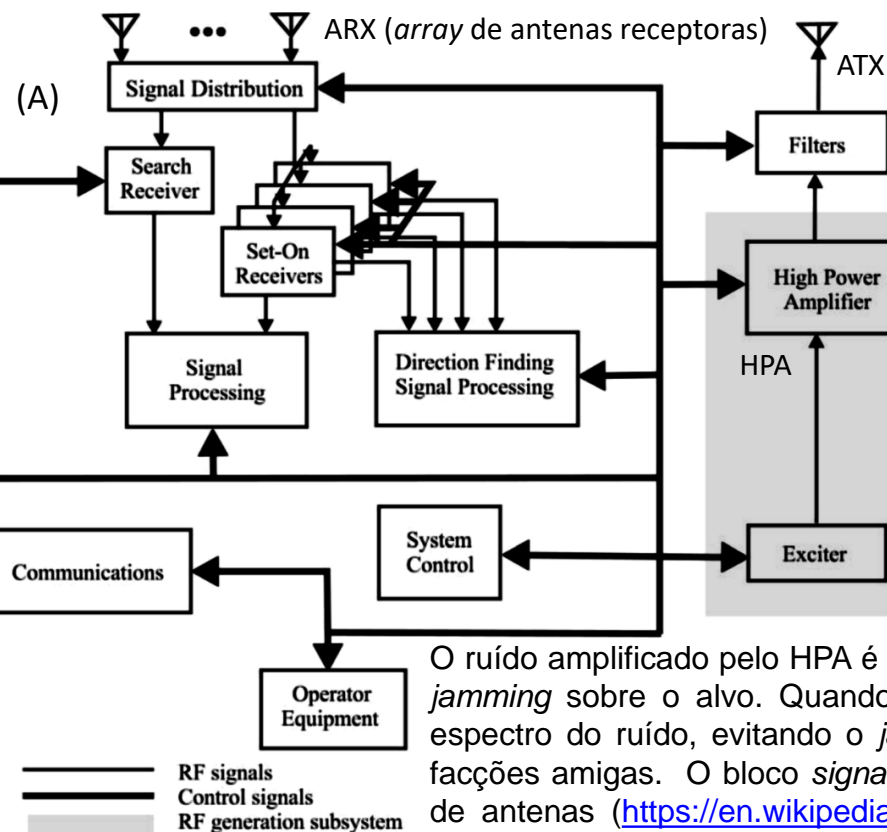
**(6) Destruição:** No contexto de EW destruição consiste na eliminação de sistemas-alvo pertencentes às forças adversárias. Sensores e nodos C2 são alvos de extrema importância estratégica porque sua destruição prejudica seriamente a percepção e a capacidade do inimigo de coordenar ações. Para efetuar a destruição de alvos, conta-se com o apoio das ações do domínio de ES para fornecer a localização do alvo, informações sobre o alvo e a avaliação de combate. Os sistemas adversários que usam o EMS podem ser destruídos por uma variedade de armas e técnicas, desde munições convencionais até armas DE (*Directed Energy* - [https://en.wikipedia.org/wiki/Directed-energy\\_weapon](https://en.wikipedia.org/wiki/Directed-energy_weapon)). Embora a destruição do equipamento adversário seja um meio eficaz de negar ao adversário o uso do EMS, a duração da negação dependerá da capacidade de recuperação do adversário.

**(7) Proteção:** Proteção consiste no uso de propriedades físicas, táticas operacionais, técnicas e procedimentos (TTP – *tactics, techniques and procedures*), bem como processos de planejamento e execução para proteger o uso do EMS pelas facções amigas. Isso inclui garantir que as atividades EW ofensivas conjuntas não desabilitem, destruam ou degradem eletronicamente sensores de informações para inteligência ou sistemas de processamento de informação de facções amigas.

Proteção é obtida através do *hardening* de componentes eletrônicos quanto aos efeitos de radiação EM e/ou ionizante (por exemplo, <https://www.militaryaerospace.com/computers/article/14035385/radiationhardened-sdram-space>), através do controle de emissão de sinais EM (para evitar que emissões EM espúrias sejam detectadas pelo inimigo), e através do gerenciamento e coordenação das frequências usadas no teatro de operações de EW. O gerenciamento e a coordenação para minimizar conflitos de frequência no cenário operacional inclui a capacidade para detectar, caracterizar, localizar geograficamente e mitigar a interferência EM que pode afetar as operações de EW. Mísseis anti-radiação são frequentemente utilizados para contra-atacar e derrotar as tentativas do adversário de controlar o EMS (por exemplo, [https://pt.wikipedia.org/wiki/AGM-88\\_HARM](https://pt.wikipedia.org/wiki/AGM-88_HARM)).



## Conceitos básicos – diagrama de blocos simplificado de um sistema básico de comunicações para EW :



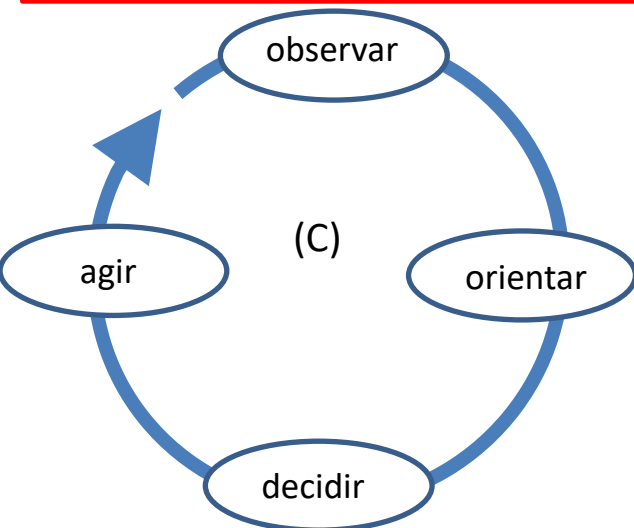
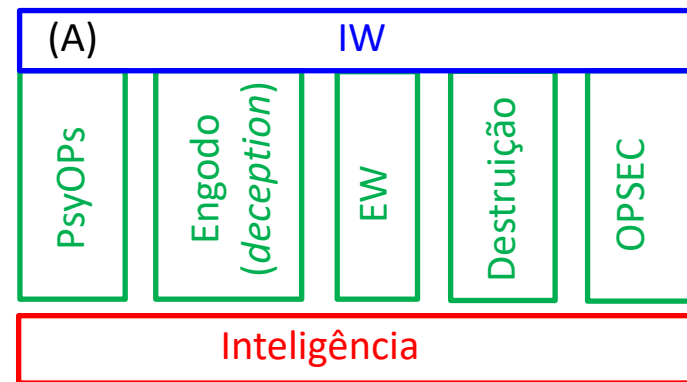
A figura (A) mostra o diagrama de blocos geral de um sistema básico de comunicações p/ EW. O excitador (*Exciter*), consiste em uma cadeia de amplificadores intermediários que excita o amplificador de potência (HPA – *High Power Amplifier*). O excitador compreende também o sintetizador de frequência que precede a cadeia de amplificadores intermediários e gera os sinais de RF com a estabilidade e precisão de frequência e fase necessárias para a operação da(s) antena(s) transmissora(s) ([https://pt.qwe.wiki/wiki/Frequency\\_synthesizer](https://pt.qwe.wiki/wiki/Frequency_synthesizer)). A antena transmissora (ATX), excitada pela potência de 1KW ou mais do HPA, é usualmente construída na forma de um *phased array*, o que permite direcionar o feixe de irradiação na direção do alvo (ver <https://apps.dtic.mil/dtic/tr/fulltext/u2/1033425.pdf> e [https://en.wikipedia.org/wiki/Phased\\_array](https://en.wikipedia.org/wiki/Phased_array)). Ainda dentro do excitador, o sinal de RF gerado pelo sintetizador na frequência do alvo a ser interferido (*jamming*) é modulado por ruído branco ([https://en.wikipedia.org/wiki/Colors\\_of\\_noise](https://en.wikipedia.org/wiki/Colors_of_noise)).

O ruído amplificado pelo HPA é irradiado pela ATX na direção do alvo de modo a efetuar a ação de *jamming* sobre o alvo. Quando necessário, filtros (*Filters*) na saída do HPA delimitam o amplo espectro do ruído, evitando o *jamming* de canais adjacentes eventualmente sendo utilizados por facções amigas. O bloco *signal distribution* efetua a combinação dos sinais provenientes do array de antenas ([https://en.wikipedia.org/wiki/Antenna\\_array](https://en.wikipedia.org/wiki/Antenna_array)) que constitui a antena receptora (ARX), combinação feita através de técnicas de *beamforming* (<https://en.wikipedia.org/wiki/Beamforming>).

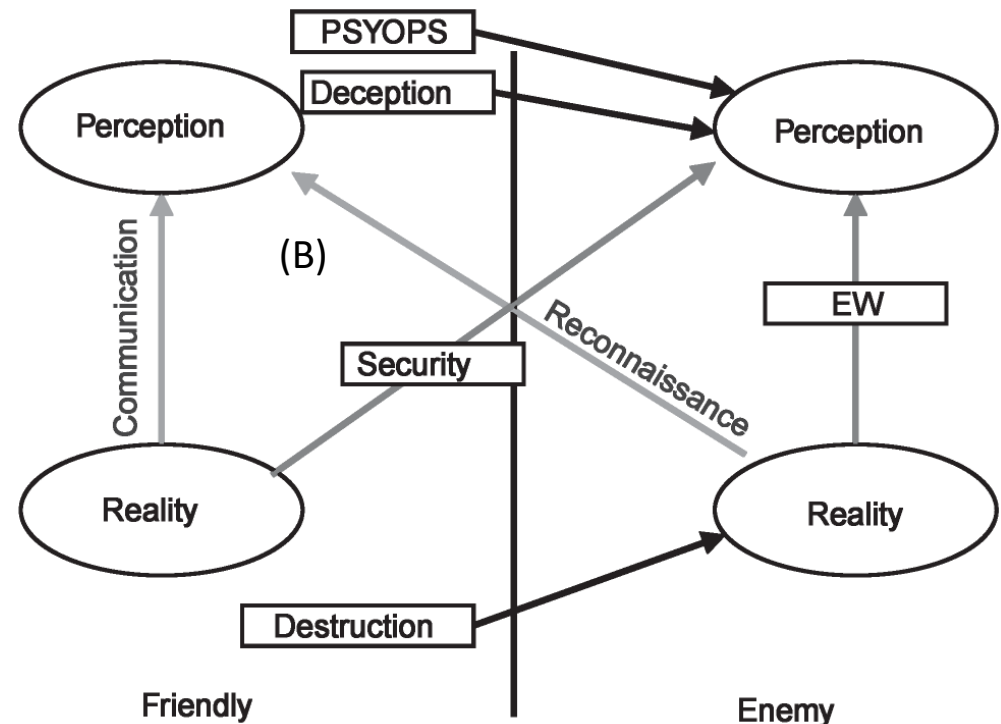
O *Search Receiver* varre constantemente o EMS (*electromagnetic spectrum*) ao longo de uma ampla faixa de frequências em busca de sinais de interesse, de maneira muito semelhante a um analisador de espectro ([https://en.wikipedia.org/wiki/Spectrum\\_analyzer](https://en.wikipedia.org/wiki/Spectrum_analyzer)). Note aqui a importância do *beamforming* acima referido, que modela o diagrama de radiação da ARX de modo a maximizar individualmente cada sinal detectado pelo *Search Receiver*. Cada um destes sinais é analisado por um respectivo receptor no banco de receptores *Set-On Receivers* (*Monitor Receivers*), que, em conjunto com o bloco *Signal Processing*, não somente identifica os parâmetros da modulação do sinal detectado como também demodula o sinal para que o operador tenha acesso à informação transmitida pelo alvo detectado. O bloco *Direction Finding Signal Processing* determina os ângulos de elevação e azimute (DOA – *Direction Of Arrival*) que cada sinal detectado pelo *Search Receiver* incide na ARX ([https://en.wikipedia.org/wiki/Direction\\_finding](https://en.wikipedia.org/wiki/Direction_finding)) e envia esta informação à ATX p/ que ela direcione seu feixe de irradiação na direção do alvo que deve sofrer o *jamming*. O *System Control* é tipicamente um computador que controla o barramento *Control signals* (por exemplo, <https://pt.wikipedia.org/wiki/FireWire>), e que opera em rede com o centro de comando através do bloco *Communications*.

## Conceitos básicos – EW é uma subdivisão de IW (*Information Warfare*):

EW é considerado parte integrante da área de guerra de informação (IW- *information warfare*), sendo EW o braço de ação de IW. IW inclui ações tomadas para preservar a integridade de seu próprio sistema de informação contra exploração, corrupção ou disrupção, enquanto ao mesmo tempo busca explorar, corromper, ou destruir o sistema de informação de um adversário. IW integra também o processo de obtenção de vantagem de informação na aplicação de força bélica. Em (A) abaixo são mostrados os chamados pilares de IW: operações psicológicas (PsyOps), engodo, guerra eletrônica (EW), destruição física e segurança operacional (OPSEC *operational security*), todos suportados pela área de inteligência. Esses elementos interferem na capacidade do inimigo de usar efetivamente suas forças armadas, conforme mostrado em (B), afetando a maneira como as instâncias envolvidas no cenário de IW percebem a realidade seja no lado amigo, seja no lado inimigo.



O ciclo OODA (observar, orientar, decidir, agir) mostrado em (C) é o processo necessário para se ter eficácia nas ações de IW. IW interfere com as três primeiras etapas do ciclo OODA, com EW sendo o 4º elemento do ciclo (ação).



## Detecção de ameaças:

EW é, por natureza, reativa a ameaças. Os receptores EW são projetados para detectar, identificar e localizar ameaças, e as contra-medidas de EW são projetadas para reduzir a eficácia dessas ameaças. Neste contexto é necessário avaliar o conjunto de ameaças em EW de maneira integrada: as classes de ameaças, as plataformas que são por elas ameaçadas, os sinais associados a elas e as classes de contramedidas usadas contra elas.

Ameaças são propriamente os reais dispositivos e sistemas com poder destrutivo. No entanto, EW considera como sendo ameaça os sinais associados a estes dispositivos e sistemas com poder destrutivo.

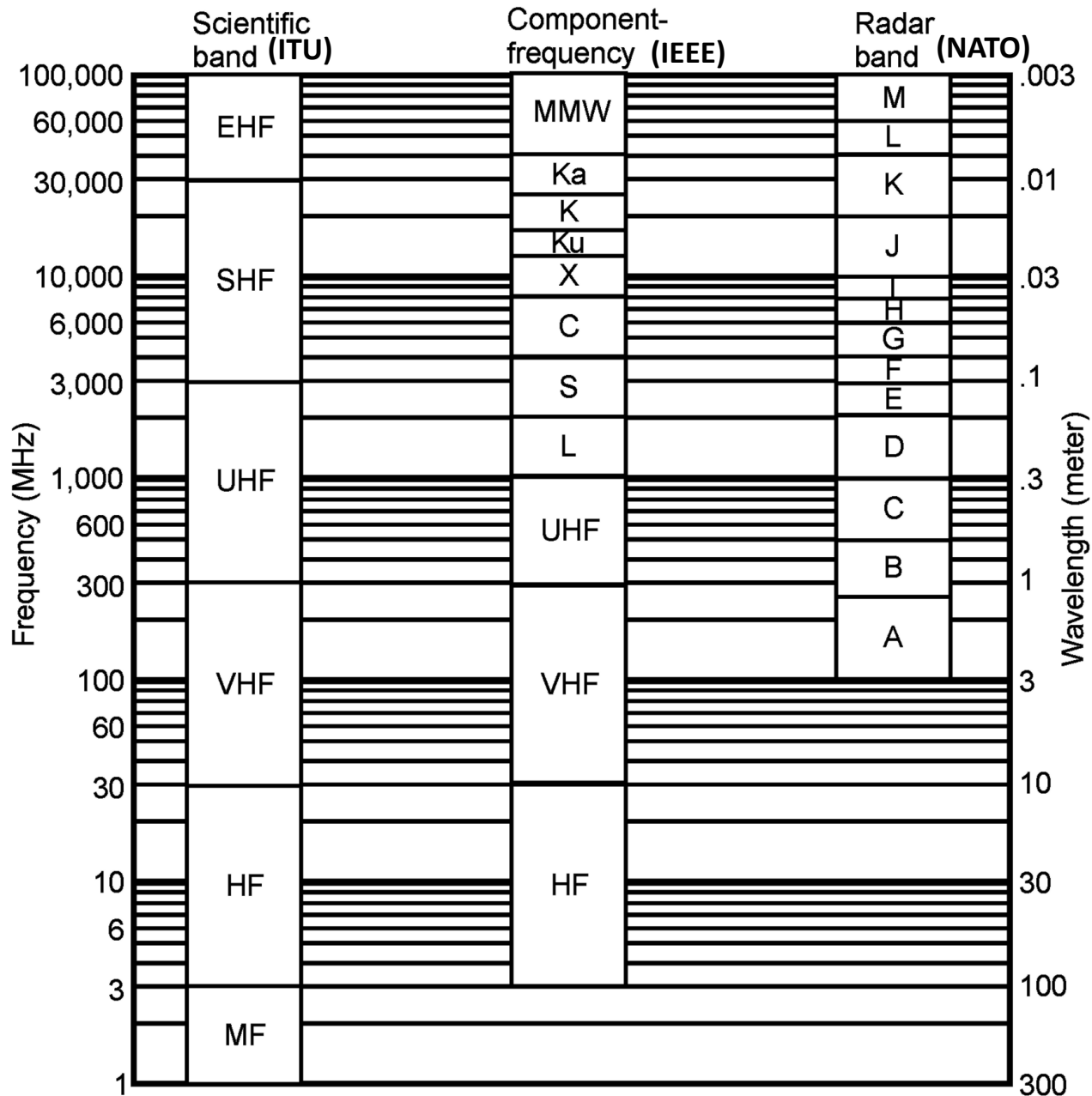
É usual dividir os sinais de ameaça em duas grandes classes: **sinais de radar** e **sinais de comunicações**. Sinais de radar são usados para medir a localização, distância e velocidade, enquanto que sinais de comunicação transportam informação de um ponto a outro. Embora tenham funções totalmente diferentes, os dois tipos de sinais podem ter parâmetros semelhantes. Os sinais de radar podem ser de onda pulsada ou de onda contínua, enquanto que sinais de comunicação são, por natureza, contínuos (exceto em casos especiais raros).

O espectro dos sinais de radar está tipicamente localizado nas faixas de frequências S, C e X de micro-ondas do EMS (*electromagnetic spectrum*) – ver tabela de faixas de frequências no próximo slide (nomenclatura IEEE). Alguns radares com funções específicas podem utilizar sinais com espectro em faixas de frequências tão baixa quanto a faixa de VHF ([https://www.youtube.com/watch?v=nvl\\_tj67jm8](https://www.youtube.com/watch?v=nvl_tj67jm8)) ou mesmo em HF (<https://ioos.noaa.gov/project/hf-radar/>). Outros radares utilizam sinais com espectro em faixas tão altas como a faixa MMW (*millimeter-wave*) (<https://www.arrow.com/en/research-and-events/articles/millimeter-wave-radar>).

Os sinais de comunicação podem transportar voz, vídeo e/ou dados. O espectro destes sinais normalmente ocorrem nas faixas de frequência HF, VHF ou UHF. No entanto, eles podem ser encontrados desde a faixa VLF até a faixa de ondas milimétricas MMW.

As ameaças são identificadas a partir dos parâmetros do sinal por elas irradiado. Cada sinal, ao ser recebido pelo sistema de EW (ver slide 11), é identificado, caracterizado e catalogado em uma base de dados. Estes parâmetros são basicamente: (1) a curva de magnitude do espectro do sinal, a frequência central do espectro e a magnitude do sinal nesta frequência, (2) o tipo de modulação do sinal e os parâmetros da modulação (de modo que o sinal possa ser demodulado, tanto para uma modulação analógica como para uma modulação digital), (3) o padrão de varredura espacial do diagrama de irradiação da antena transmissora, (4) Se o sinal for de radar, o intervalo de repetição e a largura dos pulsos transmitidos pelo radar.





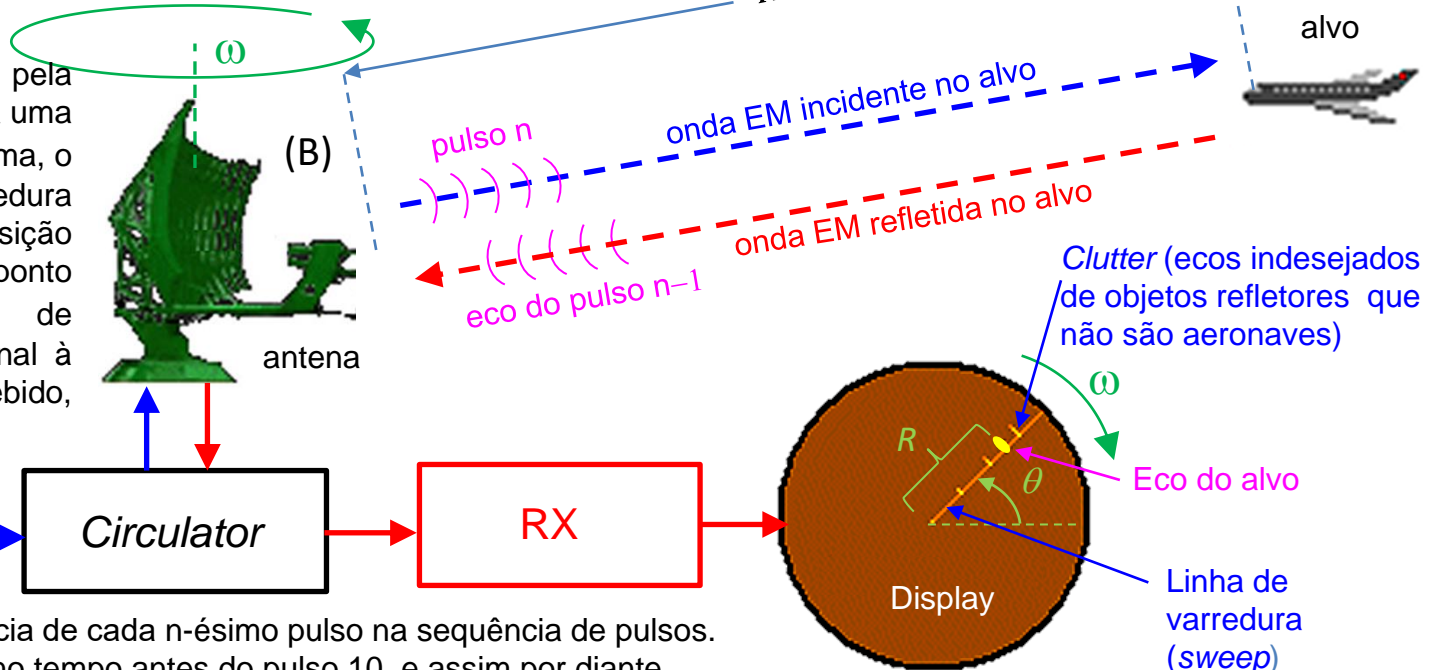
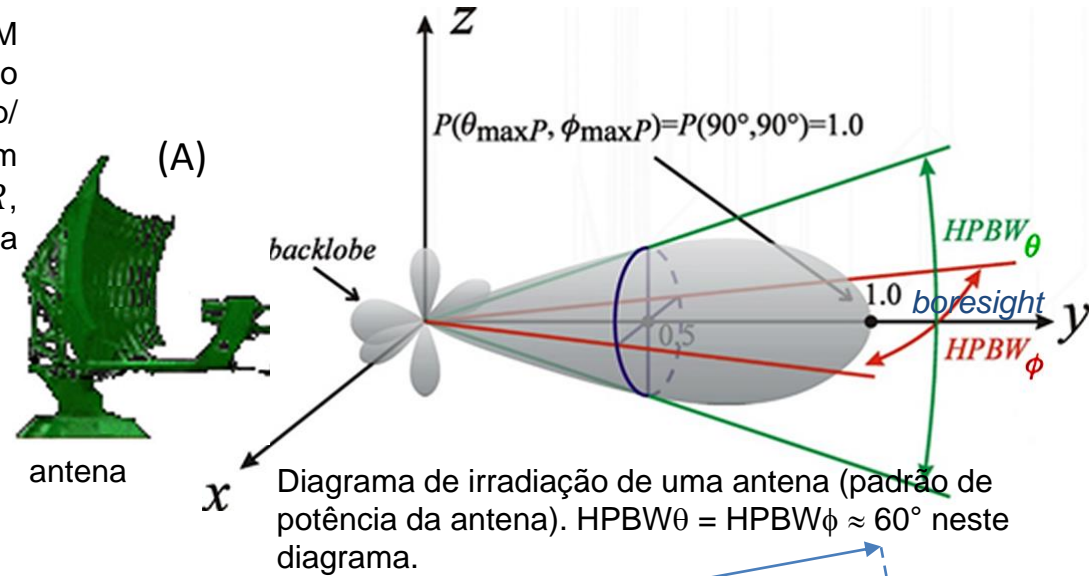


## Detecção de ameaças – sinais de radar:

Enquanto a antena gira com velocidade  $\omega$ , a onda EM gerada pelos pulsos de RF da Magnetron se propaga no espaço confinada no feixe de irradiação da antena. Se, p/ um azimute  $\theta$  de giro da antena a onda EM incidir em um alvo refletor e interceptar o mesmo a uma distância  $R$ , então os pulsos serão refletidos de volta p/ a antena na forma de ecos, conforme mostrado em (B).

Após o *Receiver* detectar os pulsos refletidos (ecos), o bloco *Video Processing* (ver diagrama no slide anterior) mede o tempo  $t_0$  que cada n-ésimo pulso e respectivo eco na onda EM demoram para percorrer a distância  $2R$  no trajeto antena  $\rightarrow$  alvo  $\rightarrow$  antena e determina a distância  $R$  entre alvo e antena (*target range*) através de  $R = 0.5 c t_0$ , onde  $c = 2.9979246 \times 10^8$  m/s é a velocidade de propagação da onda EM.

Para cada alvo interceptado pela onda EM irradiada pela antena a uma distância  $R$  e azimute  $\theta$  da mesma, o Display, cujo cuja linha de varredura (*sweep*) acompanha a posição angular da antena, plota um ponto nas coordenadas  $(R, \theta)$  de intensidade luminosa proporcional à intensidade do eco recebido, conforme mostrado em (B).



**Nota:** "n" é o índice de ocorrência de cada n-ésimo pulso na sequência de pulsos. Por exemplo, o pulso 9 ocorre no tempo antes do pulso 10, e assim por diante.

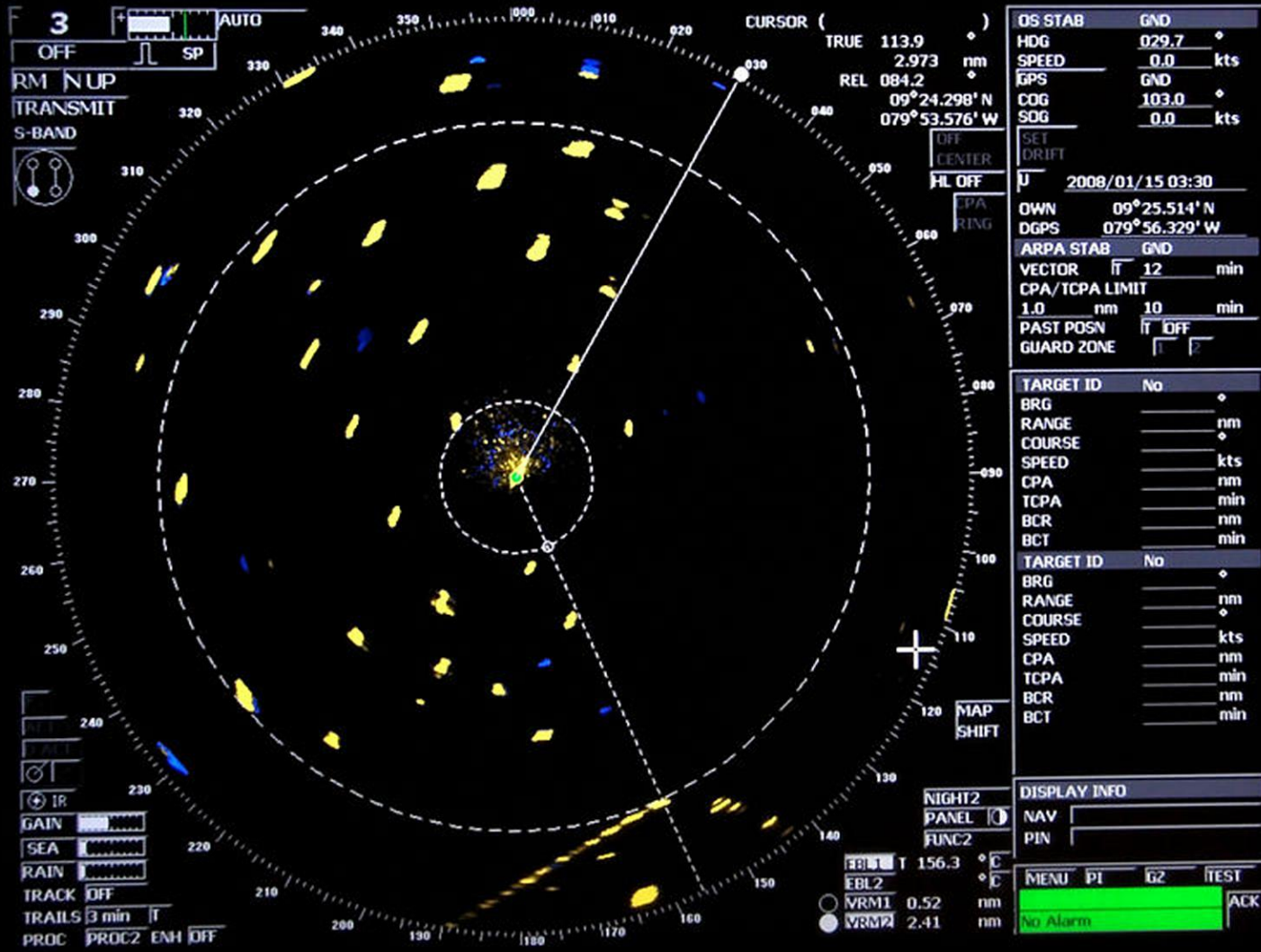


## Detecção de ameaças – display de um radar aeronáutico:



IFF – *Identify Friend or Foe* ver <http://sistemasdearmas.com.br/ca/cid1intro.html>

# Detecção de ameaças – display de um radar marítimo:



OS STAB GND  
HDG 029.7  
SPEED 0.0  
GPS GND  
COG 103.0  
SOG 0.0

SET DRIFT  
2008/01/15 03:30

OWN 09°25.514' N  
DGPS 079°56.329' W

ARPA STAB GND  
VECTOR 12 min  
CPA/TCPA LIMIT 1.0 nm 10 min  
PAST POSN OFF  
GUARD ZONE

TARGET ID No  
BRG  
RANGE nm  
COURSE  
SPEED kts  
CPA nm  
TCPA min  
BCR nm  
BCT min

TARGET ID No  
BRG  
RANGE nm  
COURSE  
SPEED kts  
CPA nm  
TCPA min  
BCR nm  
BCT min

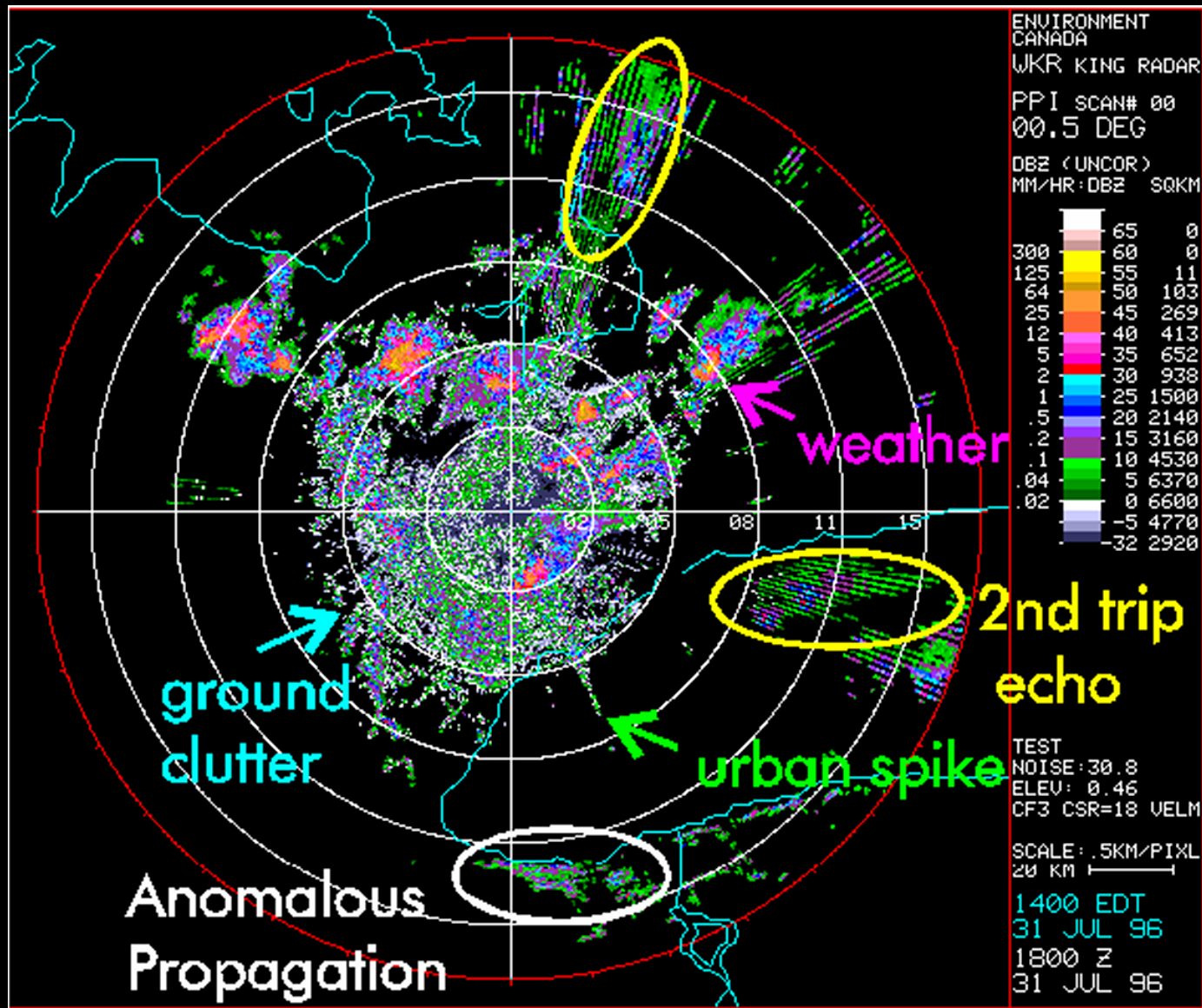
DISPLAY INFO  
NAV  
PIN

MENU PI GZ TEST  
No Alarm ACK

IR  
GAIN  
SEA  
RAIN  
TRACK OFF  
TRAILS 3 min  
PROC PROC2 ENH OFF

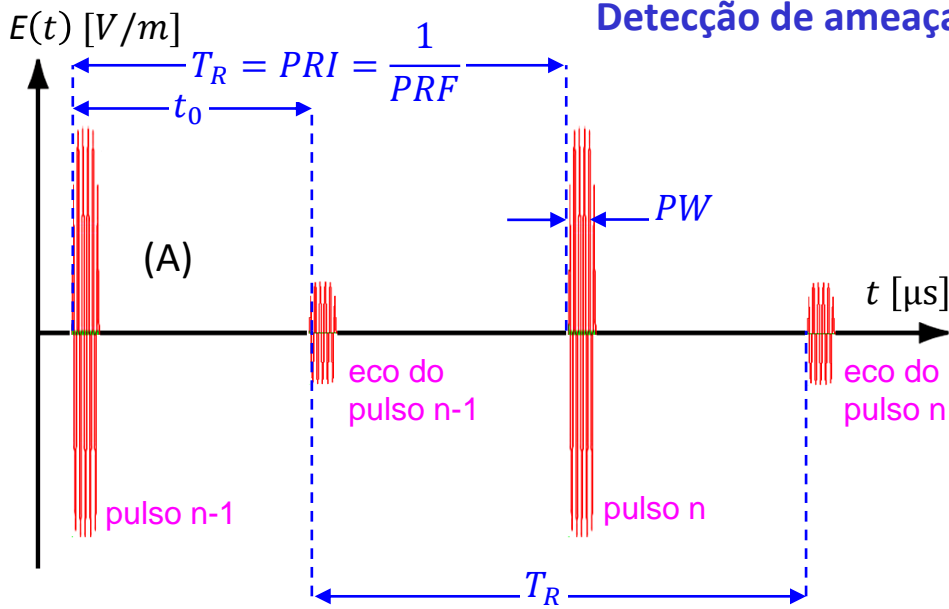
NIGHT2  
PANEL  
FUNC2  
EBL2  
VRM1 0.52 nm  
VRM2 2.41 nm

# Detecção de ameaças – display de um radar meteorológico:

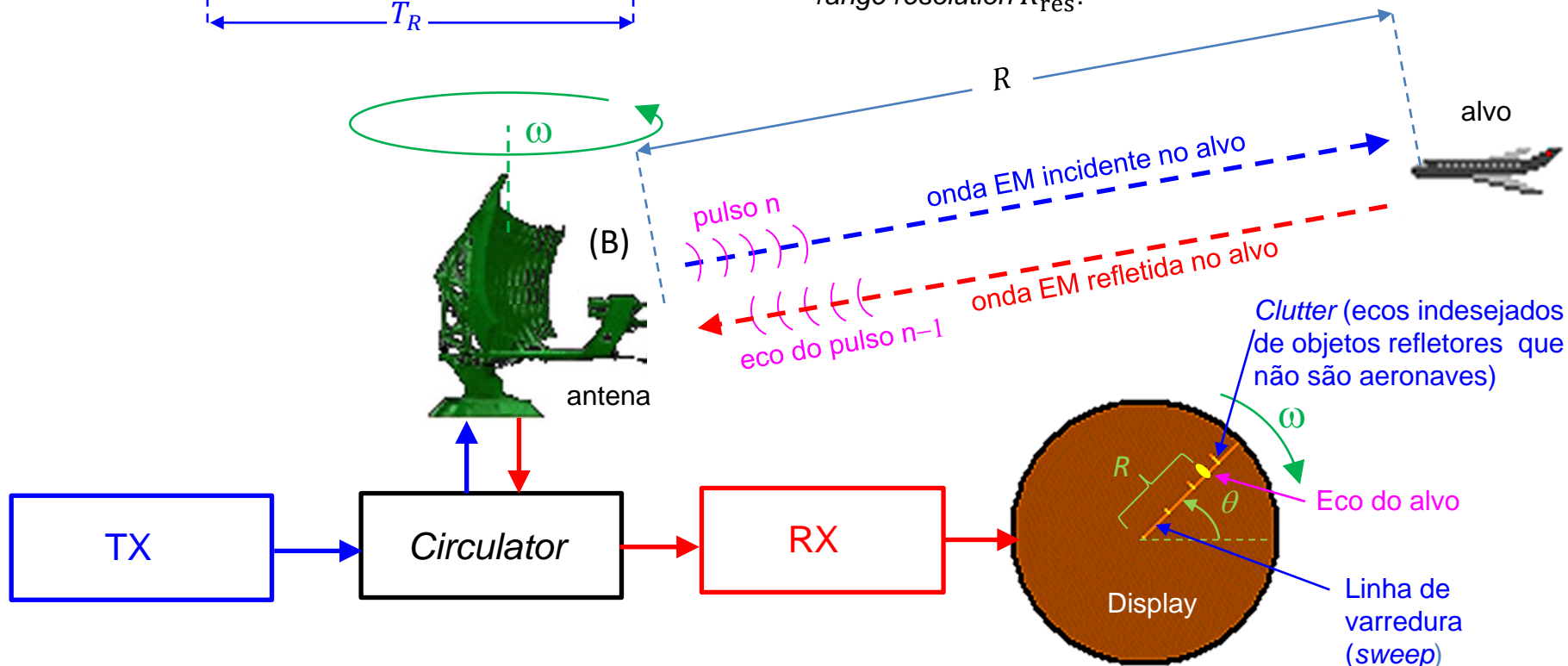




## Detecção de ameaças – sinais de radar:



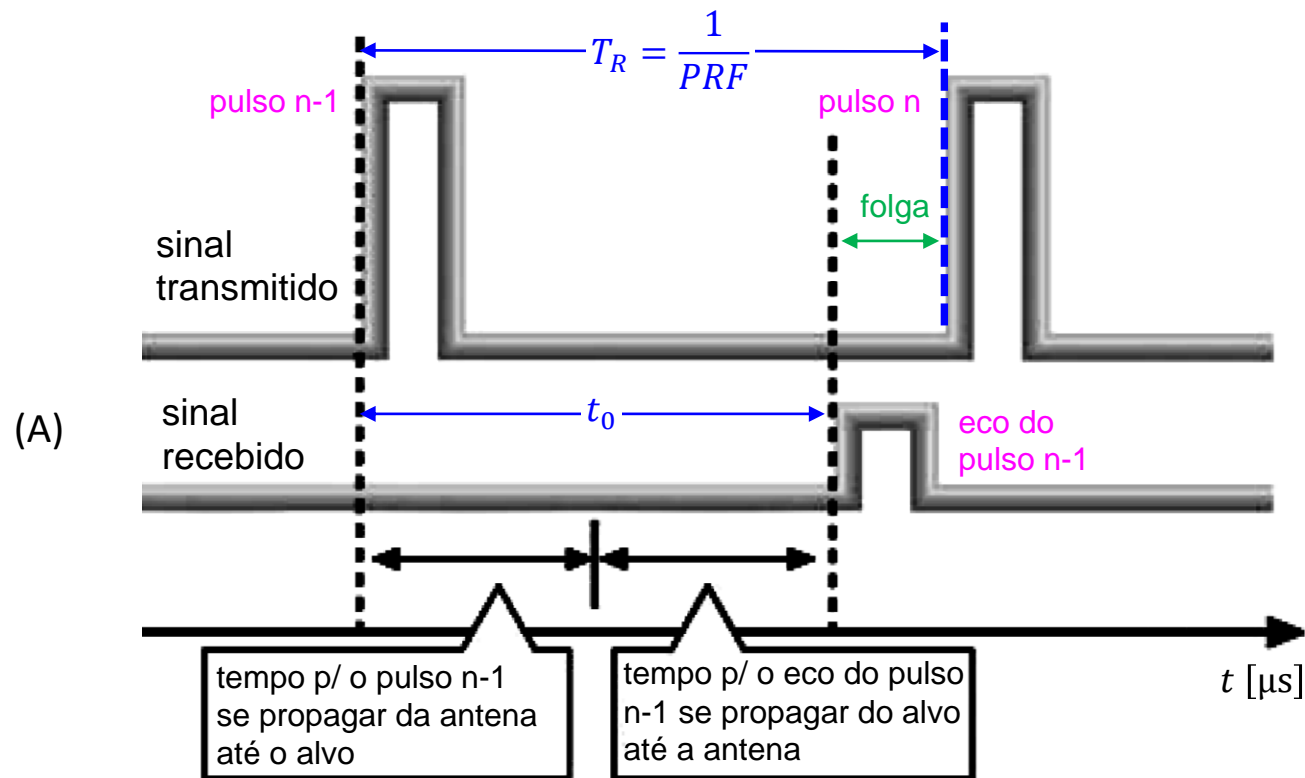
**Exemplo 1:** Um radar opera com um *pulse repetition frequency*  $PRF = 1/T_R = 10\text{KHz}$ , sendo  $T_R$  o *pulse repetition interval (PRI)* conforme mostrado em (A). O bloco *Video Processing* (ver diagrama no slide 15) mediu o tempo  $t_0 = 20\mu\text{s}$  que cada pulso e respectivo eco na onda EM demoram para percorrer a distância  $2R$  no trajeto antena→alvo→antena mostrado em (B). O *duty cycle* (razão entre a largura de pulso  $PW$  e o intervalo  $T_R$  de repetição dos pulsos) é  $\delta = PW/T_R = 0.1$ . **Pede-se:** (a) Determine o *target range*  $R$ . (b) Determine o *maximum unambiguous range*  $R_{\text{max}}$ . (c) Determine o *minimum range*  $R_{\text{min}}$  e o *range resolution*  $R_{\text{res}}$ .



## Detecção de ameaças – sinais de radar:

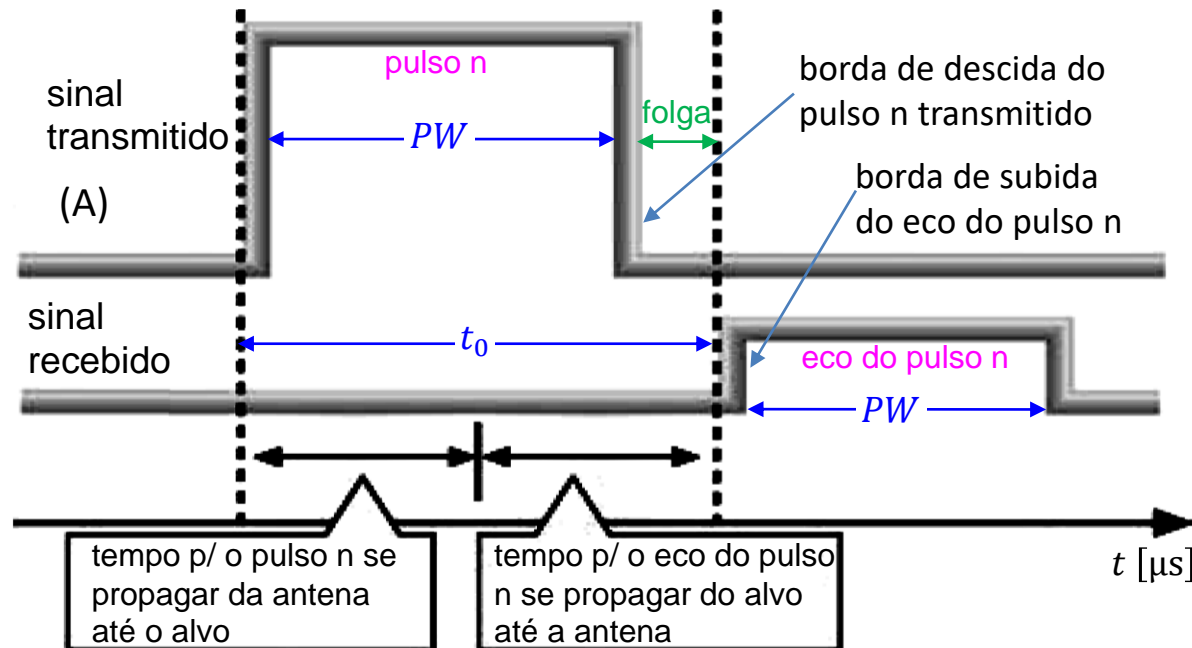
**Solução: (a)** Conforme discutido no slide 16, a distância  $R$  entre alvo e antena (*target range*) é dada por  $R = 0.5 c t_0 = 2.998\text{Km}$ , sendo  $t_0 = 20\mu\text{s}$  dado no enunciado e sendo  $c = 2.9979246 \times 10^8\text{m/s}$  a velocidade de propagação da onda EM.

**(b)** Para um dado  $T_R = 1/PRF$  (=PRI), o *maximum unambiguous range*  $R_{\text{max}}$  é a máxima distância entre antena e alvo para que o eco do pulso n-1 tenha tempo de retornar à antena antes que o pulso n seja por ela transmitido, conforme pulsos em banda-base mostrados em (A). Se a distância entre antena e alvo for maior que  $R_{\text{max}}$  resultará que o eco do pulso n-1 será considerado o eco do pulso n, gerando ambiguidade na determinação do range  $R$ . Para que esta situação não ocorra, o tempo  $t_0$  que o pulso n-1 e respectivo eco levam para percorrer a distância  $2R_{\text{max}}$  no trajeto antena→alvo→antena deve ser **no máximo** igual a  $T_R$ , situação limite em que o intervalo “folga” mostrado em (A) será nulo. Portanto, o *maximum unambiguous range* é  $R_{\text{max}} = 0.5 c t_0\text{max} = 0.5 c T_R = 0.5 c /PRF = 14.99\text{Km}$ , sendo  $PRF = 10\text{KHz}$  dado no enunciado. Note portanto que o PRF deve ser proporcionalmente reduzido para evitar ambiguidade na determinação do range  $R$  à medida que a distância  $R_{\text{max}}$  até o alvo necessita ser aumentada.



## Detecção de ameaças – sinais de radar:

(c) O *minimum range*  $R_{\min}$  é a mínima distância entre antena e alvo p/ que a borda de descida do pulso n transmitido ocorra antes que a borda de subida do eco do pulso n, conforme pulsos em banda-base mostrados em (A). Dado que o RX do radar é desabilitado enquanto o TX está ativo, basta que a distância entre antena e alvo seja apenas pouco menor que  $R_{\min}$  p/ que a borda de subida do eco do pulso n seja interferida pela borda de descida do pulso n transmitido. Para que esta situação não ocorra, o tempo  $t_0$  que o pulso n e respectivo eco levam p/ percorrer a distância  $2R_{\min}$  no trajeto antena→alvo→antena deve ser **no mínimo** igual à largura  $PW$  dos pulsos, situação limite em que o intervalo “folga” mostrado em (A) será nulo. Portanto, o *minimum range* é  $R_{\min} = 0.5 c t_0 \min = 0.5 c PW = 0.5 c \delta T_R = 0.5 c \delta / PRF = 1.499 \text{Km}$ , sendo  $\delta = PW/T_R = 0.1$  e  $PRF = 1/T_R = 10 \text{KHz}$  dados no enunciado. Note portanto que a largura  $PW$  dos pulsos deve ser proporcionalmente reduzida p/ evitar interferência na borda de subida dos ecos dos pulsos à medida que a distância  $R_{\min}$  até o alvo necessita ser diminuída em consequência da proximidade do alvo. Por exemplo, radares aeronáuticos coordenam o tráfego aéreo em aeroportos, situação em que os alvos podem estar próximos da antena do radar na aproximação final para pouso, demandando não raro a operação sob um  $R_{\min}$  de apenas algumas centenas de metros. Para evitar uma consequente largura  $PW$  dos pulsos muito pequena (que resultaria em uma largura espectral muito grande do sinal irradiado, interferindo em outros serviços) é usual adotar técnicas de compressão de pulso no processamento de sinal do RX, não somente para reduzir o *minimum range*  $R_{\min}$  como também para aumentar a precisão do *range resolution*  $R_{\text{res}} = 0.5 c PW$  (ver <https://www.radartutorial.eu/01.basics/Range%20Resolution.en.html>).

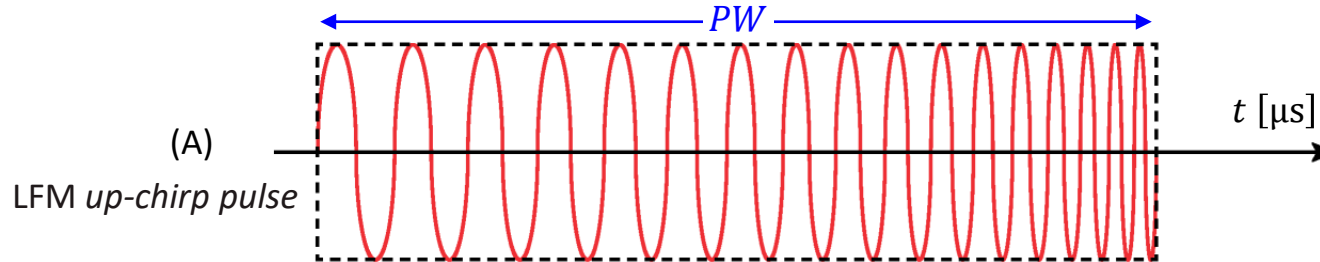


O *range resolution* é a capacidade do sistema de radar distinguir entre dois ou mais alvos posicionados ao longo de uma reta que parte da antena do radar alinhada na direção dos alvos. A mínima distância de separação entre os alvos ao longo da reta que permita a detecção dos mesmos sem superposição espacial entre os alvos na tela do radar é dada pelo *range resolution*  $R_{\text{res}} = 0.5 c PW$ , que será tanto mais preciso quanto menor for a largura  $PW$  do pulso transmitido. Para os valores dados do enunciado,  $R_{\text{res}} = 0.5 c PW = 1.499 \text{Km}$ .



## Detecção de ameaças – sinais de radar:

Uma das técnicas para compressão de pulso que discutiremos adiante nos slides 70 e 71 (Cap I.3) é a modulação LFM (*Linear Frequency Modulation*) ou *chirp modulation*. Cada pulso transmitido é modulado em frequência, conforme mostrado em (A) (ver <https://www.radartutorial.eu/08.transmitters/Intrapulse%20Modulation.en.html>). O processamento de sinal do RX faz o pulso LFM transmitido ser “visto” pelo RX com uma largura reduzida que é uma fração da largura PW do pulso transmitido, conforme discutiremos no slide 71.



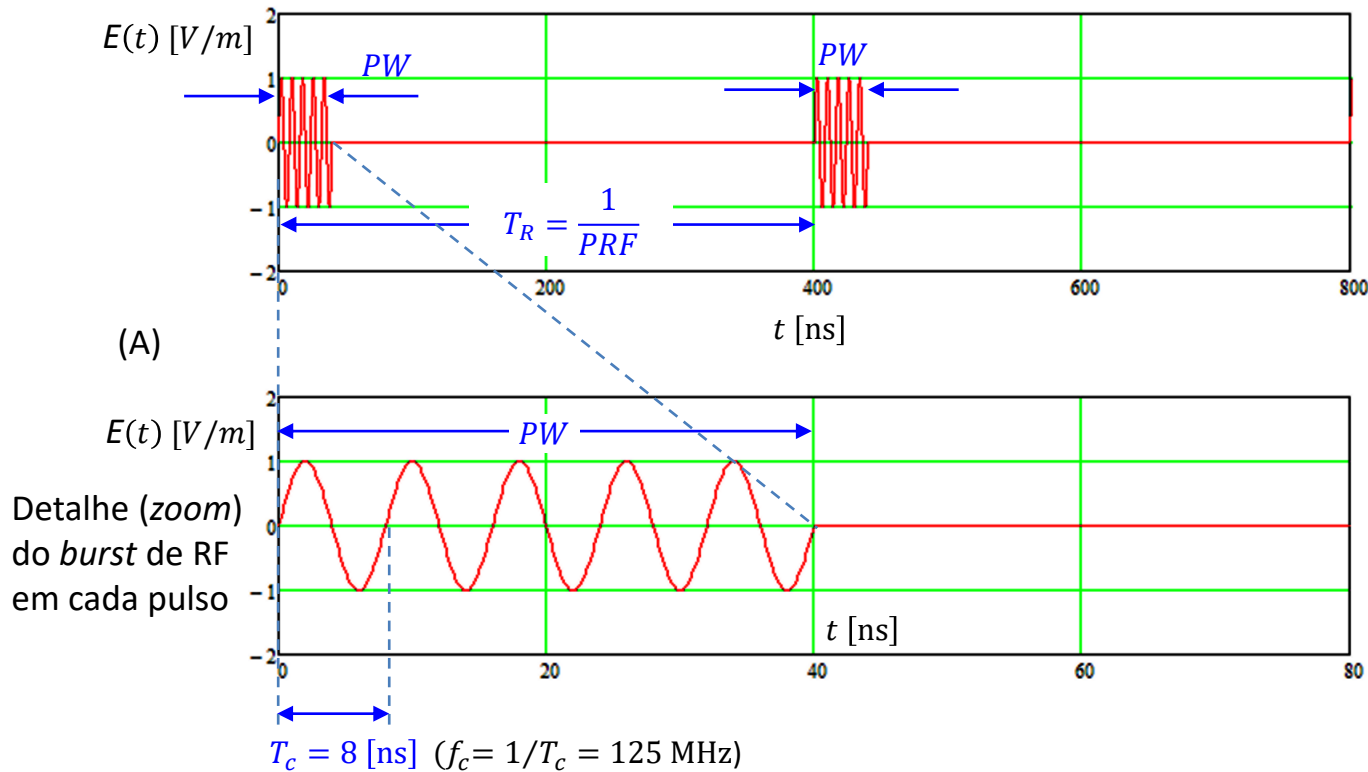
A modulação LFM também é adotada em radares FMCW (*Frequency Modulated Continuous Wave*), cujo método de determinação do *target range* discutiremos no Exemplo 4 do slide 38.

Neste capítulo nosso interesse específico é identificar ameaças através dos sinais irradiados por elas, tarefa que está ao encargo do *Search Receiver* e do banco de receptores *Set-On Receivers* (também conhecidos por *Monitor Receivers*) conforme slide 11, e que, em conjunto com o bloco *Signal Processing*, identificam os parâmetros da modulação do sinal detectado a partir basicamente do espectro do sinal determinado pelo *Search Receiver*. A demodulação do sinal em si é um processo simples se o sinal é analógico, mas se o sinal é digital o processo é muito mais complicado. Isto ocorre porque um sinal digital envolve inúmeros tipos possíveis de modulação digital, inúmeros tipos possíveis de códigos corretores de erro e inúmeros tipos possíveis de códigos para compressão do *stream* de bits (ver [http://www.fccdecastro.com.br/pdf/T2\\_Aula2\\_13032020.pdf](http://www.fccdecastro.com.br/pdf/T2_Aula2_13032020.pdf)). Sem saber os parâmetros da modulação e dos códigos é bastante complicado demodular o sinal digital, sem falar da criptografia aplicada ao *stream* de bits demodulado em alguns sistemas. Por exemplo, o padrão digital APCO 25 usa várias possíveis criptografias no *stream* de bits demodulado (ver [https://pt.qwe.wiki/wiki/Project\\_25](https://pt.qwe.wiki/wiki/Project_25)), entre elas o AES-256. Mas, no caso de sinais de radar, muitas informações podem ser obtidas apenas do espectro do sinal recebido, conforme exemplos que seguem. A solução destes exemplos foram implementadas com o auxílio de *scripts* do software MathCad. Uma versão “free” do MathCad 14 pode ser obtida p/ *download* em

[https://www.dropbox.com/sh/3wtjenppcic9c5c/AABvk3Rlf\\_xDxfOIH6Hphgza?dl=0MathCad14.rar&preview=MathCad14.rar](https://www.dropbox.com/sh/3wtjenppcic9c5c/AABvk3Rlf_xDxfOIH6Hphgza?dl=0MathCad14.rar&preview=MathCad14.rar).

## Detecção de ameaças – sinais de radar:

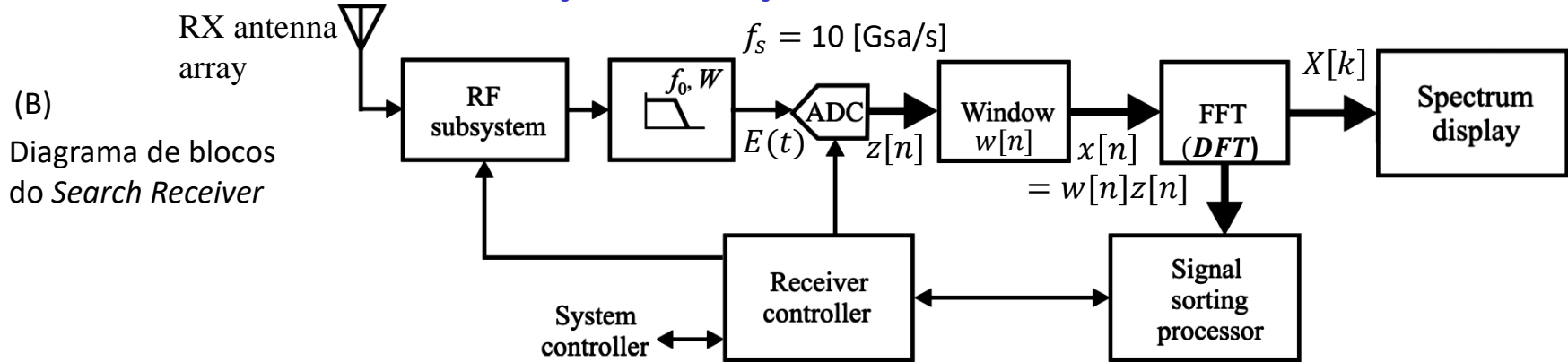
**Exemplo 2:** Um radar inimigo opera na banda A (OTAN – ver slide 14) e sua antena irradia uma sequência de pulsos de radiofrequência (*bursts* de RF) com valor normalizado do campo elétrico da onda EM irradiada conforme mostrado em (A).



O campo elétrico  $E(t)$  [V/m] irradiado mostrado em (A) é captado pelo *array* de antenas receptoras de um sistema de EW (ver (A) no slide 11), cujo bloco *Search Receiver* converte o campo  $E(t)$  [V/m] em um sinal de tensão analógico  $E(t)$  [V] conforme mostrado no diagrama em (B) no próximo slide. O conversor A/D (=ADC) do *Search Receiver* digitaliza o sinal  $E(t)$  com frequência de amostragem  $f_s = 10$  [Gsa/s]. O objetivo do *Search Receiver* é determinar o espectro  $X[k]$  do sinal captado aplicando a DFT (*Discrete Fourier Transform*) sobre o sinal  $E(t)$  digitalizado, conforme (B) no próximo slide. Usualmente a DFT é implementada através da FFT (*Fast Fourier Transform*).

(ver [http://www.fccdecastro.com.br/pdf/SS\\_aula27a29\\_06072020.pdf](http://www.fccdecastro.com.br/pdf/SS_aula27a29_06072020.pdf))

## Detecção de ameaças – sinais de radar:



**Pede-se:** (a) Determine e plote o gráfico da magnitude do espectro  $X[k]$  que é mostrado na tela “Spectrum display” do Search Receiver em (B). (b) A partir do gráfico do espectro  $X[k]$  obtido em (a) determine o PRF (pulse repetition frequency), o PW (pulse width – largura de pulso) e a frequência  $f_c$  dos bursts de RF nos pulsos de  $E(t)$  em (A) no slide anterior.

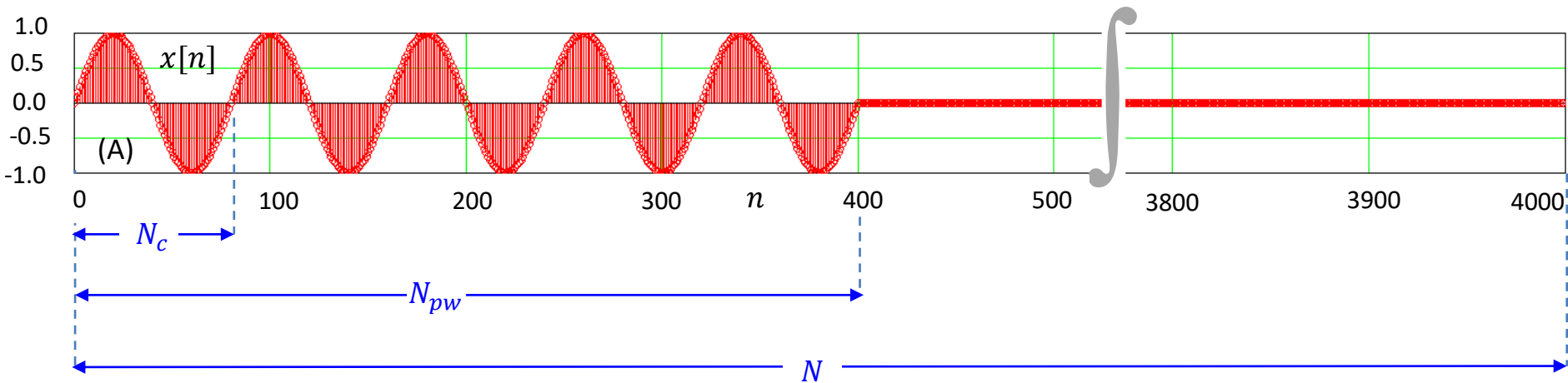
**Solução:** (a) O enunciado não especifica a sequência de amostras  $z[n]$  na saída do ADC. Portanto, para determinar  $x[n] = w[n]z[n]$  e aplicar a DFT sobre  $x[n]$  determinando o espectro  $X[k] = \text{DFT}\{x[n]\}$ , será necessário determinar  $z[n]$  a partir da definição do sinal analógico  $E(t)$  mostrado em (A) no slide anterior. Este é o 1º passo para efeito da solução do exemplo.

No entanto, é importante preliminarmente notar aqui que, na prática, sob operação em tempo real, o Search Receiver não necessita da definição analítica de  $E(t)$  para efetuar  $X[k] = \text{DFT}\{x[n]\}$ , dado que o processo realizado é inteiramente numérico, i.e., o Search Receiver simplesmente digitaliza através do ADC o sinal analógico  $E(t)$  e obtém  $z[n]$ . Daí aplica uma janela  $w[n]$  sobre  $z[n]$  obtendo  $x[n] = w[n]z[n]$  (ver [https://en.wikipedia.org/wiki/Window\\_function](https://en.wikipedia.org/wiki/Window_function)). A seguir, efetua  $X[k] = \text{DFT}\{x[n]\}$  e plota no Spectrum display a magnitude de  $X[k]$ , que representa o espectro de  $E(t)$ .

Importante notar também que, a título de aqui simplificar a obtenção de  $z[n]$  a partir de  $E(t)$ , os valores dados no enunciado nos dão liberdade de utilizar uma janela retangular  $w[n] = 1$  com um número  $N$  de amostras que faz a duração da janela ser exatamente igual a um período  $T_R$  do sinal analógico  $E(t)$ . Sendo assim, não ocorre spectral leakage e não há distorção nas componentes espectrais do espectro  $X[k]$  (ver <https://dspillustrations.com/pages/posts/misc/spectral-leakage-zero-padding-and-frequency-resolution.html>), de modo que podemos considerar  $x[n] = z[n]$ . Mas, no processo de digitalização em tempo real a ação da janela  $w[n]$  é crucial para a fidelidade do espectro (usualmente uma Blackman window ou uma Hann window - ver [https://en.wikipedia.org/wiki/Window\\_function](https://en.wikipedia.org/wiki/Window_function)), dado que  $T_R$  é desconhecido a priori impossibilitando a duração da janela  $w[n]$  ser escolhida exatamente igual a um múltiplo inteiro de  $T_R$ .

## Detecção de ameaças – sinais de radar:

Para obter a definição da sequência de amostras  $x[n] = z[n]$  na entrada da DFT a partir do sinal  $E(t)$  mostrado em (A) no slide 24, precisamos primeiramente considerar que o intervalo de tempo entre as amostras de  $x[n]$  é  $\Delta t = 1/f_s = 0.1$  ns, onde  $f_s = 10$  [Gsa/s] é a frequência de amostragem do ADC dada no enunciado. Visto que de (A) no slide 24 temos  $T_R = 400$ ns,  $PW = 40$ ns e  $T_c = 8$ ns, então o número de amostras no intervalo  $T_R$  é  $N = T_R/\Delta t = 4000$  amostras, o número de amostras no intervalo  $PW$  é  $N_{pw} = PW/\Delta t = 400$  amostras e o número de amostras no intervalo  $T_c$  é  $N_c = T_c/\Delta t = 80$  amostras, conforme mostrado em (A) abaixo.



A partir de (A) acima, a definição da sequência de amostras  $x[n]$  é portanto:

$$x[n] = \begin{cases} A \cos(\theta_c n + \phi) & p/ 0 \leq n < N_{pw} \\ 0 & p/ N_{pw} \leq n < N \end{cases} \quad (1)$$

onde  $A = 1$  é a amplitude do cosseno,  $\theta_c = \frac{2\pi}{N_c} = 0.07854$  [rad/amostra] (radiano/amostra) é a frequência digital do cosseno e  $\phi = -90^\circ$  é o ângulo de fase do cosseno (devido ao *burst* de RF ser um seno, conforme mostra (A) acima).



## Detecção de ameaças – sinais de radar:

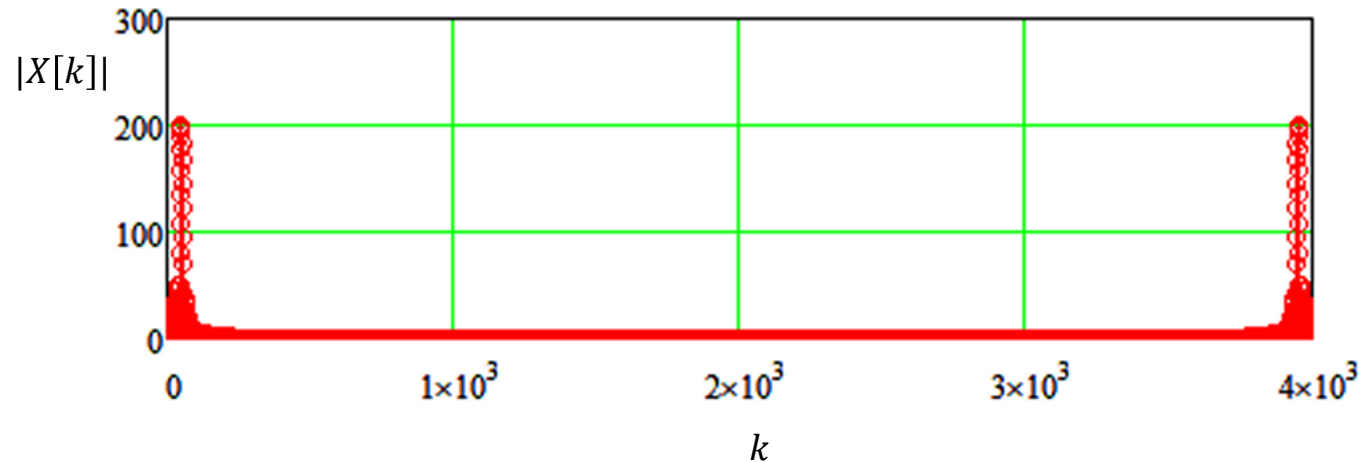
O espectro  $X[k] = \text{DFT}\{x[n]\}$  (ver [http://www.fccdecastro.com.br/pdf/SS\\_aula27a29\\_06072020.pdf](http://www.fccdecastro.com.br/pdf/SS_aula27a29_06072020.pdf)) é determinado através de

$$X[k] = \text{DFT}\{x[n]\} = \sum_{n=0}^{N-1} x[n] e^{-j(2\pi/N)nk}, \quad k = 0, 1, \dots, N-1 \quad (2)$$

Substituindo (1) em (2) temos:

$$X[k] = \text{DFT}\{x[n]\} = \sum_{n=0}^{N_{pw}} A \cos(\theta_c n + \phi) e^{-j(2\pi/N)nk}, \quad k = 0, 1, \dots, N-1 \quad (3)$$

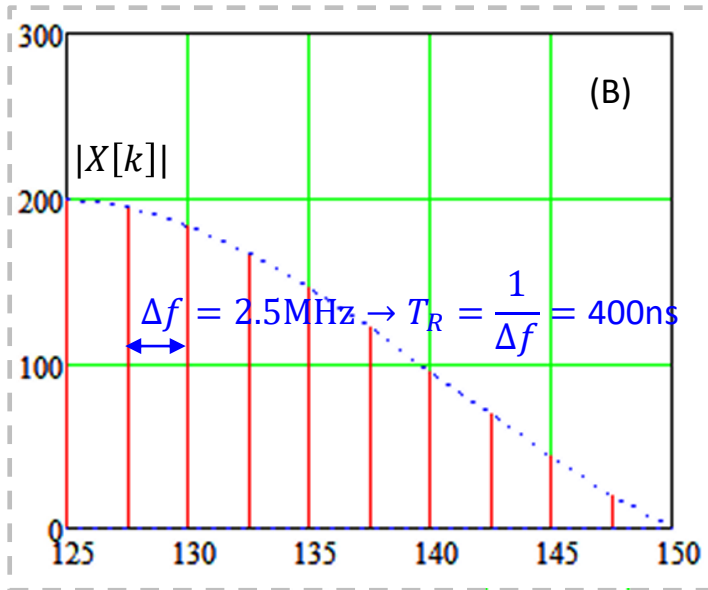
Que resulta no seguinte gráfico para a magnitude  $|X[k]|$  do espectro no domínio frequência discreta  $k$ :



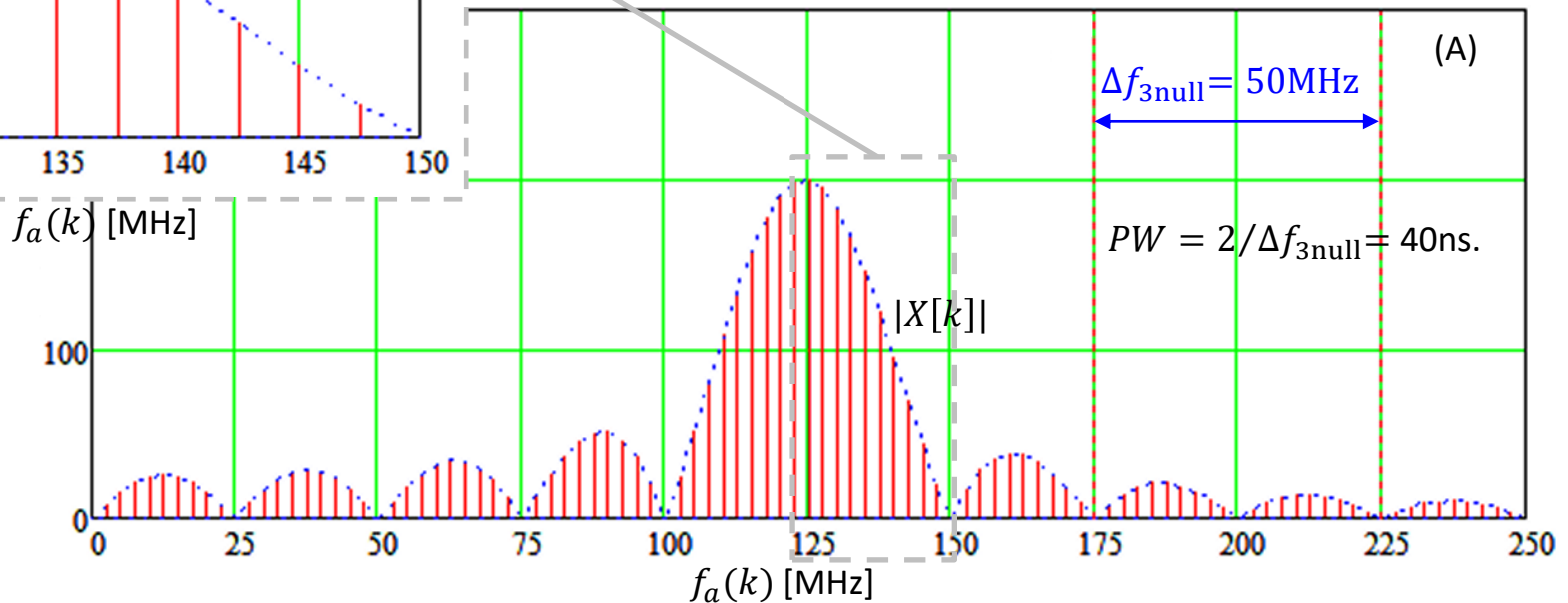
## Detecção de ameaças – sinais de radar:

Para facilitar a análise dos parâmetros do espectro  $X[k]$ , é conveniente converter o domínio frequência discreta  $k$  nas correspondentes frequências no domínio frequência analógica  $f_a$  através de

$$f_a(k) = \begin{cases} \frac{k f_s}{N} & p/ k \leq N/2 \\ \frac{(k - N) f_s}{N} & p/ k > N/2 \end{cases} \quad (4)$$



Plotando a magnitude  $|X[k]|$  do espectro de  $x[n]$  no domínio frequência analógica  $f_a(k)$  para  $f_a(k) > 0$  com  $k = 0, 1, \dots, N - 1$  (que é o que mostra a tela do *Spectrum Display* - ver slide 25), obtemos:



## Detecção de ameaças – sinais de radar:

**(b)** Em (B) no slide anterior, observa-se que a separação entre as componentes espectrais é  $\Delta f = 2.5\text{MHz}$ . O inverso de  $\Delta f$  determina o *PRI* (*pulse repetition interval*) dado por  $PRI = T_R = 1/\Delta f = 400\text{ns}$ . O inverso do *PRI* determina o *PRF* (*pulse repetition frequency*) dado por  $PRF = 1/PRI = 2.5\text{MHz}$ .

Em (A) no slide anterior, observa-se que a separação  $\Delta f_{3\text{null}}$  entre 3 nulos consecutivos da curva  $|X[k]|$  é  $\Delta f_{3\text{null}} = 50\text{MHz}$ . O *PW* (*pulse width* – largura de pulso) do sinal  $E(t)$  mostrado em (A) no slide 24 pode ser obtido através de  $PW = 2/\Delta f_{3\text{null}} = 40\text{ns}$ .

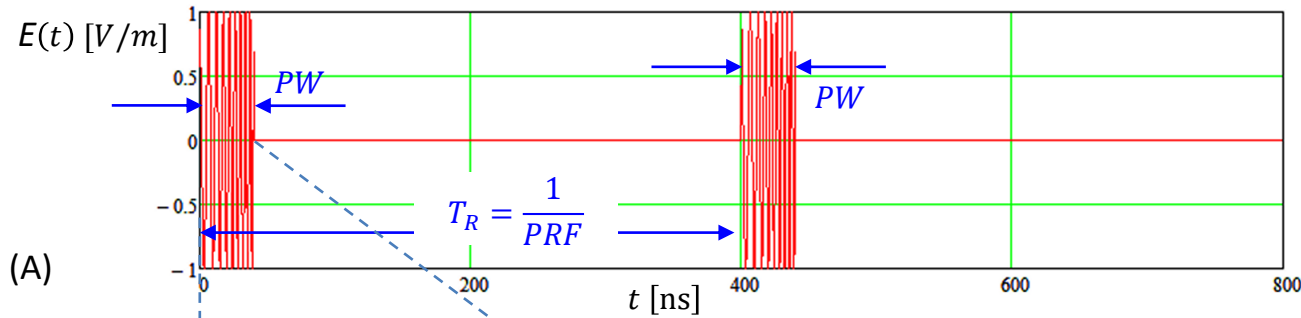
A frequência  $f_c$  dos *bursts* de RF nos pulsos do sinal  $E(t)$  mostrado em (A) no slide 24 é obtida da frequência correspondente ao máximo da curva  $|X[k]|$  no slide anterior, que por inspeção visual resulta em  $f_c = 125\text{MHz}$ .

Conforme discutido no slide 25, sob operação em tempo real o *Search Receiver* obtém o espectro de  $E(t)$  diretamente através do procedimento numérico  $X[k] = \text{DFT}\{w[n]z[n]\}$ . Portanto, na prática, o *PRF* (*pulse repetition frequency*), o *PW* (*pulse width* – largura de pulso) e a frequência  $f_c$  dos pulsos de RF do sinal  $E(t)$  irradiado pela antena do radar são determinados através de simples inspeção visual da curva da magnitude do espectro mostrada na tela “Spectrum display” do *Search Receiver* – ver diagrama de blocos em (B) no slide 25.

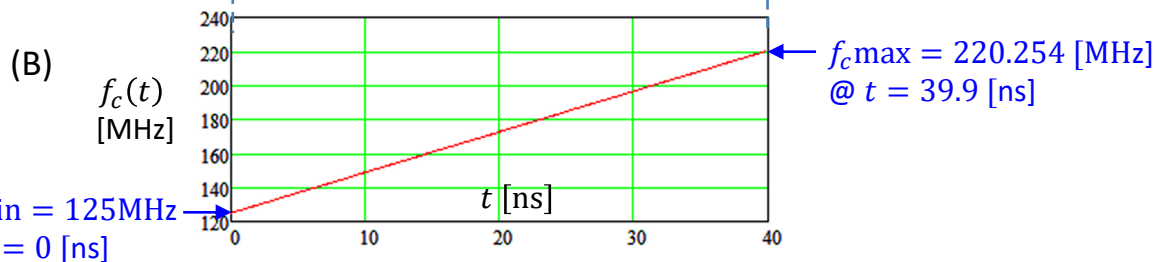
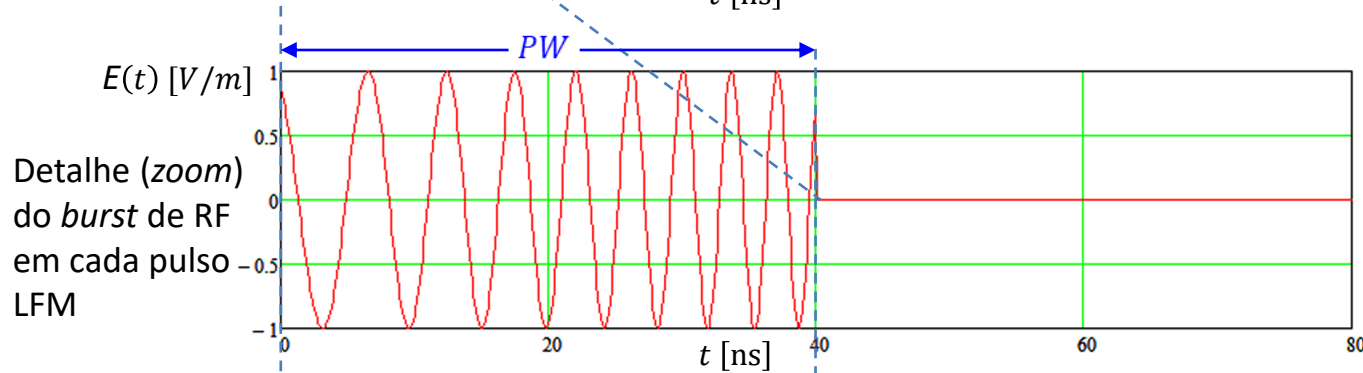
O *script* do software MathCad utilizado como auxílio na solução deste exemplo está disponível em <http://www.fccdecastro.com.br/ZIP/E2S24.zip>.

## Detecção de ameaças – sinais de radar:

**Exemplo 3:** Um radar inimigo opera na banda A e sua antena irradia uma sequência de pulsos LFM ( *Linear Frequency Modulation*) para efeito de compressão dos pulsos. O valor normalizado do campo elétrico da onda EM irradiada é conforme mostrado em (A).



Em (B) é mostrada a variação linear da frequência instantânea  $f_c(t)$  do cosseno que define o *burst* de RF em cada pulso LFM



O campo elétrico  $E(t)$  [V/m] irradiado mostrado em (A) é captado pelo *array* de antenas receptoras de um sistema de EW (ver (A) no slide 11 ), cujo bloco *Search Receiver* converte o campo  $E(t)$  [V/m] em um sinal de tensão analógico  $E(t)$  [V] conforme mostrado em (B) no slide 25. O conversor A/D (=ADC) do *Search Receiver* digitaliza o sinal  $E(t)$  com frequência de amostragem  $f_s = 10 \text{ [Gsa/s]}$ .

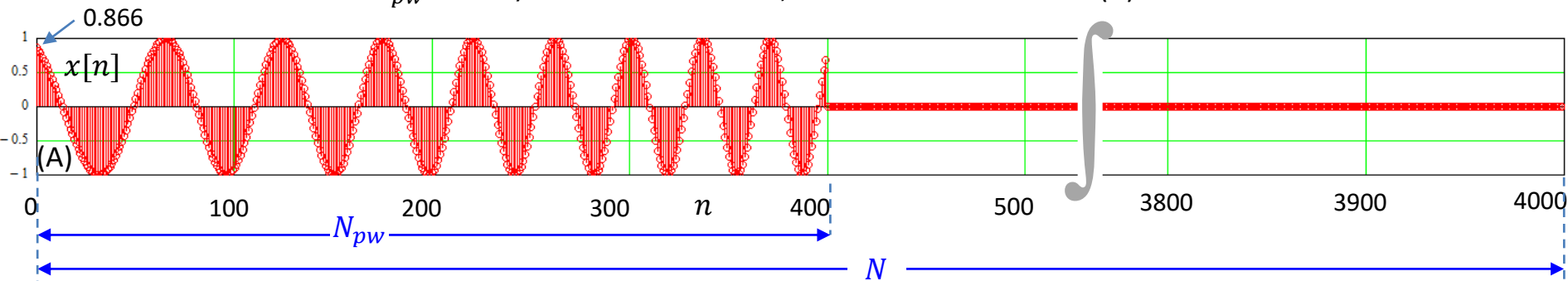
**Pede-se:** (a) Determine e plote o gráfico da magnitude do espectro  $X[k]$  que é mostrado na tela “Spectrum display” do *Search Receiver* em (B) no slide 25. (b) A partir do gráfico do espectro  $X[k]$  obtido em (a) determine o *PRF* (*pulse repetition frequency*) e o *PW* (*pulse width* – largura de pulso). Estime aproximadamente as frequências  $f_c \min$  e  $f_c \max$  do *burst* de RF em cada pulso de  $E(t)$  mostrado em (A).



## Detecção de ameaças – sinais de radar:

**Solução: (a)** O enunciado não especifica a sequência de amostras  $z[n]$  na saída do ADC. Portanto, conforme já discutido na solução do Exemplo 2, para determinar  $x[n] = w[n]z[n]$  e aplicar a DFT sobre  $x[n]$  determinando o espectro  $X[k] = \text{DFT}\{x[n]\}$ , será necessário determinar  $z[n]$  a partir da definição do sinal analógico. Assim como fizemos na solução do Exemplo 2, vamos utilizar uma janela retangular  $w[n] = 1$  com um número  $N$  de amostras que faz a duração da janela ser exatamente igual a um período  $T_R$  do sinal analógico  $E(t)$ . Sendo assim, não ocorre *spectral leakage* e não há distorção nas componentes espectrais do espectro  $X[k]$ , de modo que podemos considerar  $x[n] = z[n]$ .

Para obter a definição da sequência de amostras  $x[n] = z[n]$  na entrada da DFT a partir do sinal  $E(t)$  mostrado em (A) no slide anterior, precisamos primeiramente considerar que o intervalo de tempo entre as amostras de  $x[n]$  é  $\Delta t = 1/f_s = 0.1$  ns, onde  $f_s = 10$  [Gsa/s] é a frequência de amostragem do ADC dada no enunciado. Visto que de (A) no slide anterior temos  $T_R = 400$ ns e  $PW = 40$ ns, então o número de amostras no intervalo  $T_R$  é  $N = T_R/\Delta t = 4000$  amostras e o número de amostras no intervalo  $PW$  é  $N_{pw} = PW/\Delta t = 400$  amostras, conforme mostrado em (A) abaixo.



A partir de (A) acima, a definição da sequência de amostras  $x[n]$  é portanto:

$$x[n] = \begin{cases} A \cos(\theta_c[n] n + \phi) & p/ 0 \leq n < N_{pw} \\ 0 & p/ N_{pw} \leq n < N \end{cases} \quad (4)$$

onde  $A = 1$  é a amplitude do cosseno e  $\phi = 30^\circ$  é o ângulo de fase do cosseno ( $x[n = 0] = A \cos \phi = 0.866 \rightarrow \phi = \arccos(0.866/1) = 30^\circ$ ).  $\theta_c[n]$  [rad/sa] é a frequência digital instantânea do cosseno dada por

$$\theta_c[n] = \theta_c \text{min} + k\theta n \quad (5)$$

## Detecção de ameaças – sinais de radar:

$$\theta_c[n] = \theta_c \text{min} + k\theta n \quad (5)$$

onde  $\theta_c \text{min}$  é a frequência digital mínima  $\theta_c[n = 0] = \theta_c \text{min}$  que corresponde à frequência analógica mínima  $f_c \text{min} = 125\text{MHz}$ , conforme mostrado em (B) no slide 30:

$$\theta_c \text{min} = 2\pi \frac{f_c \text{min}}{f_s} = 2\pi \frac{125\text{MHz}}{10\text{GHz}} = 0.07854 \left[ \frac{\text{rad}}{\text{sa}} \right] \quad (6)$$

A constante  $k\theta$  é a declividade da rampa  $[\text{rad}/\text{sa}^2]$  da frequência digital instantânea  $\theta_c[n]$  dada por (5), e obtida de (5) através de:

$$\theta_c \text{max} = \theta_c[N_{pw} - 1] = \theta_c \text{min} + k\theta (N_{pw} - 1)$$

$$2\pi \frac{f_c \text{max}}{f_s} = 2\pi \frac{f_c \text{min}}{f_s} + k\theta (N_{pw} - 1)$$

$$k\theta = 2\pi \frac{(f_c \text{max} - f_c \text{min})}{f_s(N_{pw} - 1)} = 0.00015 \left[ \frac{\text{rad}}{\text{sa}^2} \right] \quad (7)$$

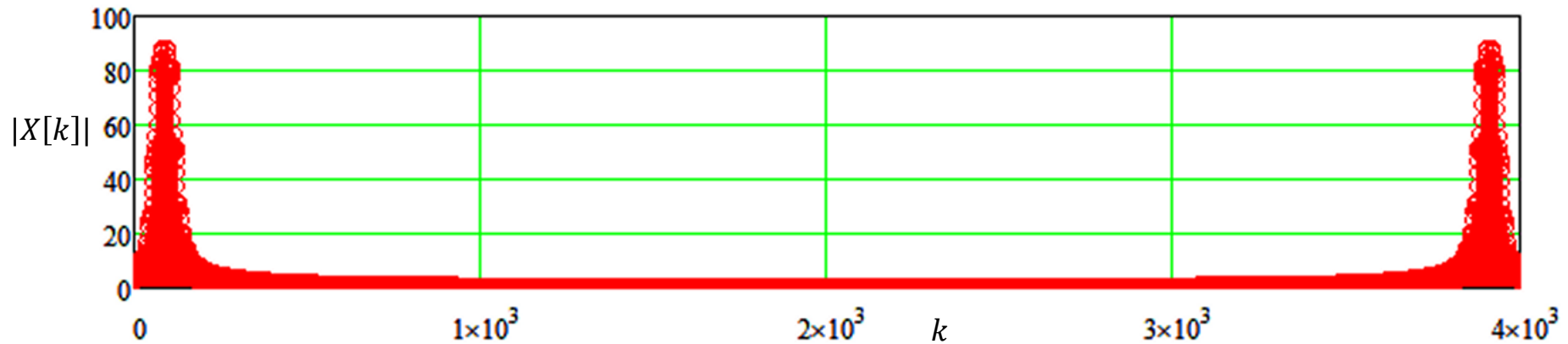
onde  $f_c \text{min} = 125 \text{ MHz}$  e  $f_c \text{max} = 220.254 \text{ MHz}$  são dados em (B) no enunciado no slide 30,  $N_{pw} = PW/\Delta t = 400$  amostras foi determinado no slide anterior e  $f_s = 10 \text{ [Gsa/s]}$  é dado no enunciado.

O espectro  $X[k] = \text{DFT}\{x[n]\}$  é determinado através de (2), abaixo reproduzida novamente por conveniência:

$$X[k] = \text{DFT}\{x[n]\} = \sum_{n=0}^{N-1} x[n] e^{-j(2\pi/N)nk}, \quad k = 0, 1, \dots, N - 1 \quad (2)$$

## Detecção de ameaças – sinais de radar:

Substituindo (4) em (2) e plotando a magnitude  $|X[k]|$  do espectro no domínio frequência discreta  $k$ , com  $\theta_c[n]$ ,  $\theta_c \min$  e  $k\theta$  sendo respectivamente dados por (5), (6) e (7), temos:

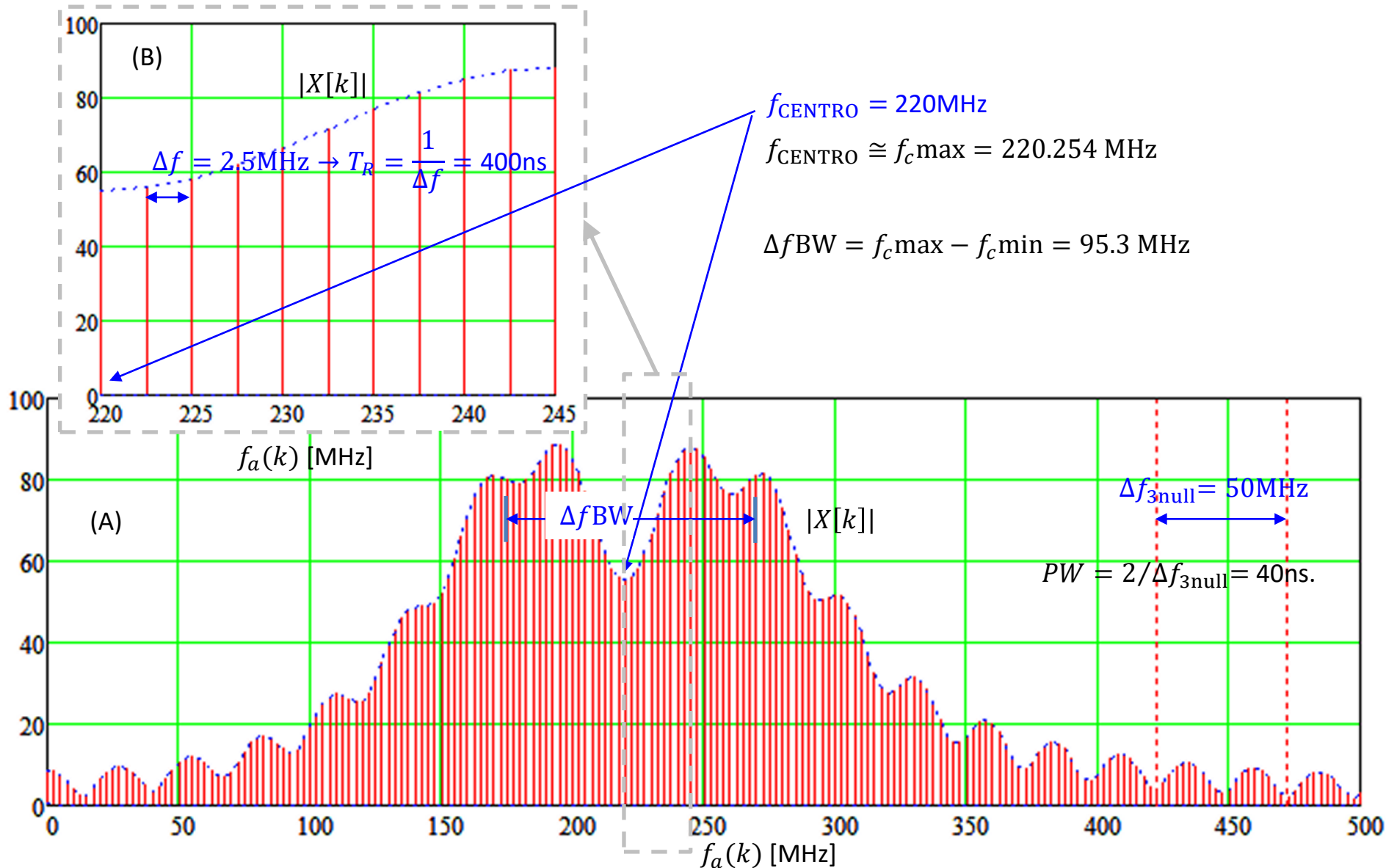


Para facilitar a análise dos parâmetros do espectro  $X[k]$ , é conveniente converter o domínio frequência discreta  $k$  nas correspondentes frequências no domínio frequência analógica  $f_a$  através de (4), abaixo reproduzida novamente por conveniência:

$$f_a(k) = \begin{cases} \frac{k f_s}{N} & p/ \ k \leq N/2 \\ \frac{(k - N) f_s}{N} & p/ \ k > N/2 \end{cases} \quad (4)$$

## Detecção de ameaças – sinais de radar:

Plotando a magnitude  $|X[k]|$  do espectro de  $x[n]$  no domínio frequência analógica  $f_a(k)$  para  $f_a(k) > 0$  com  $k = 0, 1, \dots, N - 1$  (que é o que mostra a tela do *Spectrum Display* - ver slide 25), obtemos:





## Detecção de ameaças – sinais de radar:

**(b)** Em (B) no slide anterior, observa-se que a separação entre as componentes espectrais é  $\Delta f = 2.5\text{MHz}$ . O inverso de  $\Delta f$  determina o *PRI* (*pulse repetition interval*) dado por  $PRI = T_R = 1/\Delta f = 400\text{ns}$ . O inverso do *PRI* determina o *PRF* (*pulse repetition frequency*) dado por  $PRF = 1/PRI = 2.5\text{MHz}$ .

Em (A) no slide anterior, observa-se que a separação  $\Delta f_{3\text{null}}$  entre 3 nulos consecutivos da curva  $|X[k]|$  é  $\Delta f_{3\text{null}} = 50\text{MHz}$ . O *PW* (*pulse width* – largura de pulso) do sinal  $E(t)$  mostrado em (A) no slide 24 pode ser obtido através de  $PW = 2/\Delta f_{3\text{null}} = 40\text{ns}$ . Importante notar que, diferentemente do Exemplo 2,  $|X[k]|$  não simétrico em relação à sua frequência central  $f_{\text{CENTRO}} = 220\text{MHz}$ . Portanto os 3 nulos consecutivos da curva  $|X[k]|$  devem estar localizados à direita e suficientemente afastados de  $f_{\text{CENTRO}}$  para maximizar a precisão da estimativa de  $PW = 2/\Delta f_{3\text{null}}$ .

A frequência  $f_{c\text{max}} = 220.254\text{MHz}$  dos *bursts* de RF nos pulsos do sinal  $E(t)$  mostrado em (A) no slide 30 é aproximadamente obtida da frequência  $f_{\text{CENTRO}} = 220\text{MHz}$  correspondente ao centro do espectro  $|X[k]|$  no slide anterior. A frequência  $f_{c\text{min}} = 125\text{MHz}$  dos *bursts* de RF pode ser aproximada através de  $\Delta f_{\text{BW}} = f_{c\text{max}} - f_{c\text{min}}$ , onde  $\Delta f_{\text{BW}}$  é a banda de frequências entre as frequências (aproximadamente) centrais dos máximos à esquerda e à direita do centro do espectro, conforme mostrado em (A) no slide anterior. O problema nesta abordagem é que as frequências centrais dos máximos à esquerda e à direita do centro do espectro não são precisamente definidas e dependem largamente da constante  $k\theta$  de declividade da rampa de variação da frequência.

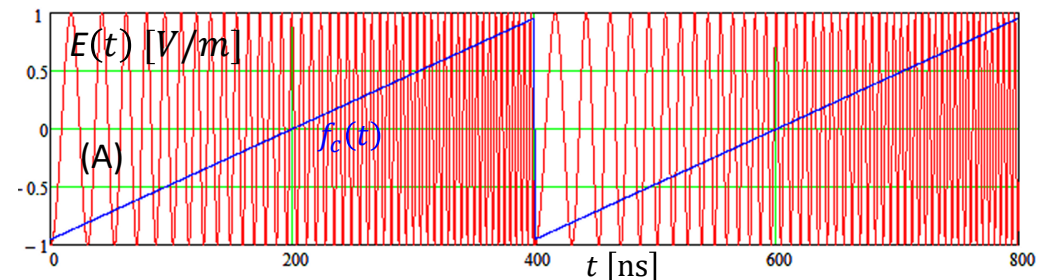
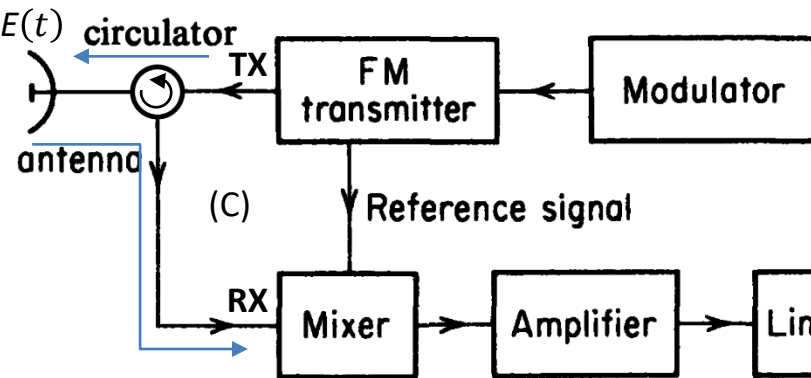
O *script* do software MathCad utilizado como auxílio na solução deste exemplo está disponível em <http://www.fccdecastro.com.br/ZIP/E3S30.zip> .

## Detecção de ameaças – sinais de radar:

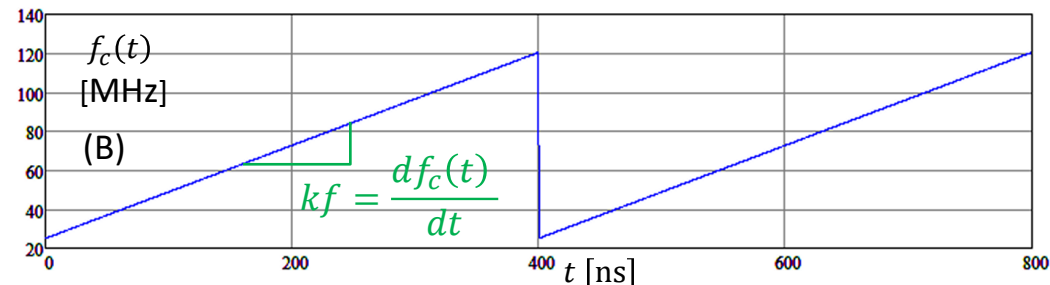
Em um teatro de EW é crucial operar em modo *stealth*, i.e., operar sob o paradigma “ver sem ser visto”. Para tanto, é necessário que os sinais irradiados pelos sistemas de comunicações e pelos sistemas de radar tenham pouca probabilidade de serem interceptados pelos sistemas de EW do inimigo (sinal LPI – *low probability of intercept signal*). Um problema neste sentido com radares pulsados é a enorme potência de pico necessária (usualmente , mais de 500 kW), não somente gerando interferência em outros serviços (ver <https://www.hindawi.com/journals/ijap/2015/849695/> ) como também tornando a onda EM irradiada pelo radar pulsado “visível” à longa distância aos sistemas de EW do inimigo.

Para contornar a fácil detecção do sinal de radares pulsados por sistemas EW inimigos, radares FMCW (*Frequency Modulated Continuous Wave*) têm sido largamente utilizados em aplicações militares e em navegação marítima devido às características *stealth* do sinal por eles irradiado (ver [https://en.wikipedia.org/wiki/Continuous-wave\\_radar#Modulated\\_continuous-wave](https://en.wikipedia.org/wiki/Continuous-wave_radar#Modulated_continuous-wave) ).

O radar FMCW difere do radar pulsado no fato de o sinal de RF ser emitido continuamente. Conseqüentemente, o tempo  $t_0$  que mede a distância do trajeto antena→alvo→antena da onda EM deve ser medido indiretamente. Para tanto o radar FMCW emite um sinal de RF  $E(t)$  conforme (A) cuja frequência varia de forma linear (LFM - *Linear Frequency Modulation*) conforme (B). O sinal recebido é então heterodinado com o sinal emitido, conforme (C), e devido à rampa de  $f_c(t)$  e ao atraso de tempo  $t_0$ , a onda EM refletida no alvo será recebida com uma diferença de frequência  $\Delta f_c$  em relação à onda transmitida, o que permite determinar o *target range* conforme veremos no próximo em slide.

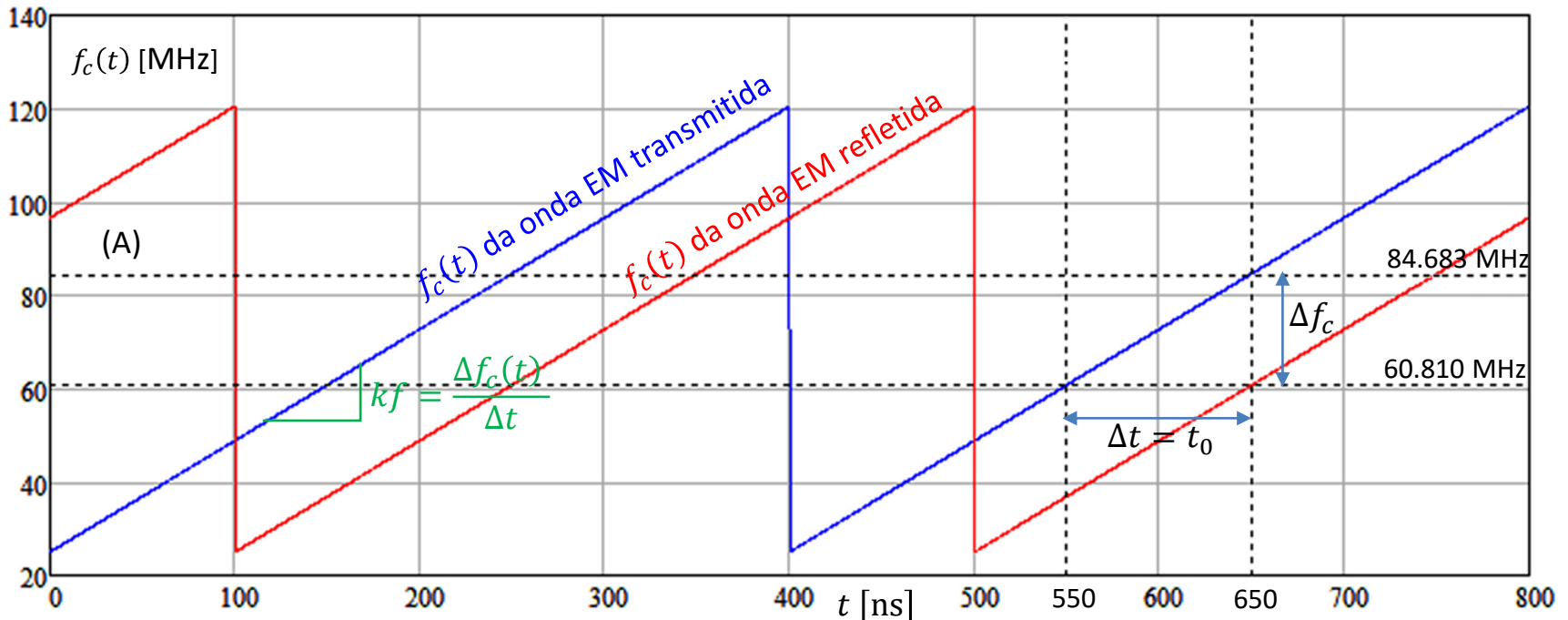


A constante  $k_f = \frac{df_c(t)}{dt}$  [Hz/s] é a declividade da rampa da frequência instantânea  $f_c(t)$ .



## Detecção de ameaças – sinais de radar:

A distância  $R$  entre alvo e antena (*target range*) para um radar FMCW é obtida conforme discussão-exemplo que segue. Em (A) é mostrado em **azul** o valor instantâneo **da frequência da onda EM que está sendo transmitida** pela antena do radar e é mostrado em **vermelho** o valor instantâneo **da frequência da onda EM que foi refletida no alvo e que está sendo recebida** na forma de eco pela antena do radar. A constante  $kf = \frac{\Delta f_c(t)}{\Delta t}$  que define a declividade da rampa da frequência instantânea  $f_c(t)$  é uma característica de cada radar, e no exemplo em questão tem o valor  $kf = 0.238732$  [MHz/ns].



Em  $t = 650$  [ns] o RX mede a diferença  $\Delta f_c = 84.683$  [MHz] -  $60.810$  [MHz] =  $23.873$  [MHz] entre o  $f_c(t)$  da onda EM transmitida e o  $f_c(t)$  da onda EM refletida (na realidade, o RX mede recorrentemente a diferença  $\Delta f_c$  em diversos instantes e faz a média). Mas note que o valor de  $f_c(t)$  da onda EM refletida difere  $\Delta f_c$  do valor de  $f_c(t)$  da onda EM transmitida porque transcorreu um intervalo  $\Delta t = t_0$  em que a onda EM e respectivo eco levou para percorrer a distância  $2R$  no trajeto antena→alvo→antena. Dado que  $kf$  é conhecido (é uma constante característica de cada radar) e é o mesmo para a onda EM transmitida e refletida mesmo que o alvo esteja em movimento, então  $t_0 = \Delta f_c / kf = 100$  [ns]. Daí, portanto, o *target range* é  $R = 0.5 c t_0 = 14.99$  m, onde  $c = 2.9979246 \times 10^8$  m/s é a velocidade de propagação da onda EM. Note, portanto, que a resolução espacial de um radar FMCW é melhor que a de um radar pulsado.

## Detecção de ameaças – sinais de radar:

A equação do tempo de trajeto antena→alvo→antena  $t_0 = \Delta f_c / kf$  que utilizamos no slide anterior para determinar o *target range*  $R = 0.5 c t_0$  para um radar FMCW precisa contemplar a situação em que ocorre movimento relativo com velocidade  $v$  entre antena e alvo. Esta situação tem como consequência que o valor instantâneo da rampa da frequência da onda EM que foi refletida no alvo e que está sendo recebida na forma de eco pela antena do radar tem o valor de sua frequência instantânea desviada de um valor  $\Delta f_D = \pm 2f_0(v/c)$ .  $\Delta f_D$  corresponde ao desvio Doppler resultante do movimento relativo com velocidade  $v$  entre antena e alvo (ver <https://www.radartutorial.eu/11.coherent/co06.en.html>). Note que o fator 2 resulta do fato de ocorrer desvio Doppler tanto no trajeto antena→alvo como no trajeto do eco alvo→antena. O desvio Doppler  $f_D$  é positivo quando o alvo se aproxima da antena com velocidade  $v$  e é negativo em caso contrário, e  $f_0$  é o valor instantâneo da frequência da onda EM que está sendo transmitida pela antena do radar.

Para que haja um valor de referência  $f_0$  constante, o sinal irradiado pelo radar prevê um intervalo de tempo ao final do ciclo da modulação LFM ao longo do qual a frequência da onda EM que está sendo transmitida pela antena do radar é mantida em valor constante  $f_0$  conforme mostrado em (A) abaixo.

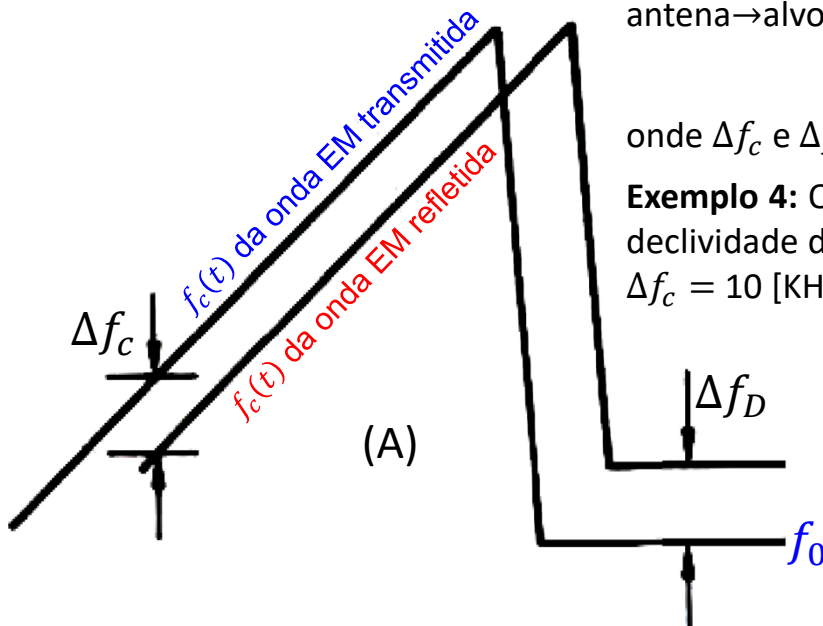
Portanto, incluindo o desvio Doppler na equação do tempo de trajeto antena→alvo→antena para um radar FMCW resulta em

$$t_0 = (\Delta f_c + \Delta f_D) / kf \quad (8)$$

onde  $\Delta f_c$  e  $\Delta f_D$  são medidos pelo processamento do RX.

**Exemplo 4:** O TX de um radar FMCW transmite na banda X com  $f_0 = 10$  [GHz] e declividade da rampa  $kf = 10$  [Hz/ $\mu$ s]. O RX do radar mede  $\Delta f_D = 14.825$  [KHz] e  $\Delta f_c = 10$  [KHz]. **Determine:** (a) O *target range*  $R$ . (b) A velocidade  $v$  do alvo.

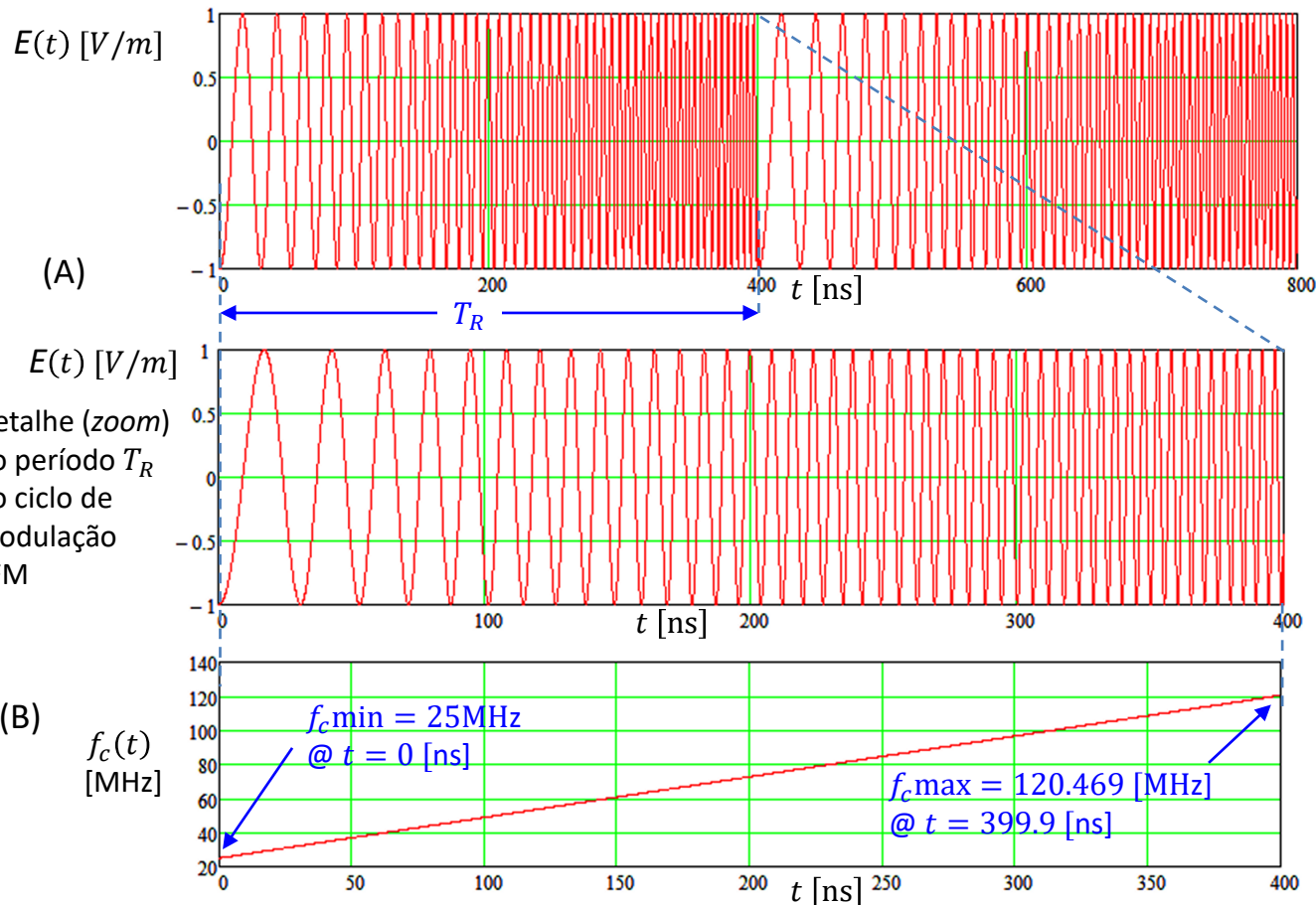
**Solução:** (a) De (8),  $t_0 = 2.483$  [ms]. Daí  $R = 0.5 c t_0 = 372.1$  [Km].  
(b)  $v = 0.5 (c/f_0)\Delta f_D = 800$  [Km/h].





## Detecção de ameaças – sinais de radar:

**Exemplo 5:** Um radar FMCW inimigo opera na banda A. O valor normalizado do campo elétrico  $E(t)$  da onda EM irradiada pela antena é conforme mostrado em (A).



Em (B) é mostrada a variação linear da frequência instantânea  $f_c(t)$  do cosseno definido ao longo do ciclo da modulação LFM de duração  $T_R$ .

O campo elétrico  $E(t)$  [V/m] irradiado mostrado em (A) é captado pelo *array* de antenas receptoras de um sistema de EW (ver (A) no slide 11), cujo bloco *Search Receiver* converte o campo  $E(t)$  [V/m] em um sinal de tensão analógico  $E(t)$  [V] conforme mostrado em (B) no slide 25. O conversor A/D (=ADC) do *Search Receiver* digitaliza o sinal  $E(t)$  com frequência de amostragem  $f_s = 10$  [Gsa/s].

**Pede-se:** (a) Determine e plote o gráfico da magnitude do espectro  $X[k]$  que é mostrado na tela “Spectrum display” do *Search Receiver* em (B) no slide 25. (b) A partir do gráfico do espectro  $X[k]$  obtido em (a) determine o período  $T_R$  do ciclo da modulação LFM. Estime aproximadamente as frequências  $f_{c\min}$  e  $f_{c\max}$  do ciclo da modulação LFM.



## Detecção de ameaças – sinais de radar:

$$\theta_c[n] = \theta_c \text{min} + k\theta n \quad (5)$$

onde  $\theta_c \text{min}$  é a frequência digital mínima  $\theta_c[n = 0] = \theta_c \text{min}$  que corresponde à frequência analógica mínima  $f_c \text{min} = 25\text{MHz}$ , conforme mostrado em (B) no slide 39:

$$\theta_c \text{min} = 2\pi \frac{f_c \text{min}}{f_s} = 2\pi \frac{25\text{MHz}}{10\text{GHz}} = 0.0157 \left[ \frac{\text{rad}}{\text{sa}} \right] \quad (10)$$

A constante  $k\theta$  é a declividade da rampa [ $\text{rad}/\text{sa}^2$ ] da frequência digital instantânea  $\theta_c[n]$  dada por (5), e obtida de (5) através de (ver slide 32):

$$k\theta = 2\pi \frac{(f_c \text{max} - f_c \text{min})}{f_s(N_{pw} - 1)} = 0.000015 \left[ \frac{\text{rad}}{\text{sa}^2} \right] \quad (11)$$

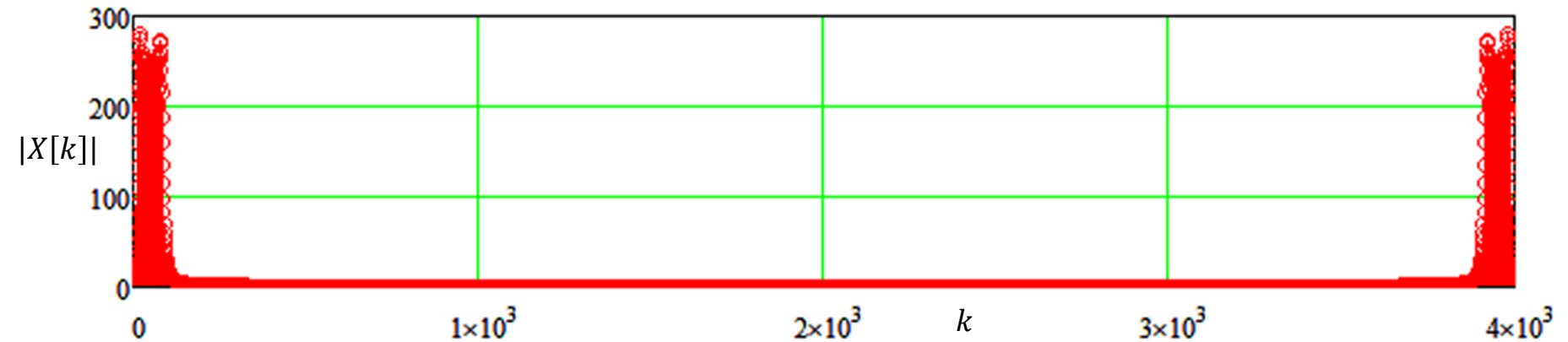
onde  $f_c \text{min} = 25 \text{ MHz}$  e  $f_c \text{max} = 120.469 \text{ MHz}$  são dados em (B) no enunciado no slide 39,  $N_{pw} = N = 4000$  amostras foi determinado no slide anterior e  $f_s = 10 \text{ [Gsa/s]}$  é dado no enunciado.

O espectro  $X[k] = \text{DFT}\{x[n]\}$  é determinado através de (2), abaixo reproduzida novamente por conveniência:

$$X[k] = \text{DFT}\{x[n]\} = \sum_{n=0}^{N-1} x[n] e^{-j(2\pi/N)nk}, \quad k = 0, 1, \dots, N - 1 \quad (2)$$

## Detecção de ameaças – sinais de radar:

Substituindo (9) em (2) e plotando a magnitude  $|X[k]|$  do espectro no domínio frequência discreta  $k$ , com  $\theta_c[n]$ ,  $\theta_c \min$  e  $k\theta$  sendo respectivamente dados por (5), (10) e (11), temos:

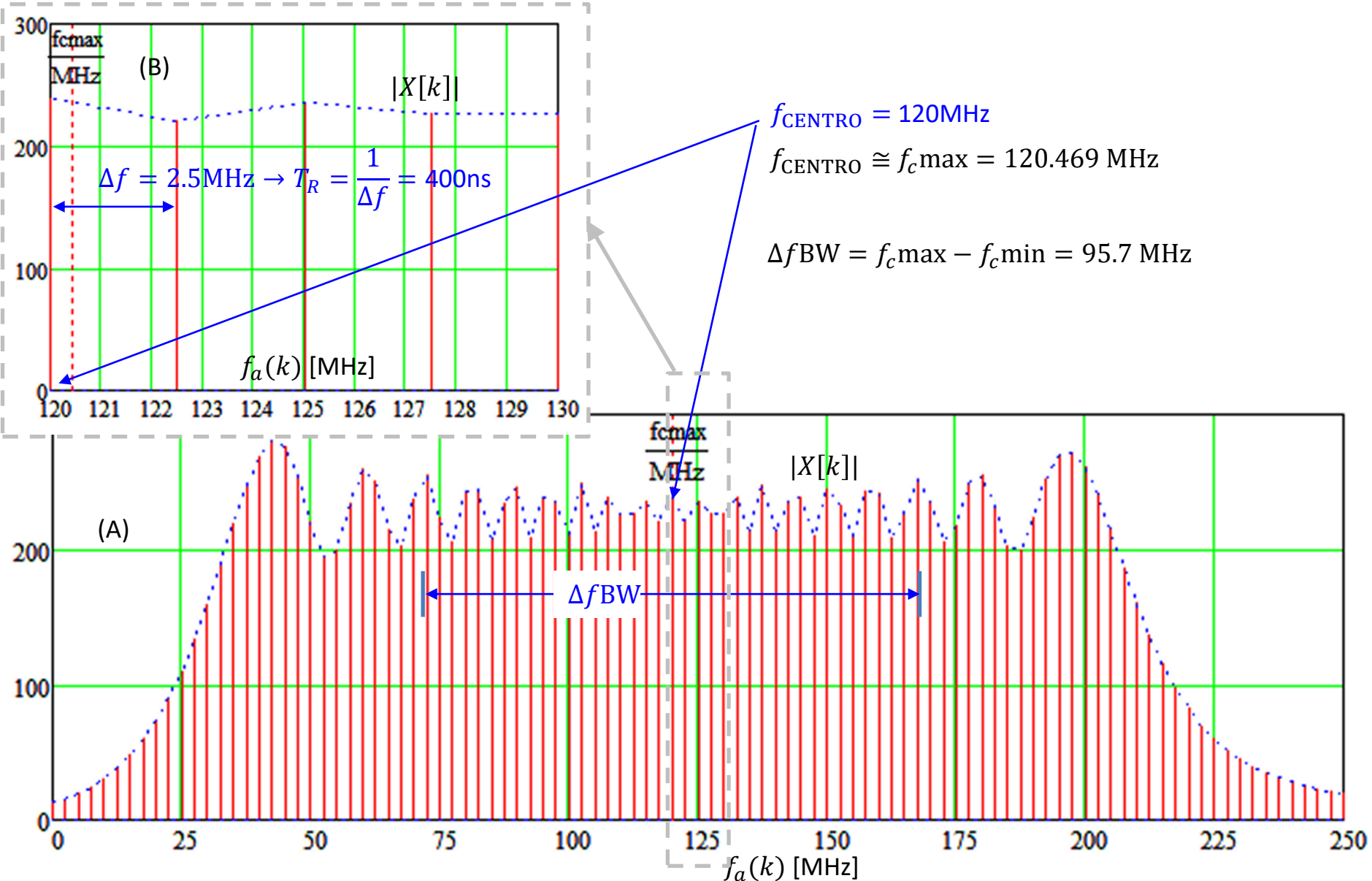


Para facilitar a análise dos parâmetros do espectro  $X[k]$ , é conveniente converter o domínio frequência discreta  $k$  nas correspondentes frequências no domínio frequência analógica  $f_a$  através de (4), abaixo reproduzida novamente por conveniência:

$$f_a(k) = \begin{cases} \frac{k f_s}{N} & p/ \ k \leq N/2 \\ \frac{(k - N) f_s}{N} & p/ \ k > N/2 \end{cases} \quad (4)$$

## Detecção de ameaças – sinais de radar:

Plotando a magnitude  $|X[k]|$  do espectro de  $x[n]$  no domínio frequência analógica  $f_a(k)$  para  $f_a(k) > 0$  com  $k = 0, 1, \dots, N - 1$  (que é o que mostra a tela do *Spectrum Display* - ver slide 25), obtemos:





## Detecção de ameaças – sinais de radar:

**(b)** Em (B) no slide anterior, observa-se que a separação entre as componentes espectrais é  $\Delta f = 2.5\text{MHz}$ . O inverso de  $\Delta f$  determina o período do ciclo da modulação LFM  $T_R = 1/\Delta f = 400\text{ns}$ .

A frequência  $f_{c\text{max}} = 120.254\text{ MHz}$  do ciclo da modulação LFM do sinal  $E(t)$  mostrado em (A) no slide 39 é aproximadamente obtida da frequência  $f_{\text{CENTRO}} = 120\text{MHz}$  correspondente ao centro do espectro  $|X[k]|$  no slide anterior. A frequência  $f_{c\text{min}} = 25\text{ MHz}$  do ciclo de modulação pode ser aproximada através de  $\Delta f_{\text{BW}} = f_{c\text{max}} - f_{c\text{min}}$ , onde  $\Delta f_{\text{BW}}$  varia com a largura da magnitude  $|X[k]|$  do espectro. O problema nesta abordagem é que a relação entre  $\Delta f_{\text{BW}}$  e a largura da magnitude  $|X[k]|$  não é linear, o que resulta em uma péssima precisão na estimativa de  $f_{c\text{min}}$ .

O *script* do software MathCad utilizado como auxílio na solução deste exemplo está disponível em <http://www.fccdecastro.com.br/ZIP/E5S39.zip> .

## Detecção de ameaças – sinais de comunicações:

Sinais de comunicação transportam informação analógica e/ou digital em enlaces de comunicação entre TX e RX. Mesmo que a comunicação seja ponto-multiponto, i.e., um TX transmitindo para vários RXs, cada enlace em si se resume basicamente à transmissão entre o ponto de origem (TX) e o ponto de destino (RX), em que uma onda EM se propaga no caminho de propagação transportando informação entre TX e RX. O TX é o alvo do processo de detecção, interceptação e localização efetuado por um sistema de EW para localização de emissores. A grande maioria dos sinais de comunicação têm modulações contínuas e um *duty-cycle* (ciclo de trabalho) bem maior que um sinal de radar, o que facilita a sua detecção. Usualmente, os enlaces de comunicação de interesse no âmbito de EW convencional, sejam eles analógicos ou digitais, ocorrem nas faixas de HF, VHF, UHF e microondas.

As modulações adotadas dependem basicamente da finalidade do enlace e das condições de propagação e de *jamming* no cenário de EW em que o enlace opera. Como regra geral: (1) Quanto maior a largura de banda do espectro do sinal transportado pela onda EM que se propaga entre TX e RX mais informação a onda EM pode transportar por unidade de tempo. (2) Quanto maior a frequência do sinal maior largura de banda o processo de modulação pode atribuir ao espectro do sinal, no entanto mais dependente se torna a viabilidade do enlace da condição de o mesmo necessitar operar sob linha de visada (LOS – *line of sight*) entre TX e RX no caminho de propagação da onda EM.

Em enlaces analógicos a informação transportada é basicamente voz, e as modulações usualmente adotadas em um cenário de EW são a modulação SSB (*single sideband* – ver [https://en.wikipedia.org/wiki/Single-sideband\\_modulation](https://en.wikipedia.org/wiki/Single-sideband_modulation) e o NBFM (*narrowband FM* – ver <https://www.electronics-notes.com/articles/radio/modulation/fm-frequency-modulation-index-deviation-ratio.php>). É imperativo que a frequência central do enlace analógico seja variada em saltos (*frequency hopping*), obedecendo a um padrão de saltos de frequência estabelecido através de um protocolo conhecido somente entre TX e RX (ver, por exemplo, <https://ieeexplore.ieee.org/abstract/document/6772597>), caso contrário o sigilo da informação transportada será facilmente quebrado dado que é uma operação simples demodular sinais analógicos.

Em enlaces digitais, há três funcionalidades básicas do sistema que determinam as suas características operacionais e o seu desempenho (ver diagrama de blocos no slide 3 de [http://www.fccdecastro.com.br/pdf/T2\\_Aula2\\_13032020.pdf](http://www.fccdecastro.com.br/pdf/T2_Aula2_13032020.pdf)):

- 1) Codificador/decodificador de fonte: Responsáveis por comprimir (reduzir o número de bits) a informação a ser transmitida para efeito de reduzir a largura de banda do espectro do sinal transmitido.
- 2) Codificador/decodificador de canal: Responsáveis por corrigir as palavras binárias erradas recebidas pelo RX cujos bits errados originam-se da degradação da onda EM que ocorre no canal de transmissão entre TX e RX. A degradação da onda EM é causada pelo ruído aditivo no canal e pelos ecos da onda EM originados em pontos de reflexão no canal (*multipath*).

## Detecção de ameaças – sinais de comunicações:

3) Modulador/Demodulador: O modulador é responsável por converter as palavras binárias a serem transmitidas na onda EM que se propaga no canal entre TX e RX, e busca efetuar a contenção espectral do sinal transmitido mediante filtragem e pré-distorção ([http://www.highfrequencyelectronics.com/Apr04/HFE0404\\_Stapleton.pdf](http://www.highfrequencyelectronics.com/Apr04/HFE0404_Stapleton.pdf)) de modo a minimizar espúrios espectrais no espectro da onda EM. O demodulador é responsável por converter a onda EM recebida nas palavras binárias originalmente transmitidas, e busca minimizar o efeito de *multipath* do canal (ver [http://www.fccdecastro.com.br/pdf/T2\\_Aula3\\_18032020.pdf](http://www.fccdecastro.com.br/pdf/T2_Aula3_18032020.pdf)) e de ruído aditivo do canal (ver [http://www.fccdecastro.com.br/pdf/T2\\_Aula12\\_24042020.pdf](http://www.fccdecastro.com.br/pdf/T2_Aula12_24042020.pdf)).

Um sistema digital é totalmente caracterizado e se torna reproduzível em termos de funcionalidades de *hardware* desde que se conheça não somente a modulação digital adotada no modulador/demodulador, como também o código corretor de erro adotado no codificador/decodificador de canal e o código para compressão adotado no codificador/decodificador de fonte. No entanto, é usual a modulação dar o nome ao sistema, dado que não somente o modulador/demodulador são os blocos com maior complexidade e sofisticação de algoritmos para processamento de sinal como também é a modulação que determina as características do espectro da onda EM irradiada, de modo que o espectro irradiado é a “impressão digital” do tipo de modulação adotado.

Nomes típicos de sistemas associados à modulação: sistema OFDM ([https://en.wikipedia.org/wiki/Orthogonal\\_frequency\\_division\\_multiplexing](https://en.wikipedia.org/wiki/Orthogonal_frequency_division_multiplexing)), sistema CDMA ([https://en.wikipedia.org/wiki/Code-division\\_multiple\\_access](https://en.wikipedia.org/wiki/Code-division_multiple_access)), sistema SC-FDMA ([https://en.wikipedia.org/wiki/Single-carrier\\_FDMA](https://en.wikipedia.org/wiki/Single-carrier_FDMA)), e assim por diante.

No âmbito do processo de detecção e identificação de sinais, inúmeros sistemas de comunicação podem ser encontrados em um teatro de operações de EW. Categorizados pelo tipo de modulação digital adotada, segue abaixo o rol de possíveis (sem esgotar as possibilidades) sistemas de comunicações usualmente em operação em um teatro de EW:

### **Sistemas de portadora única (*single carrier*):**

#### • *Quadrature Amplitude Modulation*

(QAM - ver slides 2 a 22 de [http://www.fccdecastro.com.br/pdf/T2\\_Aula10&11\\_22042020.pdf](http://www.fccdecastro.com.br/pdf/T2_Aula10&11_22042020.pdf))

#### • *Phase Shift Keying* (PSK - ver slides 23 a 33 de [http://www.fccdecastro.com.br/pdf/T2\\_Aula10&11\\_22042020.pdf](http://www.fccdecastro.com.br/pdf/T2_Aula10&11_22042020.pdf))

#### • *Pulse Amplitude Modulation*

(PAM - ver slides 34 a 40 de [http://www.fccdecastro.com.br/pdf/T2\\_Aula10&11\\_22042020.pdf](http://www.fccdecastro.com.br/pdf/T2_Aula10&11_22042020.pdf))

## Detecção de ameaças – sinais de comunicações:

- *Frequency Shift Keying* (FSK - ver [http://www.fccdecastro.com.br/pdf/T2\\_Aula15\\_08052020..pdf](http://www.fccdecastro.com.br/pdf/T2_Aula15_08052020..pdf) )
- *Gaussian Minimum Shift Keying* (GMSK - <https://www.electronics-notes.com/articles/radio/modulation/what-is-gmsk-gaussian-minimum-shift-keying.php> )

### **Sistemas multiportadora (*multicarrier*):**

- *Orthogonal Frequency Division Multiplexing*  
(OFDM – ver slides 60 a 115 de [http://www.fccdecastro.com.br/pdf/T2\\_Aulas21a26\\_26062020.pdf](http://www.fccdecastro.com.br/pdf/T2_Aulas21a26_26062020.pdf))

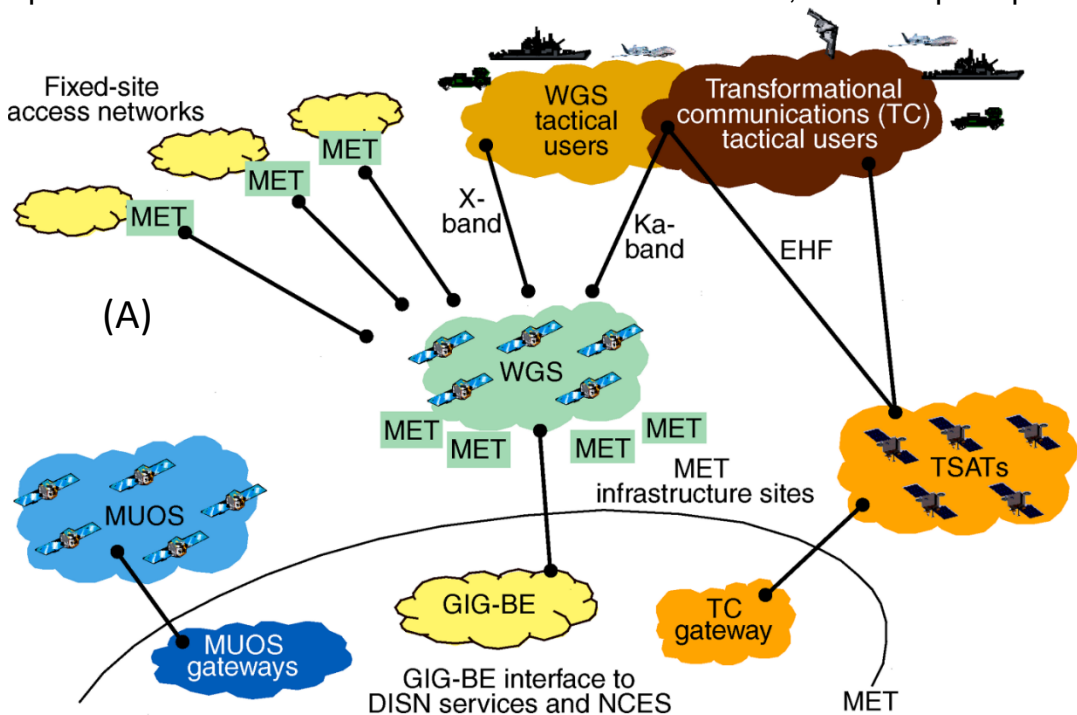
### **Sistemas *spread-spectrum*:**

- *Direct Sequence – Code Division Multiple Access*  
(DS-CDMA – ver slides 14 a 59 de [http://www.fccdecastro.com.br/pdf/T2\\_Aulas21a26\\_26062020.pdf](http://www.fccdecastro.com.br/pdf/T2_Aulas21a26_26062020.pdf))
- *Frequency Hopping – Spread Spectrum*  
(FH-SS – [https://en.wikipedia.org/wiki/Frequency-hopping\\_spread\\_spectrum](https://en.wikipedia.org/wiki/Frequency-hopping_spread_spectrum))
- *Multicarrier – Code Division Multiple Access*  
(MC-CDMA – ver slide 117 de [http://www.fccdecastro.com.br/pdf/T2\\_Aulas21a26\\_26062020.pdf](http://www.fccdecastro.com.br/pdf/T2_Aulas21a26_26062020.pdf) )
- *Multicarrier – Direct Sequence – Code Division Multiple Access*  
(MC-DS-CDMA – ver slide 118 de [http://www.fccdecastro.com.br/pdf/T2\\_Aulas21a26\\_26062020.pdf](http://www.fccdecastro.com.br/pdf/T2_Aulas21a26_26062020.pdf) )

Portanto, dado as inúmeras modulações digitais possíveis, um considerável trabalho de prospecção do espectro eletromagnético está envolvido na tarefa de identificar sinais em um cenário de EW. Importante notar que identificar o tipo de modulação de um sinal de comunicação digital não significa que se tenha a habilidade de demodular o mesmo, de modo a se ter acesso à informação que está sendo transmitida. Sem saber todos os parâmetros da modulação, todos os parâmetros dos códigos corretores de erro e todos os parâmetros dos códigos de compressão é impossível demodular um sinal digital. Identificar tais parâmetros a partir do sinal recebido envolve um considerável número de algoritmos e de técnicas de processamento digital, bem como um considerável tempo de processamento. Acresce ainda à complexidade do processo de demodulação o fato de que o *stream* de bits demodulados em qualquer sistema de comunicações militares estará encriptado por um sistema de criptografia, possivelmente através de criptografia de chave assimétrica (uma senha pública para encriptar o *stream* de bits no TX e uma senha privada para desencriptar o *stream* de bits no RX). Ver, por exemplo, [https://en.wikipedia.org/wiki/RSA\\_\(cryptosystem\)](https://en.wikipedia.org/wiki/RSA_(cryptosystem)) , [https://en.wikipedia.org/wiki/Elliptic-curve\\_cryptography](https://en.wikipedia.org/wiki/Elliptic-curve_cryptography), [https://en.wikipedia.org/wiki/Advanced\\_Encryption\\_Standard](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard) e [https://en.wikipedia.org/wiki/Data\\_Encryption\\_Standard](https://en.wikipedia.org/wiki/Data_Encryption_Standard).

## Detecção de ameaças – sinais de comunicações:

De particular interesse estratégico no âmbito de EW são os *data-links* entre estações terrenas e satélites, para comunicação de voz/vídeo e para enlaces de dados, usualmente operando nas bandas de UHF, SHF e EHF em geral com modulação PSK ou FSK ([https://en.wikipedia.org/wiki/Defense\\_Satellite\\_Communications\\_System](https://en.wikipedia.org/wiki/Defense_Satellite_Communications_System) e <https://www.defesanet.com.br/defesa/noticia/6861/indra>). Em (A) é mostrado uma concepção do Departamento de Defesa dos Estados Unidos (DoD-USA), em parte ainda futurística, quanto à integração das comunicações de um teatro de EW em uma rede de satélites. É perceptível, portanto, a tendência de o cenário operacional de EW tornar-se cada vez mais *net-centric*, com nós principais da rede concentrados em satélites.



WGS - *Wideband Global SATCOM*. Sistema de satélite de alta capacidade de comunicações planejado para uso em parceria do Departamento de Defesa dos Estados Unidos (DoD-USA) com o Departamento de Defesa australiano. Ver [https://pt.wikipedia.org/wiki/Wideband\\_Global\\_SATCOM](https://pt.wikipedia.org/wiki/Wideband_Global_SATCOM).

TC - *Transformational Communications*. Sistema de satélites de alta capacidade de dados, ainda não implementado pelo DoD-USA em função do alto custo. [https://en.wikipedia.org/wiki/Transformational\\_Satellite\\_Communications\\_System](https://en.wikipedia.org/wiki/Transformational_Satellite_Communications_System). TSATs são satélites da rede TC.

GIG - *Global Information Grid*. Internet militar em desenvolvimento pelo DoD-USA. Ver [https://en.wikipedia.org/wiki/Global\\_Information\\_Grid](https://en.wikipedia.org/wiki/Global_Information_Grid). GIG-BE é o *backbone* óptico da rede GIG.

MUOS - *Mobile User Objective System*. Sistema de satélites militares que opera na banda de UHF com modulação CDMA. Ver [https://en.wikipedia.org/wiki/Mobile\\_User\\_Objective\\_System](https://en.wikipedia.org/wiki/Mobile_User_Objective_System)

MET - *Modernization of Enterprise Terminals*. Programa de modernização de terminais de satélites militares do DoD-USA, terminais estes que operam em estações terrenas. Ver <https://ieeexplore.ieee.org/document/6127660>.

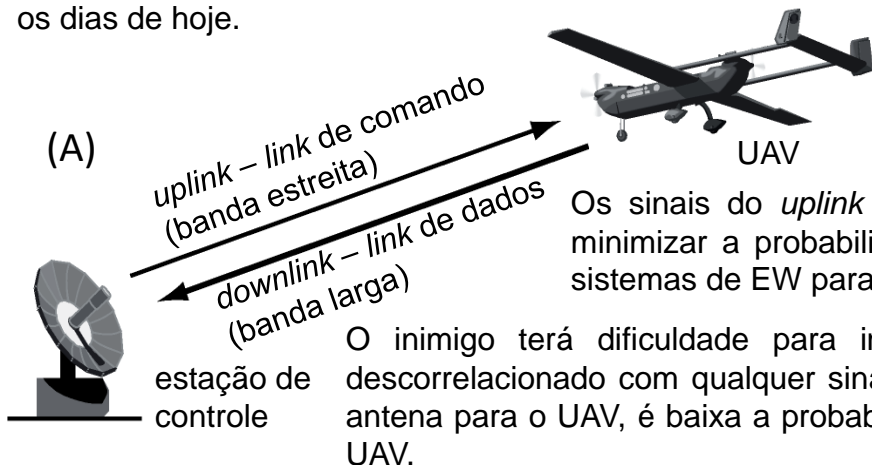
DISN - *Defense Information System Network*. Rede do DoD-USA para provimento de dados, video e voz em teatros de EW. Ver [https://en.wikipedia.org/wiki/Defense\\_Information\\_System\\_Network](https://en.wikipedia.org/wiki/Defense_Information_System_Network).

NCES - *Net-Centric Enterprise Services*. Programa do DoD-USA para desenvolver infra-estrutura de tecnologia da informação. Ver [https://en.wikipedia.org/wiki/Net-Centric\\_Enterprise\\_Services](https://en.wikipedia.org/wiki/Net-Centric_Enterprise_Services).



## Detecção de ameaças – sinais de comunicações:

Não menos estratégicos são os *data-links* de veículos aéreos não tripulados (UAV - *unmanned aerial vehicles*), usualmente operando na banda S, banda C, VHF ou UHF, com diversos tipos de modulação (GMSK, FSK, FH-SS e DS-CDMA – ver, por exemplo, <https://www.unmannedsystemstechnology.com/company/commtact-ltd/>). Uma das operações de EW mais emblemáticas no âmbito de detecção e identificação de sinais ocorreu em 2011, quando uma unidade de *cyberwarfare* das forças armadas do Iran identificou, demodulou e interceptou todos os sinais de um UAV RQ-170 “Sentinel”, fabricado pela empresa americana Lockheed Martin, ao ponto de assumir controle total e absoluto do UAV e fazê-lo descer intacto em solo iraniano ([https://en.wikipedia.org/wiki/Iran%E2%80%93U.S.\\_RQ-170\\_incident](https://en.wikipedia.org/wiki/Iran%E2%80%93U.S._RQ-170_incident)). As implicações geopolíticas deste incidente ainda ecoam até os dias de hoje.



Conforme mostrado em (A) o UAV recebe comandos da estação de controle e retorna o *stream* de bits gerado pelo *payload* (carga útil) para essa estação. O *link* de comando (*uplink*) geralmente é de banda estreita, porque o sinal de comando tem taxa de dados baixas.

Os sinais do *uplink* são criptografados e usualmente usam modulação DS-CDMA para minimizar a probabilidade de que a estação de controle seja detectada e localizada por sistemas de EW para localização de emissores de radiação EM.

O inimigo terá dificuldade para interferir (*jamming*) no controle do UAV porque o sinal CDMA é descorrelacionado com qualquer sinal que não seja ele mesmo. Assim, mesmo que o *jammer* aponte sua antena para o UAV, é baixa a probabilidade de que o mesmo interfira o sinal do *uplink* recebido pelo RX do UAV.

De mesma forma, o inimigo terá dificuldade para efetuar *jamming* no sinal do *downlink* porque é baixa a probabilidade de o inimigo detectar o sinal DS-CDMA do *uplink* irradiado pela estação de controle, e portanto é baixa a probabilidade de que a estação de controle seja localizada. Assim, o *jammer* fica impossibilitado de apontar a sua antena p/ a estação de controle e efetuar *jamming* no sinal do *downlink* recebido pelo RX da estação de controle.

Normalmente o espectro do sinal do *downlink* tem uma largura de banda muito maior do que o espectro do sinal de *uplink* porque o *downlink* transporta um grande volume de informação gerada pelo *payload* do UAV. O *payload* mais comum do UAV é o *payload* de vídeo de alta definição, usualmente câmeras digitais para luz visível ou para infra-vermelho, gerando taxas de algumas dezenas de megabits/segundo no *stream* de bits do *downlink* de sistemas que operam nas bandas S e C e de algumas dezenas de kilobits/segundo no *stream* de bits do *downlink* de sistemas que operam nas bandas VHF e UHF. O sinal do *downlink* é usualmente criptografado com criptografia AES-256 ([https://en.wikipedia.org/wiki/Advanced\\_Encryption\\_Standard](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard)) e eventualmente usa modulação FH-SS ou DS-CDMA para dificultar o *jamming* do sinal pelo inimigo. No entanto as altas taxas do *downlink* limitam a viabilidade técnica de espalhar o sinal ao longo de um espectro muito amplo.

## Detecção de ameaças – sinais de comunicações:

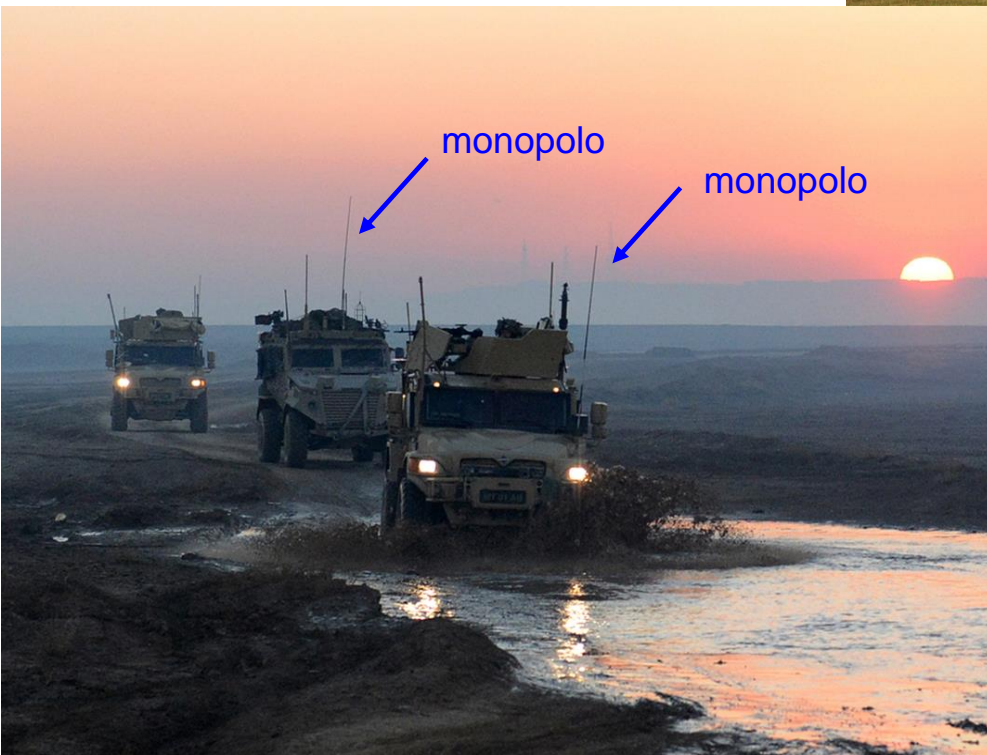
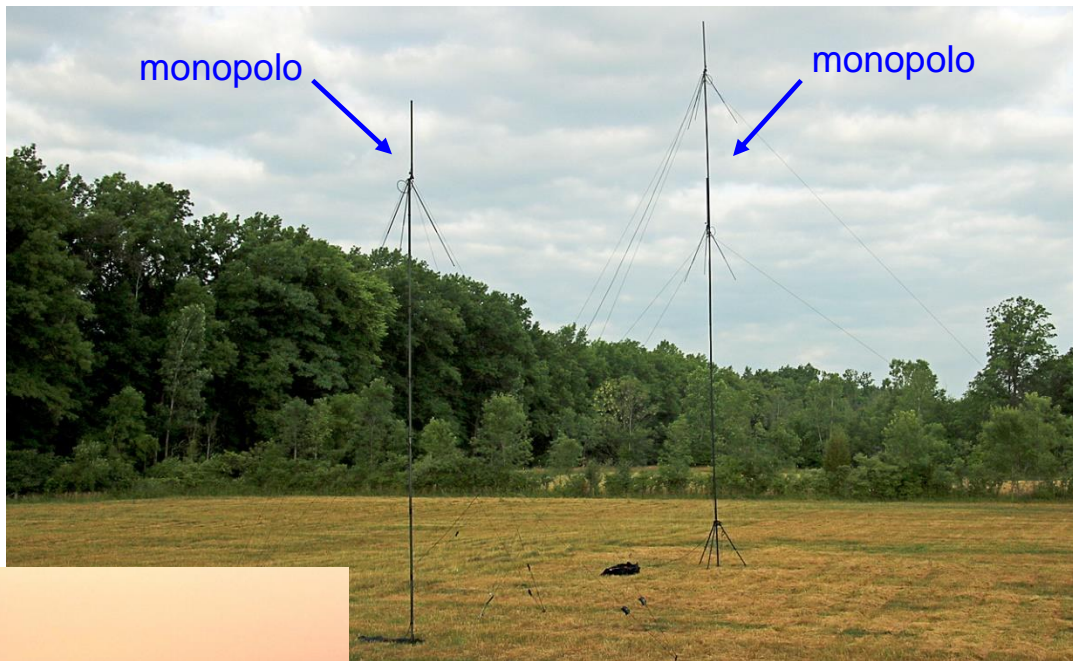
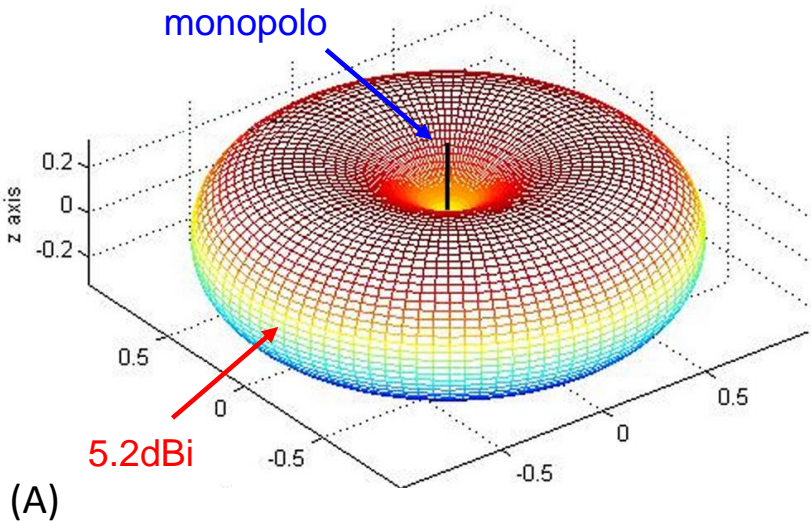
A antena do TX (e do RX) do *uplink* na estação de controle normalmente tem HPBW (*half power beam width* – ver página 8 de [http://www.fccdecastro.com.br/pdf/A\\_C3.pdf](http://www.fccdecastro.com.br/pdf/A_C3.pdf)) de apenas alguns poucos graus, minimizando assim a probabilidade de o sinal do *uplink* ser interceptado pelo *search receiver* (ver slide 25) de sistemas de EW para localização de emissores de radiação EM (ver slide 11). A antena do TX (e do RX) do *downlink* afixada na estrutura do UAV é estritamente limitada em tamanho não somente devido às dimensões máximas da estrutura do UAV como também devido ao arrasto aerodinâmico gerado pela antena, que será tanto maior quanto maior for a antena. Portanto, a antena do *downlink* localizada no UAV usualmente tem ganho menor e, conseqüentemente, maior largura de feixe (HPBW) do que a antena do *uplink* localizada na estação de controle.

Conforme discutido no slide 47, sem a identificação de todos os parâmetros da modulação, de todos os parâmetros dos códigos corretores de erro e de todos os parâmetros dos códigos de compressão é impossível demodular um sinal digital, de modo a que se possa ter acesso à informação que está sendo transmitida, seja ela dados, vídeo ou voz. Identificar tais parâmetros somente a partir do sinal recebido envolve um considerável número de algoritmos e de técnicas de processamento digital, bem como um considerável tempo de processamento. Acresce ainda à complexidade do processo de demodulação a criptografia aplicada ao *stream* de bits demodulados. Talvez os sinais com maior chance de serem detectados, identificados e demodulados em um menor espaço de tempo com um menor esforço de processamento sejam os sinais de comunicação tática.

Sinais de comunicação tática incluem múltiplos enlaces de comunicação solo-solo, comunicação ar-solo e comunicação ar-ar. O espectro destes sinais usualmente é encontrado nas bandas de HF, VHF e UHF e os transceptores usualmente operam com antenas monopolos verticais, o que confere a estes sistemas um padrão de irradiação da antena com cobertura omnidirecional (360°) no plano do azimute, exibindo um ganho de aproximadamente 5dBi conforme mostrado em (A) no próximo slide. Para frequências acima de 30 MHz é usual a adoção de antenas discone ([https://en.wikipedia.org/wiki/Discone\\_antenna](https://en.wikipedia.org/wiki/Discone_antenna)) devido a sua muito maior banda operacional, mas com o mesmo padrão de irradiação omnidirecional de um monopolo vertical. Esta característica omnidirecional do padrão de irradiação das antenas de comunicações táticas não somente maximiza a probabilidade de o sinal da estação tática inimiga ser interceptado pelo *search receiver* (ver slide 25) do sistema de EW para localização de emissores, como também maximiza a probabilidade de múltiplas estações táticas serem interceptadas simultaneamente. Isso permite que algoritmos para determinação da correlação entre os diversos sinais possam ser aplicados aumentando a chance de os parâmetros da modulação e das diversas codificações serem identificados pelos algoritmos de processamento e identificação.



# Detecção de ameaças – sinais de comunicações:

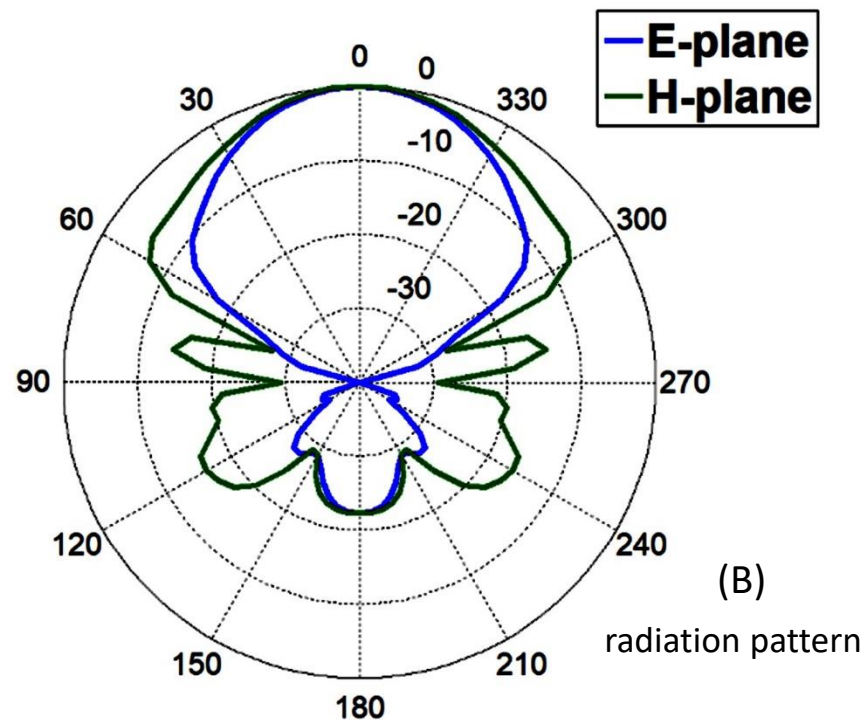
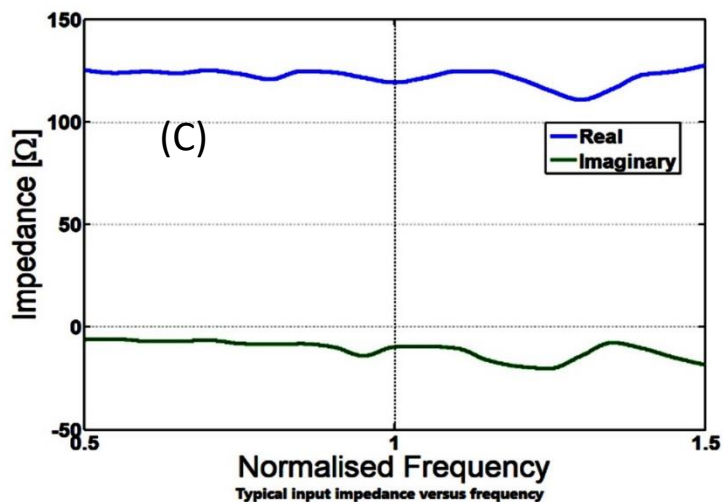


## Detecção de ameaças – sinais de comunicações:

Para enlaces de comunicações táticas de longa distância em HF é usual utilizar antenas log-periódicas ([https://en.wikipedia.org/wiki/Log-periodic\\_antenna](https://en.wikipedia.org/wiki/Log-periodic_antenna)), devido ao seu maior ganho (~10 dBi) e sua maior banda operacional (8:1), conforme (A) e (C) abaixo. Estações táticas que usam antenas log-periódicas são em geral localizadas em bases militares, afastadas do teatro de operações ativas de guerra. Devido ao seu maior tamanho, antenas log-periódicas não são adequadas para estações moveis em HF. Apesar de seu maior ganho, o HPBW do padrão de irradiação de uma log-periódica é suficientemente amplo, conforme (B), para que seu sinal e os sinais das demais múltiplas estações táticas no teatro de operações ativas de guerra sejam interceptados simultaneamente, facilitando o processo de correlação e identificação dos diversos sinais.

### (A) Quick Summary (CST Antenna Magus)

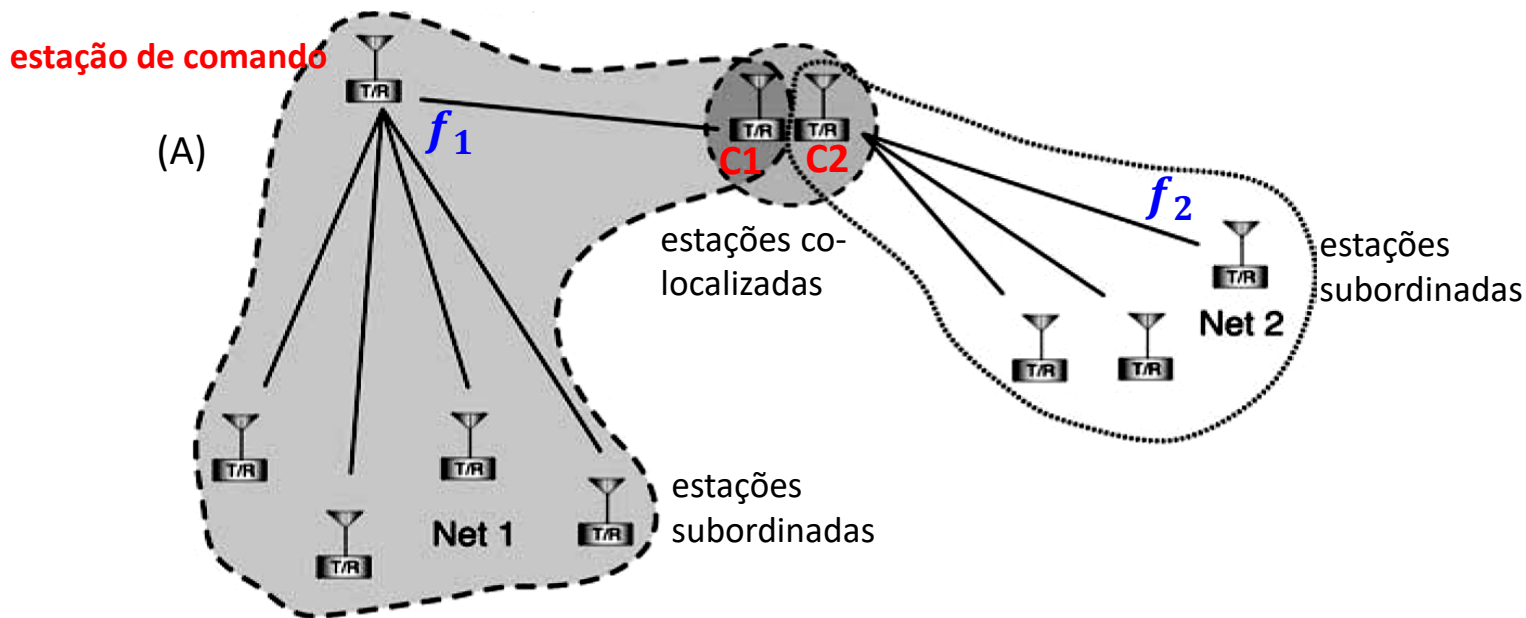
Quantity	Typical	Minimum	Maximum
Polarization	Linear	-	-
Radiation pattern	Unidirectional, axial back-fire beam.		E -30°; H-40° E-80°; H-150°
Gain	10 dBi	6 dBi	12 dBi
Bandwidth	8:1	2:1	150:1
Complexity	Medium	-	-
Impedance	100 $\Omega$	50 $\Omega$	300 $\Omega$
Balun	Infinite balun	-	-
Phase center	Varying with frequency	-	-





## Detecção de ameaças – sinais de comunicações:

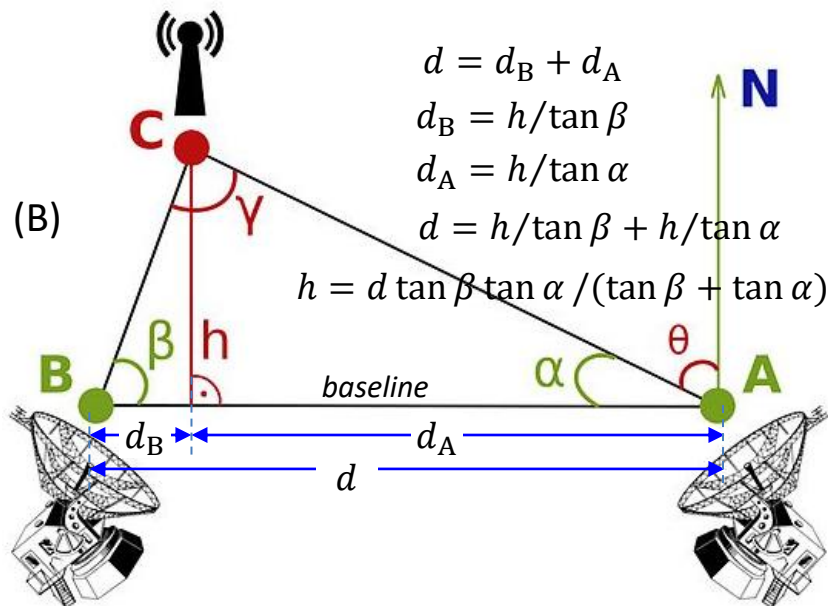
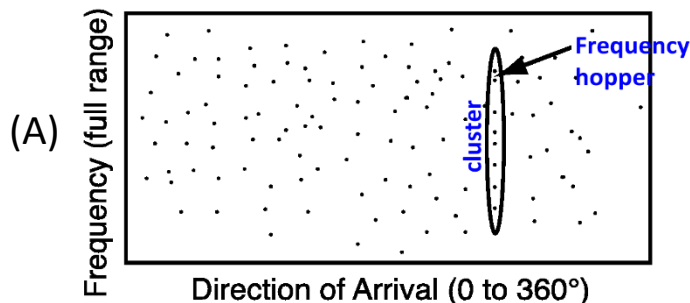
Em grande parte, comunicações táticas ocorrem em redes “push-to-talk” (<https://en.wikipedia.org/wiki/Push-to-talk>). Isso envolve vários transceptores operando na mesma frequência no teatro de operações ativas de guerra, com apenas uma estação transmitindo por vez. Conforme mostrado em (A), uma rede típica tem um comando e várias estações subordinadas. A maior parte da comunicação ocorre entre a estação de comando e as subordinadas, com a estação de comando transmitindo com um *duty-cycle* (ciclo de trabalho) significativamente maior que o das subordinadas. A rede “Net 1” em (A) opera na frequência  $f_1$  e é comandada diretamente pela estação de comando, estação que é usualmente localizada em uma base militar afastada do teatro de operações ativas de guerra. A rede “Net 2” opera na frequência  $f_2$  e é comandada pela estação co-localizada C2. Situada no mesmo local que a estação C2, a estação C1 se comunica com a estação de comando viabilizando o fluxo de informação entre Net 2 e a estação de comando. Note que para maximizar a eficácia de uma ação de EA (*Electronic Attack*) sobre a rede através de *jamming*, o primeiro nó da rede que deve ser alvo de interrupção são as estações co-localizadas C1 e C2, porque desta forma fica imediatamente inviabilizada a intercomunicação de todas as estações da Net 2 com a estação de comando. Para que o *jammer* possa apontar sua antena para o alvo, preliminarmente um sistema de EW para localização de emissores de radiação EM (slide 11) deve interceptar o sinal das estações C1 e/ou C2 e determinar sua localização através de algoritmos para determinação do DOA (*Direction of Arrival*) do sinal interceptado, simultaneamente efetuando a triangulação dos ângulos de DOA conforme mostrado em (B) no próximo slide (ver [https://en.wikipedia.org/wiki/Direction\\_finding](https://en.wikipedia.org/wiki/Direction_finding)).





## Detecção de ameaças – sinais de comunicações:

Sistemas de EW para interceptação de sinais de comunicação (slides 11 e 25) frequentemente incluem um *display* exibindo frequência  $\times$  ângulo DOA de cada sinal interceptado, conforme mostrado em (A). Em um teatro de operações ativas de guerra os sinais das estações táticas tendem a ser espalhados aleatoriamente em azimuth (DOA), porque usualmente as estações estarão em movimento, como também são aleatoriamente espalhados em frequência, porque os sistemas de comunicações táticas sempre adotam algum esquema de *frequency hopping* para minimizar a probabilidade de detecção e identificação. Instantaneamente, cada ponto do *display* em (A) representa o DOA e a frequência do sinal de uma estação interceptada. No entanto, quando se efetua o somatório (integração) de todos os pontos mostrados no *display* ao longo de um intervalo de tempo  $\Delta t$  (intervalo de integração), um padrão de pontos emerge como resultado do somatório, ocorrendo um *cluster* (agrupamento) de pontos ao longo da linha que identifica o DOA da estação interceptada conforme mostra (A), o que permite identificar o DOA de cada estação. Se a estação estiver parada, o *cluster* respectivo a ela será indicado por um único DOA estático no *display*. Se a estação estiver em movimento, para um especificado intervalo  $\Delta t$  em que é efetuado o somatório dos pontos no *display*, é possível acompanhar no *display* o histórico de evolução do *cluster* ao longo da sequência de somatórios que ocorrem a cada  $\Delta t$ , viabilizando assim estimar ao longo do tempo o DOA da estação respectiva ao *cluster*. Uma vez determinados os DOAs  $\alpha$  e  $\beta$  de uma estação C interceptada simultaneamente por dois sistemas de EW A e B para interceptação de sinais, sendo A e B separados de uma distância  $d$ , é possível determinar a localização da estação C mediante, por exemplo, triangulação simples, conforme mostrado em (B). Obviamente as antenas parabólicas mostradas em (B) são inviáveis nas faixas de HF, VHF e UHF devido ao seu tamanho, situação em que são substituídas por *phased arrays* ([https://en.wikipedia.org/wiki/Phased\\_array](https://en.wikipedia.org/wiki/Phased_array)), que serão estudados em capítulo posterior desta disciplina.



**Exemplo 6:** Dois sistemas de EW A e B para interceptação de sinais são separados por uma *baseline* de  $d = 19\text{Km}$ . Ambos interceptam o sinal de uma estação inimiga C respectivamente recebido com azimutes do DOA  $\alpha = 35^\circ$  e  $\beta = 53^\circ$ . **Determine:** (a) A distância  $h$  entre C e a *baseline*. (b) As distâncias  $d_A$  e  $d_B$  que localizam a intersecção da linha  $h$  com a *baseline*. **Solução:** (a)  $h = \frac{d \tan \beta \tan \alpha}{\tan \beta + \tan \alpha} = 8.709 \text{ [Km]}$  (b)  $d_A = h / \tan \alpha = 12.437 \text{ [Km]}$   $d_B = h / \tan \beta = 6.563 \text{ [Km]}$ .

Um sinal é considerado LPI (*low probability of intercept*) quando a forma de onda do sinal (*waveform*) minimiza a probabilidade de o mesmo ser detectado pelo *search receiver* de um sistema de EW (slides 11 e 25). A forma de onda do sinal é determinada pelo processo de modulação adotado.

Tanto para um sistema de radar como para um sistema de comunicações, **o objetivo é viabilizar que o sistema que transmite o sinal LPI funcionalmente opere de modo eficaz sob o paradigma “ver sem ser visto”, mas simultaneamente mantenha a detectabilidade do sinal LPI irradiado abaixo do limiar de detecção do *search receiver* da facção inimiga ou de qualquer outro sub-sistema de detecção similar pertencente à facção inimiga.**

Radares LPI serão discutidos em capítulo posterior desta disciplina. Usualmente radares LPI adotam uma combinação de HPBW estreito e minimização dos lobos secundários no padrão de irradiação da antena, baixa potência efetiva irradiada e modulação LFM (*chirp*).

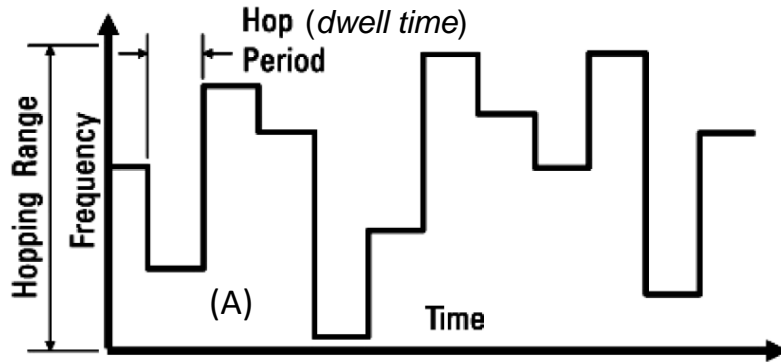
Sinais LPI para comunicações minimizam o seu limiar de detecção basicamente em função da modulação adotada, que procura assemelhar o sinal modulado a um ruído aleatório, o que dificulta a detecção e *jamming* do sinal pelo(s) RX(s) de EW da facção inimiga. Independente da modulação, a forma mais simples e imediata para gerar um sinal LPI em um enlace de comunicações é reduzir a potência do TX a um nível mínimo mas que assegure uma relação sinal ruído (SNR – *signal to noise ratio*) suficientemente alta para que o RX do enlace possa demodular o sinal. A menor potência do TX reduz o alcance no qual qualquer RX da facção inimiga possa detectar o sinal transmitido. Outra maneira simples para gerar um sinal LPI é o uso de antenas com padrão de radiação estreito e lobos secundários reduzidos. Uma antena com esta característica irradia menos potência fora da direção de *boresight* que aponta para o RX do enlace, tornando difícil o sinal ser detectado por um RX inimigo localizado fora da direção de *boresight*. Ainda, se a duração do sinal irradiado for reduzida, os algoritmos de detecção do RX inimigo terão menos tempo de processamento disponível para detectar o sinal e muito menos tempo ainda para determinar o(s) seu(s) ângulo(s) de DOA (*Direction Of Arrival*), reduzindo assim a probabilidade de interceptação.

No entanto, nenhuma técnica para geração de sinais LPI é tão eficaz quanto um processo de modulação que torne o sinal irradiado um sinal aleatório. Neste contexto, três tipos de modulação são usualmente adotadas para este fim: (1) *Frequency hopping*, (2) *Chirp* e (3) *Direct sequence spread spectrum*.

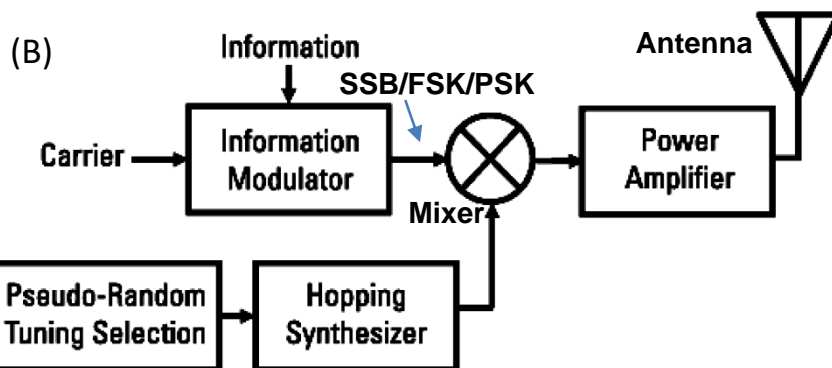
- **Frequency hopping:** A frequência  $f_n$  da portadora do sinal irradiado pelo TX muda periodicamente de valor, mudança que é efetuada em saltos de frequência. Especificamente, o valor instantâneo  $f_n$  de cada frequência é extraído de um conjunto  $F = \{f_1, f_2, \dots, f_n, \dots, f_N\}$  de  $N$  frequências pré-estabelecidas e conhecidas tanto pelo TX como pelo RX. O índice  $n$  de cada frequência  $f_n$  extraída de  $F$  é determinado por um gerador pseudo-randômico, cuja sequência de frequências  $f_n$  é conhecida pelo TX e RX, mas não é conhecida pelo RX inimigo. O intervalo dos saltos no domínio frequência é muito maior do que a largura de banda do espectro da onda EM que transporta a informação (i.e., muito maior que a largura de banda da informação). Ver [https://en.wikipedia.org/wiki/Frequency-hopping\\_spread\\_spectrum](https://en.wikipedia.org/wiki/Frequency-hopping_spread_spectrum).
- **Chirp:** A frequência  $f$  da portadora do sinal irradiado pelo TX é continuamente e rapidamente variada ao longo de uma faixa de frequência significativamente mais ampla do que a largura de banda da informação. Em geral a modulação LFM (*Linear Frequency Modulation*) é adotada, no entanto não são raros sistemas com variação não-linear da frequência. A aleatoriedade é obtida através de um gerador pseudo-randômico no TX que determina o instante do início da rampa de subida da frequência (ou de descida da frequência em alguns sistemas) do sinal irradiado. O RX conhece o padrão pseudo-randômico que determina o instante de início da rampa de frequência do sinal irradiado pelo TX, de modo que o sinal recebido pode ser demodulado. Um RX inimigo, por não conhecer o padrão pseudo-randômico do instante de início da rampa, fica impossibilitado de demodular o sinal. Ver [https://en.wikipedia.org/wiki/Chirp\\_spread\\_spectrum](https://en.wikipedia.org/wiki/Chirp_spread_spectrum).
- **Direct sequence spread spectrum:** Sobre o sinal da(s) portadora(s) já modulada(s) no TX pelos símbolos IQ de alguma modulação digital (usualmente M-QAM e/ou M-PSK) é aplicada uma modulação BPSK com duração dos símbolos IQ muito menor que a duração dos símbolos IQ da modulação M-QAM/M-PSK, processo que é denominado de *spreading*. Como a taxa de símbolos BPSK (denominado *chiprate*) é muito maior que a taxa de símbolos M-QAM/M-PSK (denominado *symbolrate*), a largura do espectro resultante é muito maior que o espectro do sinal modulado em M-QAM/M-PSK. A razão *chiprate/symbolrate* é denominada de *processing gain*. A sequência de símbolos BPSK no TX é obtida a partir de um gerador pseudo-randômico de bits – bit 1 para o símbolo BPSK  $1e^{j0^\circ}$  e bit 0 para o símbolo BPSK  $1e^{j180^\circ}$ , ou vice-versa. O RX conhece a sequência de símbolos pseudo-randômicos gerada no TX, o que habilita o RX a efetuar o processo de *despreading*, viabilizando a demodulação do sinal recebido. Um RX inimigo, por não conhecer a sequência de símbolos BPSK pseudo-randômicos gerada no TX, fica impossibilitado de demodular o sinal. Ver slides 14 a 59, 117 e 118 de [http://www.fccdecastro.com.br/pdf/T2\\_Aulas21a26\\_26062020.pdf](http://www.fccdecastro.com.br/pdf/T2_Aulas21a26_26062020.pdf).

## Sinais Frequency Hopping

Sinais FH (*frequency hopping*) frequência são largamente utilizados porque viabilizam um espalhamento espectral muito amplo no domínio frequência. O gráfico em (A) mostra a frequência versus tempo para um sinal FH. O sinal pausa em uma frequência por um curto período de tempo e então salta (*hop*) para outra frequência selecionada aleatoriamente. O tempo de permanência em uma frequência é denominado *dwell time*. O *hopping rate* é o número de saltos por segundo e é o inverso do *dwell time*. O *hopping range* é a faixa de frequência na qual as frequências de transmissão podem ser selecionadas. Toda a largura de banda do sinal é movida para a frequência atribuída para cada salto.



O diagrama de blocos de um TX FH é mostrado em (B). O sinal analógico em banda-base (usualmente SSB) ou o digital em banda-base (usualmente FSK ou PSK) é convertido em sinal FH através do processo de heterodinação realizado pelo *Mixer* e do sinal de batimento (*beat signal*) do sintetizador de frequência (*hopping synthesizer*), cuja frequência instantânea da senóide gerada em sua saída é controlada pela palavra binária que resulta na saída do gerador pseudo-randômico (*pseudo random tuning selection*), de modo que após cada salto (*hop*) a frequência do sinal transmitido é selecionada aleatoriamente. Note que o sinal do *hopping synthesizer* é o sinal do oscilador local (*local oscillator*) para o *Mixer*. O RX FH no outro lado do enlace inclui em seu *front-end* de RF um *hopping synthesizer* que gera uma sequência de frequências idêntica à sequência do TX, de modo que o RX é sequencialmente sintonizado na frequência de cada salto efetuado no TX.

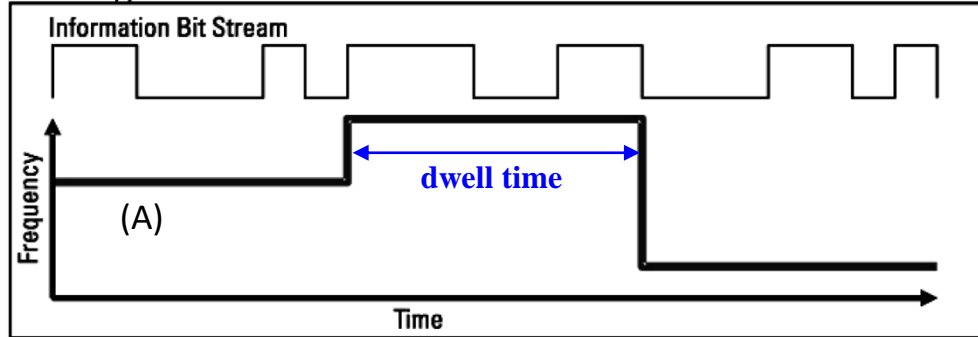


É necessário preliminarmente sincronizar os *hopping synthesizers* no TX e RX, de modo que o início de cada salto ocorra no mesmo instante de tempo. Imediatamente após o RX ser ligado é efetuada a sincronização inicial, processo que pode demorar até 500ms sob uma baixa SNR (*signal to noise ratio*) no canal. Cada vez que um novo sinal é recebido o RX ajusta os parâmetros da sincronização inicial, mas o algoritmo que faz este ajuste é de uma complexidade computacional bem menor que o algoritmo que efetua a sincronização inicial e portanto a pequena duração do recorrente processo de ajuste não impacta na operação do enlace.

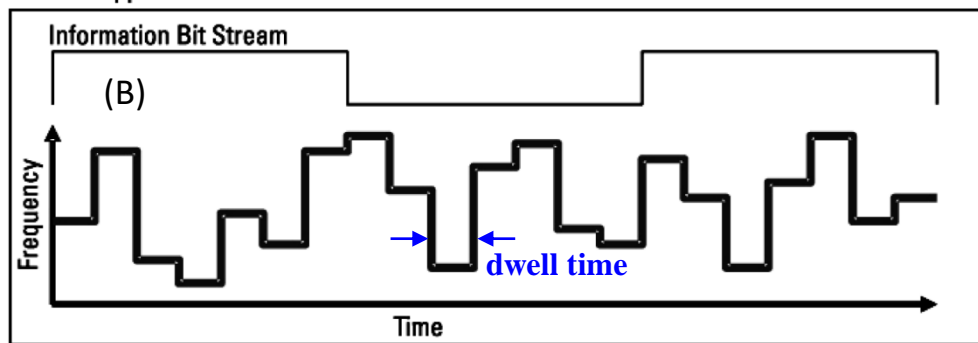
## Sinais *Slow hopper* e *Fast Hopper*

Um sinal *slow hopper* apresenta um longo *dwell time* em relação a duração do símbolo IQ da modulação digital (usualmente M-FSK ou M-PSK – ver (B) no slide anterior), de modo que múltiplos bits do *stream* de bits são transmitidos pelo TX durante o *dwell time* em cada *hop* (=salto) de frequência, conforme mostrado em (A). Um sinal *fast hopper* apresenta comportamento oposto, tendo um curto *dwell time* em relação a duração do símbolo IQ da modulação digital, conforme mostrado em (B).

Slow Hopper



Fast Hopper



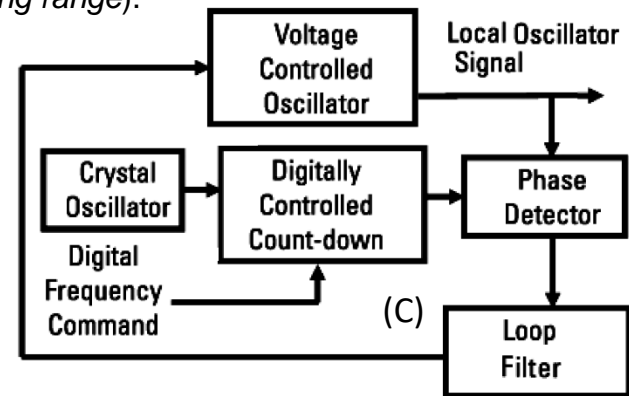
Por exemplo, ver

[http://www.worldsecurity-index.com/images/qmac/HF-90M%20Transceiver\\_Mar03\\_web.pdf](http://www.worldsecurity-index.com/images/qmac/HF-90M%20Transceiver_Mar03_web.pdf) ,

<http://www.worldsecurity-index.com/index.php?pg=91> e

<https://www.harris.com/press-releases/2019/02/harris-corporation-introduces-high-capacity-line-of-sight-radio-with> .

O *slow hopper* usa um sintetizador com PLL (*Phase Locked Loop* – ver [https://en.wikipedia.org/wiki/Phase-locked\\_loop](https://en.wikipedia.org/wiki/Phase-locked_loop) , conforme mostrado em (C)). Um sintetizador com PLL é capaz de cobrir uma faixa de frequência muito ampla (amplo *hopping range*).

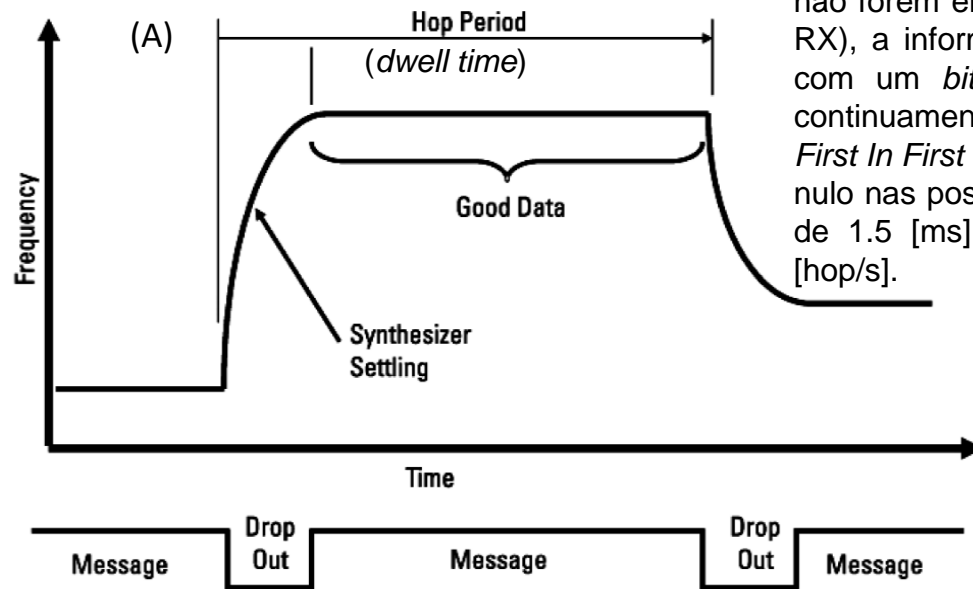


Como toda a potência do sinal *slow hopper* permanece em uma única frequência de transmissão por um tempo (*dwell time*) suficientemente longo para transmitir vários bits, o *slow hopper* é um sinal relativamente fácil de ser detectado por um RX inimigo. No entanto, os constantes saltos em múltiplas e aleatórias frequências dificulta ao sistema inimigo realizar funções importantes no âmbito de EW, como localização de emissor de radiação EM e *jamming*.



## Sinais *Slow hopper* e *Fast Hopper*

A largura de banda  $BW$  do filtro do *loop filter* do PLL do sintetizador (ver (C) no slide anterior) é crucial para o desempenho do sistema FH. Quanto mais larga for a  $BW$  do *loop filter* menor o *settling time* do *loop* e mais rápido o sintetizador pode gerar uma nova frequência. Por outro lado, quanto mais estreita for a banda  $BW$  do filtro do *loop*, maior será a  $SNR$  (*signal to noise ratio*) do sinal demodulado, aumentando a sua inteligibilidade. O período transitório (*settling time*) do *loop* de um sintetizador para sistemas FH é tipicamente 15% do *dwell time*. Assim, por exemplo, um sistema com um *hopping rate* de 100 [hop/s] terá um *dwell time* de 10 [ms] e o *settling time* do *loop* será tipicamente 1.5 [ms]. A tentativa de transmitir informação antes do término do *settling time* inviabiliza a recepção no RX. Portanto a transmissão do *stream* de bits que transporta a mensagem (informação) é interrompida durante os intervalos de *drop-out* mostrador em (A), intervalos que correspondem aos intervalos de *settling time* do *loop*.



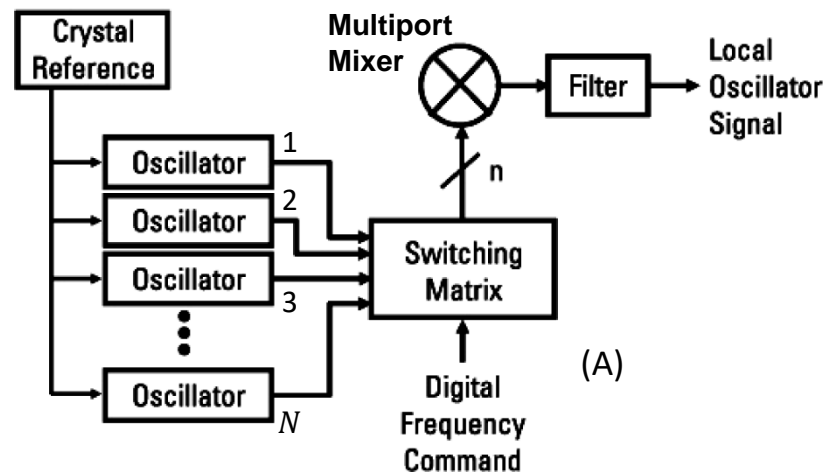
Para eliminar os intervalos de *drop-out* em sistemas FH de voz (que, se não forem eliminados, comprometeria a inteligibilidade da voz recebida no RX), a informação de voz é digitalizada gerando um *stream* de bits “#1” com um *bitrate* de, por exemplo, 16Kbps. O *stream* de bits “#1” é continuamente armazenado sob o *bitrate* de 16kbps em uma fila (FIFO – *First In First Out*). A FIFO já tem previamente gravada as amostras de valor nulo nas posições de memória que correspondem ao intervalo de *drop-out* de 1.5 [ms], conforme exemplo do sistema com *hopping rate* de 100 [hop/s].

A FIFO é continuamente lida sob um *bitrate* de 20 Kbps gerando o *stream* de bits “#2” na sua saída, que é transmitido juntamente com os intervalos de *drop-out* que foram inseridos na FIFO, em sincronismo com os *settling time* do *loop* do sintetizador. No RX, o processo é revertido. O *stream* de bits “#2” recebido sob uma taxa de 20Kbps é gravado em uma FIFO, e a FIFO é lida gerando uma réplica em sua saída do *stream* de bits “#1”, sob uma taxa de 16 kbps. Mas note que a leitura é feita somente nas posições de memória da FIFO que correspondem a amostras do sinal de informação. As amostras nas posições de memória que correspondem ao intervalo de *drop-out* não são lidas. Deste modo, os intervalos de amostras de informação são lidos sequencialmente (pulando as amostras armazenadas em posições de memória que correspondem aos intervalos de *drop-out*), reconvertendo o sinal em uma sequência de amostras contínuas de informação sem a interrupção do *drop-out*.

Quando as frequências e o *dwell time* do TX e RX são sincronizados e os *drop-outs* resultantes do *settling-time* do sintetizador são removidos, o processo de salto em frequência é basicamente transparente ao usuário. Embora a discussão nos parágrafos anteriores considere sinais de voz, as mesmas considerações se aplicam às transmissões de dados digitais.

## Sinais *Slow hopper* e *Fast Hopper*

Um sinal *fast hopper* representa um desafio significativamente maior para o RX inimigo, porque os saltos em frequência ocorrem muito rapidamente. Analisando o espectro de um sinal *fast hopper* observa-se uma relação inversa entre o *dwell time* e a largura de banda BWd do RX inimigo necessária para detectar o sinal *fast hopper*. Por exemplo, um sinal *fast hopper* com *dwell time* de 1  $\mu$ s requer BWd de 1 MHz no RX inimigo para que o sinal seja detectado. Como a largura de banda BW da informação transportada pelo sistema FH é muito mais estreita do que a BWd necessária no RX inimigo para detecção do sinal, a sensibilidade do RX inimigo será fortemente comprometida devido a redução da SNR (*Signal to Noise Ratio*) resultante da maior potência de ruído captada na maior banda BWd. Um RX com uma BW estreita sincronizado com o TX detecta normalmente o sinal *fast hopper*, e os demais blocos funcionais do RX operam com a largura de banda BW dos sinais de informação transportados, não havendo portanto degradação da SNR. No entanto, um RX inimigo desconhece a sequência de *hops* em frequência e portanto não consegue sincronizar com o sinal. Será necessário então que o RX inimigo opere em uma largura de banda BWd muito mais larga que a banda BW. Isto dificulta ao RX inimigo detectar a presença do sinal *fast hopper*, devido à redução da sensibilidade do RX em consequência da baixa SNR. Um problema com sinais *fast hopper* é que eles exigem sintetizadores com *hardware* complexo. Em (A) é mostrado o diagrama de blocos de um sintetizador *fast hopper*. Note que há  $N$  osciladores, todos eles operando em regime permanente – não há período transitório e portanto não há *settling time* para cada salto em frequência. A cada *dwell time*, o *switching matrix* conecta o sinal de  $n$  osciladores às  $n$  portas de entradas do *Multiport Mixer* (ver, por exemplo, <https://ieeexplore.ieee.org/document/4294525?arnumber=4294525>) e configura o bloco *Filter* de modo a eliminar os produtos de heterodinação indesejados na saída do *Multiport Mixer*, gerando uma única frequência na saída *Local Oscillator Signal*. Como esse processo é muito mais rápido do que sintonizar o *loop* de um PLL, o sintetizador em (A) é capaz de gerar uma sequência de saltos em frequência muito mais rapidamente que um sintetizador baseado em PLL. A complexidade do hardware do sintetizador em (A) é proporcional ao número de frequências que ele pode gerar, e, portanto, é usual que um sistema *fast hopper* gere um conjunto de frequências com menos frequências do que um sistema *slow hopper* baseado em sintetizadores com PLL.



Basicamente, há duas técnicas para implementar um sinal *chirp*:

(1) O **Wide Linear Sweep** consiste em o TX transmitir varrendo a frequência de heterodinação de um sinal digital modulado em banda-base, varredura que é feita ao longo de uma ampla faixa de frequência denominada *sweep range* ( $SwR$ ), sendo  $SwR$  muito maior do que a largura de banda  $BW$  do sinal em banda-base. O instante de início de cada ciclo de varredura em frequência é determinado por um gerador pseudo-randômico. Isso impede que um RX hostil sincronize com os ciclos de varredura em frequência do *chirp*.

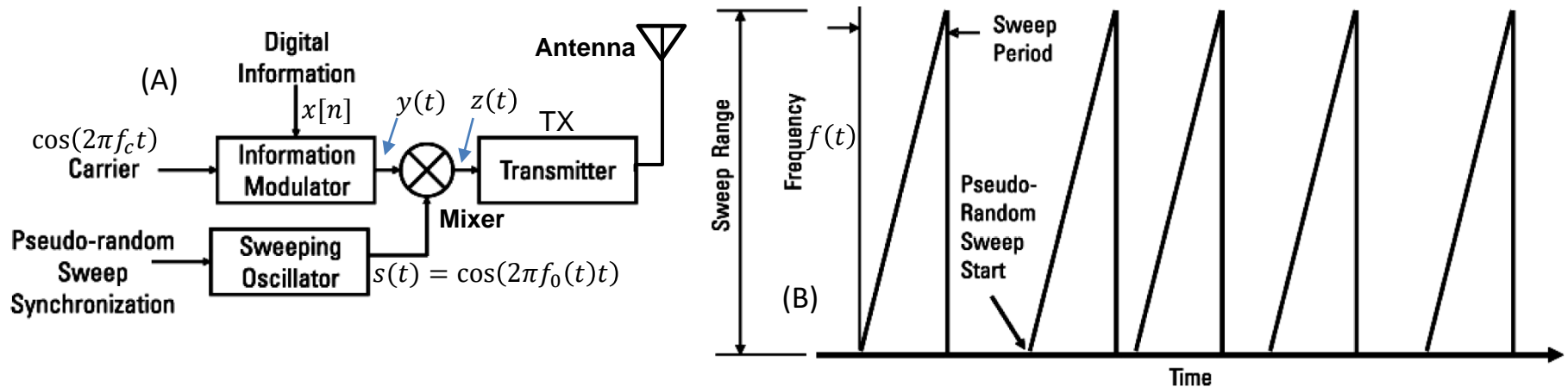
(2) O **Chirp on Each Bit** consiste em aplicar o *chirp* a cada bit do sinal digital – um sinal *upchirp* representando o bit “1” com frequência crescente no *sweep range* e um sinal *downchirp* representando o bit “0” com frequência decrescente no *sweep range*. Cada um dos dois sinais é detectado no RX pelo respectivo *matched-filter* (filtro casado – ver [http://www.fccdecastro.com.br/pdf/T2\\_Aula12\\_24042020.pdf](http://www.fccdecastro.com.br/pdf/T2_Aula12_24042020.pdf)). O *matched-filter* casado ao *upchirp* resulta em sua saída um impulso para o bit “1”. O *matched-filter* casado ao *downchirp* resulta em sua saída um impulso para o bit “0”.

Ambos métodos têm ganho de processamento  $G_p$  definido pela razão  $G_p = SwR/BW$ . Quanto maior for o ganho  $G_p$  do sinal *chirp* menor capacidade terá um sistema EW inimigo para efetuar *jamming* sobre o sinal desejado recebido no RX. A capacidade de um *jammer* é medida pelo J/S (*jamming-to-signal ratio*). J/S é a razão entre a potência do sinal do *jammer* medida na antena do RX que está sofrendo *jamming* e a potência do sinal desejado recebido medido na mesma antena.

Para cada tipo de RX e para cada tipo de sinal de *jamming* há um limiar de J/S a partir do qual o RX fica impossibilitado de demodular o sinal recebido desejado, em consequência do sinal indesejado de *jamming*. O ganho de processamento  $G_p$  do sinal *chirp* aumenta proporcionalmente o limiar de J/S a partir do qual o RX não consegue demodular o sinal, reduzindo a sensibilidade do RX ao *jamming*.

## Wide Linear Sweep

Em (A) o *sweeping oscillator* gera uma cossenóide  $s(t)$  cuja frequência  $f_0(t)$  é variada ao longo do *sweep range* ( $SwR$ ) em (B), sendo  $SwR$  muito maior do que a largura de banda  $BW$  do sinal discreto  $x[n]$  que representa a informação em banda-base. O sinal digital  $x[n]$  modula a portadora de frequência  $f_c$  e o sinal modulado  $y(t)$  resultante é heterodinado no *Mixer* com o sinal  $s(t)$ , transladando o espectro de  $y(t)$  para uma frequência  $f(t) = f_c + f_0(t)$  conforme mostrado em (B), que é a frequência central do espectro do sinal de saída  $z(t)$ .

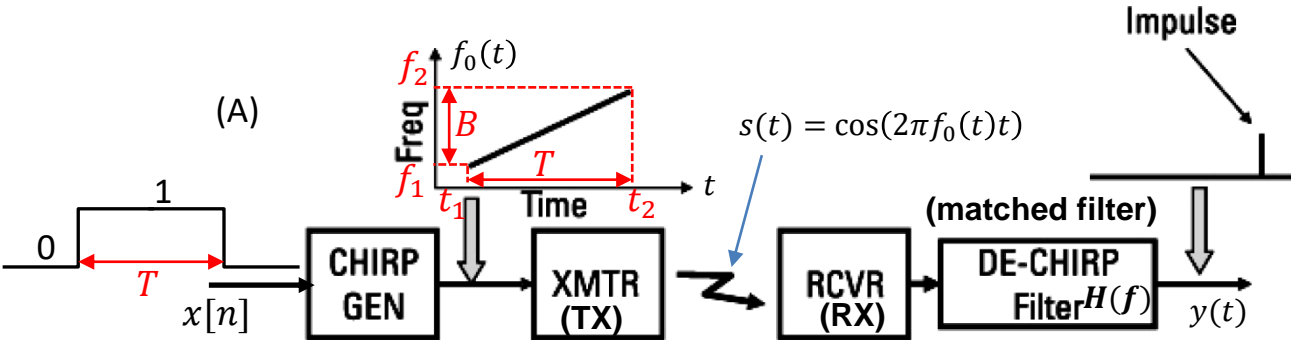


Note em (B) que o início de cada ciclo de varredura de  $f(t)$  é o início de cada rampa. Note também que o início de cada rampa é determinado por um gerador pseudo-aleatório (bloco *pseudo random sweep synchronization* em (A)), evitando que um RX inimigo seja capaz de sincronizar com a sequência de ciclos  $f(t)$ . O RX da facção amiga conhece a sequência gerada pelo bloco *pseudo random sweep synchronization* do TX, e, portanto, o *sweeping oscillator* no RX consegue sincronizar e demodular o sinal recebido. Ainda, note em (A) que o sinal irradiado pela antena do TX é o sinal  $z(t)$  e que  $f(t)$  é a frequência central instantânea do espectro de  $z(t)$ .

Observe que alguns sistemas aleatorizam também a declividade da rampa de  $f(t)$ , de modo que o *chirp* não tenha uma taxa de varredura constante, dificultando ainda mais a demodulação pelo RX inimigo.

## Chirp on Each Bit

Conforme mostrado em (A), o TX transmite um *chirp* a cada bit, i.e., transmite um *burst* de RF modulado pela modulação LFM (*Linear Frequency Modulation*), que varre a frequência  $f_0(t)$  do sinal  $s(t) = \cos(2\pi f_0(t)t)$  no intervalo  $f_1 < f_0(t) < f_2$  durante o intervalo de tempo  $T$  correspondente a cada bit "1" (ou a cada bit "0") na sequência  $x[n]$  de bits a serem transmitidos. O bloco *chirp gen* gera a rampa  $f_0(t)$  com frequência crescente, de modo que o sinal  $s(t)$  é um *upchirp*. O valor do bit "1" é recuperado no RX pelo *de-chirp filter*, que é um *matched-filter* casado ao sinal do *upchirp*, resultando em um impulso em sua saída a cada *upchirp* recebido.



Mesmo processo é adotado para transmissão e recepção de cada bit "0" na sequência  $x[n]$  de bits, com a diferença que  $f_0(t)$  é uma rampa com declividade negativa (frequência decrescente com o tempo) resultando em um impulso na saída do *matched-filter* casado ao *downchirp*, conforme discutiremos no slide 72.

O *burst* de RF (=pulso *chirp*) tem duração de  $T$  [s] e ocorre no intervalo de tempo  $t_1 < t < t_2$ , com sua frequência  $f_0(t)$  variando linearmente na banda  $B = f_2 - f_1$  [Hz] durante o intervalo  $T = t_2 - t_1$ . Para reduzir a largura do pulso *chirp* e torna-lo um pulso estreito de grande amplitude, maximizando assim a amplitude da representação do *chirp* no RX, a função de transferência  $H(f)$  do *matched filter* deve ter um atraso de grupo  $\tau_g(f) = -\frac{1}{2\pi} \frac{d\angle\{H(f)\}}{df}$  [s] que deve ser compatível com a duração  $T$  do pulso *chirp* (ver <https://dspillustrations.com/pages/posts/misc/group-delay-and-phase-delay-example.html>). Especificamente, o valor de  $\tau_g(f)$  deve ser máximo para a frequência inicial  $f_1$ , a primeira a ser gerada pelo *chirp gen*, reduzindo linearmente seu valor com o aumento da frequência  $f$  até a frequência final  $f_2$ , a última a ser gerada pelo *chirp gen*, de tal forma que a condição  $\tau_g(f_2) = \tau_g(f_1) - T$  seja obedecida. Esta condição para o atraso de grupo  $\tau_g(f)$  da função de transferência  $H(f)$  do *matched-filter* garante que cada componente espectral de  $s(t) = \cos(2\pi f_0(t)t)$  na banda  $B = f_2 - f_1$  [Hz] estejam presentes na saída do *matched-filter* no mesmo instante de tempo e com a mesma fase, interferindo-se construtivamente entre si, produzindo um pulso estreito de grande amplitude (no limite, um impulso) em consequência da amplificação pela interferência construtiva, o que maximiza a capacidade de detecção do *chirp* pelo RX.



## Sinais Chirp

A função de transferência  $H(f)$  definida em (12) abaixo é uma possível função de transferência para que o *matched filter* apresente um atraso de grupo  $\tau_g(f) = -\frac{1}{2\pi} \frac{d\angle\{H(f)\}}{df}$  [s] linearmente variante com a frequência  $f$  e obedeça a condição  $\tau_g(f_2) = \tau_g(f_1) - T$  de modo a converter o *burst* de RF (=pulso *chirp*) de duração  $T$  [s] em um impulso.

$$H(f) = e^{-j\pi \frac{(f-f_c)^2}{k}} \quad (12)$$

onde  $f_c = (f_1 + f_2)/2$  é a frequência central da banda  $B = f_2 - f_1$  [Hz] de varredura linear da frequência instantânea do *chirp*  $s(t) = \cos(2\pi f_0(t)t)$ ,  $f_0(t) = kt + f_b$  é a frequência instantânea de  $s(t)$  no intervalo de tempo  $t_1 < t < t_2$ ,  $k = \frac{f_2 - f_1}{t_2 - t_1} = \frac{B}{T}$   $\left[\frac{\text{Hz}}{\text{s}}\right]$  é a constante que define a declividade da rampa  $f_0(t)$  no intervalo de frequência  $f_1 < f_0(t) < f_2$  e  $f_b = -\frac{f_1 t_2 - f_2 t_1}{t_1 - t_2}$  de tal forma que  $f_0(t_1) = f_1$  e  $f_0(t_2) = f_2$ . Note de (12) que o sinal “-” no argumento da exponencial indica que o *matched-filter* atrasa as componentes espectrais do sinal que nele trafega e que a fase da  $H(f)$  do *matched-filter* casado ao *chirp*  $s(t) = \cos(2\pi f_0(t)t)$  é

$$\angle\{H(f)\} = \pi \frac{(f - f_c)^2}{k} \quad (13)$$

resultando em um atraso de grupo  $\tau_g(f) = -\frac{1}{2\pi} \frac{d\angle\{H(f)\}}{df}$  [s] dado por

$$\tau_g(f) = -\frac{1}{2\pi} \frac{d\angle\{H(f)\}}{df} = \frac{1}{k} (f_c - f) = \frac{1}{k} \left( \frac{(f_1 + f_2)}{2} - f \right) \quad (14)$$

Note de (14) que para  $f = f_1 \rightarrow \tau_g(f_1) = \frac{f_2 - f_1}{2k} = \frac{B}{2k} = \frac{T}{2}$  e que para  $f = f_2 \rightarrow \tau_g(f_2) = -\frac{f_2 - f_1}{2k} = -\frac{B}{2k} = -\frac{T}{2}$ . Portanto, o valor máximo  $\tau_g(f_1) = T/2$  ocorre na frequência inicial  $f_1$ , reduzindo linearmente seu valor com o aumento da frequência  $f$  até a frequência final  $f_2$ , com o valor mínimo  $\tau_g(f_2) = -T/2$  ocorrendo na frequência final  $f_2$ . Assim, conforme discutido no slide anterior, a condição  $\tau_g(f_2) = \tau_g(f_1) - T$  é obedecida, garantindo que cada componente espectral de  $s(t) = \cos(2\pi f_0(t)t)$  na banda  $B = f_2 - f_1$  [Hz] estejam presentes na saída do *matched-filter* no mesmo instante de tempo e com a mesma fase, interferindo-se construtivamente entre si, produzindo um pulso estreito de grande amplitude (no limite, um impulso) em consequência da amplificação pela interferência construtiva, o que maximiza a capacidade de detecção do *chirp* pelo RX.

## Sinais Chirp

O que precisamos comprovar agora é o fato de o sinal de *chirp*  $s(t) = \cos(2\pi f_0(t)t)$  recebido pelo RX ser transformado em um impulso na saída do *matched-filter* cuja função de transferência  $H(f)$  é dada por (12). Para tanto, para efeito de facilitar a solução das integrais no desenvolvimento que segue, vamos considerar  $s(t)$  como a parte real da função complexa

$$s_c(t) = e^{2\pi j(f_0(t)t)} = \cos(2\pi f_0(t)t) + j \sin(2\pi f_0(t)t) \quad (15)$$

A abordagem que adotaremos é determinar a saída  $y(t)$  do *matched-filter* através de  $y(t) = s(t) * h(t)$ , sendo "\*" o operador que denota a operação de convolução entre  $s(t)$  e  $h(t)$ , e onde  $h(t)$  é a resposta ao impulso do *matched-filter* obtida pela Transformada de Fourier Inversa de  $H(f)$  dada por (12), i.e.,  $h(t) = \mathcal{F}^{-1}\{H(f)\}$  (ver [http://www.fccdecastro.com.br/pdf/SS\\_Aulas9a12\\_27042020.pdf](http://www.fccdecastro.com.br/pdf/SS_Aulas9a12_27042020.pdf)). Ocorre que a operação de convolução é uma operação linear (ver [http://www.fccdecastro.com.br/pdf/SS\\_Aula5&6\\_26032020.pdf](http://www.fccdecastro.com.br/pdf/SS_Aula5&6_26032020.pdf)). Isto nos dá a liberdade para usar  $s_c(t)$  definido por (15) como representação de  $s(t)$  e simplesmente desprezar a parte imaginária no resultado da operação de convolução, i.e.,  $y(t) = \text{Re}\{y_c(t)\} = \text{Re}\{s_c(t) * h(t)\}$ . Substituindo  $f_0(t) = kt + f_b$  (ver slide anterior) em (15):

$$s_c(t) = e^{2\pi j(f_0(t)t)} = e^{j(2\pi(kt+f_b)t)} = e^{j2\pi j(kt^2+f_b t)} \quad (16)$$

onde

$$f_b = -\frac{f_1 t_2 - f_2 t_1}{t_1 - t_2} \quad (17)$$

é o valor da frequência instantânea  $f_0(t)$  do *chirp*  $s(t)$  para  $t = 0$ . Para simplificar o desenvolvimento algébrico, vamos assumir que  $f_0(t)$  tenha um valor final  $f_2$  de frequência em  $t = t_2$  e um valor inicial  $f_1$  de frequência em  $t = t_1 = -t_2$ , de modo que (17) simplifica para a frequência central  $f_c = (f_1 + f_2)/2$  da banda  $B = f_2 - f_1$  [Hz] de varredura linear do *chirp*  $s(t)$ :

$$f_b = -\frac{f_1 t_2 - f_2 t_1}{t_1 - t_2} = -\frac{f_1 t_2 - f_2(-t_2)}{(-t_2) - t_2} = \frac{f_1 t_2 + f_2 t_2}{2t_2} = (f_1 + f_2)/2 = f_c \quad (18)$$

Assim, sob a suposição  $t_1 = -t_2$ , (16) simplifica para

$$s_c(t) = e^{j2\pi j(f_c t + kt^2)} \quad (19)$$

## Sinais Chirp

Delimitando o *chirp*  $s_c(t)$  definido por (19) ao intervalo  $-T/2 < t < T/2$  para efeito de casar o *chirp* com a condição  $\tau_g(f_2) = \tau_g(f_1) - T$  do *matched-filter*, obtemos

$$s_c(t) = \text{Pulso}\left(\frac{t}{T}\right) e^{j2\pi(f_c t + kt^2)} \quad (20)$$

$$\text{onde } \text{Pulso}(x) = \begin{cases} 1.0, & |x| < 0.5 \\ 0.0, & x \geq 0.5 \end{cases}$$

Para obter  $y(t) = \text{Re}\{s_c(t) * h(t)\}$  precisamos determinar  $h(t) = \mathcal{F}^{-1}\{H(f)\}$ . Partindo de (12), isto é efetuado através de (ver [http://www.fccdecastro.com.br/pdf/SS\\_Aulas9a12\\_27042020.pdf](http://www.fccdecastro.com.br/pdf/SS_Aulas9a12_27042020.pdf)):

$$h(t) = \mathcal{F}^{-1}\{H(f)\} = \int_{-\infty}^{\infty} H(f) e^{j2\pi f t} df = \int_{-\infty}^{\infty} e^{-j\pi \frac{(f-f_c)^2}{k}} e^{j2\pi f t} df \quad (21)$$

Fazendo em (21)  $f - f_c = u$  de modo que  $f = u + f_c$  e  $df = du$  e com os limites de integração contemplando o fato de que quando  $f = \pm\infty$  então  $u = \pm\infty$ , obtemos:

$$h(t) = \int_{-\infty}^{\infty} e^{-j\pi \frac{u^2}{k}} e^{j2\pi(u+f_c)t} du = e^{j2\pi f_c t} \int_{-\infty}^{\infty} e^{-j\pi \frac{u^2}{k}} e^{j2\pi u t} du \quad (22)$$

Usando a integração simbólica do Matlab (<https://www.mathworks.com/help/symbolic/integration.html>) para resolver a integral em (22) e usando  $\lim_{u \rightarrow -\infty} \{\#1\} = 1.0$  e  $\lim_{u \rightarrow \infty} \{\#1\} = -1.0$  onde #1 é definido no script .m no próximo slide, resulta em:

$$\int_{-\infty}^{\infty} e^{-j\pi \frac{u^2}{k}} e^{j2\pi u t} du = \sqrt{-jk} e^{-j\pi k t^2} \quad (23)$$

## Sinais Chirp

```

% Integral of exp(i*pi*(u^2)/k)*exp(i*2*pi*u*t)
% from -inf to +inf
clear all % clear variables and reset symbolic engine
syms k u t % symbolic variables
assume (k > 0) % assume k > 0
% assume (t > 0) % assume t > 0
func = exp(-i*pi*(u^2)/k)*exp(i*2*pi*u*t); % function definition
Answer=int(func, u, -inf, inf); % answer
pretty(Answer); % format answer into math type-set

```

>> Answer:

```

>>      5/2          2
(-i)    sqrt(k) exp(k t pi li) ( lim #1)
      u -> -Inf

```

```

-----
      2
      5/2          2
(-i)    sqrt(k) exp(k t pi li) ( lim #1)
      u -> Inf
+ -----
      2

```

```

      5/2
(-i)    sqrt(k) = -sqrt(-i k)

```

where

```

#1 == erf(
      /      7/2          /      u pi \ \
      | (-i)    sqrt(k) | t pi - ---- | |
      |              \      k / |
      \      sqrt(pi) /

```

```

(lim #1) = 1.0
u -> -Inf

```

```

(lim #1) = -1.0
u -> Inf

```

Substituindo (23) em (22):

$$h(t) = e^{j2\pi f_c t} \int_{-\infty}^{\infty} e^{-j\pi \frac{u^2}{k}} e^{j2\pi ut} du = \sqrt{-jk} e^{j2\pi f_c t} e^{-j\pi kt^2} = \sqrt{-jk} e^{j2\pi \left( f_c t - \frac{kt^2}{2} \right)} \quad (24)$$

Uma vez obtido  $h(t)$  passamos a determinar  $y_c(t) = s_c(t) * h(t)$ . De (20) e (24) obtemos:

$$y_c(t) = s_c(t) * h(t) = \int_{-T/2}^{T/2} s_c(\tau) h(t - \tau) d\tau = \sqrt{-jk} \int_{-T/2}^{T/2} e^{j2\pi (f_c \tau + k\tau^2)} e^{j2\pi \left( f_c (t - \tau) - \frac{k(t - \tau)^2}{2} \right)} d\tau \quad (25)$$

Re-arranjando (25) :

$$y_c(t) = \sqrt{-jk} e^{j2\pi \left( f_c t - \frac{kt^2}{2} \right)} \int_{-T/2}^{T/2} e^{j2\pi \left( k\tau t + \frac{k\tau^2}{2} \right)} d\tau = \sqrt{-jk} e^{j2\pi \left( f_c t - \frac{kt^2}{2} \right)} \int_{-T/2}^{T/2} e^{j2\pi (k\tau t)} d\tau \int_{-T/2}^{T/2} e^{j2\pi \left( \frac{k\tau^2}{2} \right)} d\tau \quad (26)$$

Resolvendo as integrais de (26) e substituindo  $k = B/T$ :

$$\int_{-T/2}^{T/2} e^{j2\pi (k\tau t)} d\tau = \frac{\sin(\pi T k t)}{(\pi k t)} = \frac{\sin\left(\pi T \frac{B}{T} t\right)}{\left(\pi \frac{B}{T} t\right)} = \frac{\sin(\pi B t)}{\left(\pi \frac{B}{T} t\right)} \quad (27)$$

$$\int_{-T/2}^{T/2} e^{j2\pi \left( \frac{k\tau^2}{2} \right)} d\tau = \frac{\operatorname{erf}\left(\frac{T\sqrt{-j\pi k}}{2}\right)}{\sqrt{-jk}} = \frac{\operatorname{erf}\left(\frac{T\sqrt{-j\pi \frac{B}{T}}}{2}\right)}{\sqrt{-j \frac{B}{T}}} = \frac{\operatorname{erf}\left(\frac{\sqrt{-j\pi B T}}{2}\right)}{\sqrt{-j \frac{B}{T}}} \quad (28)$$

Nota: Para descrição da função  $\operatorname{erf}(x)$  ver <https://www.mathworks.com/help/matlab/ref/erf.html>

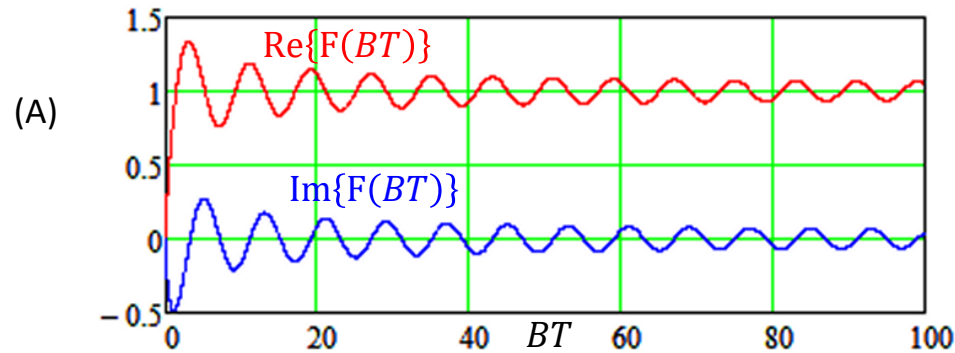


Substituindo (27) e (28) em (26):

$$y_c(t) = \sqrt{-j\frac{B}{T}} e^{j2\pi\left(f_c t - \frac{Bt^2}{2T}\right)} \frac{\sin(\pi Bt)}{\left(\pi\frac{B}{T}t\right)} \frac{\operatorname{erf}\left(\frac{\sqrt{-j\pi BT}}{2}\right)}{\sqrt{-j\frac{B}{T}}} = T e^{j2\pi\left(f_c t - \frac{Bt^2}{2T}\right)} \frac{\sin(\pi Bt)}{(\pi Bt)} \operatorname{erf}\left(\frac{\sqrt{-j\pi BT}}{2}\right) \quad (29)$$

Definindo e plotando:

$$F(BT) = \operatorname{erf}\left(\frac{\sqrt{-j\pi BT}}{2}\right) \quad (30)$$



Portanto, do gráfico em (A), a função  $F(BT) = \operatorname{erf}\left(\frac{\sqrt{-j\pi BT}}{2}\right)$  resulta em um número complexo com  $\operatorname{Re}\{F(BT)\} \cong 1$  e  $\operatorname{Im}\{F(BT)\} \cong 0$  de modo que  $F(BT)$  pode ser aproximada para o valor 1.0. Esta aproximação simplifica (29) para:

$$y_c(t) = T e^{j2\pi\left(f_c t - \frac{Bt^2}{2T}\right)} \frac{\sin(\pi Bt)}{(\pi Bt)} = T e^{j2\pi\left(f_c t - \frac{Bt^2}{2T}\right)} \operatorname{sinc}(\pi Bt), \quad \operatorname{sinc}(x) = \sin(x)/x \quad (31)$$

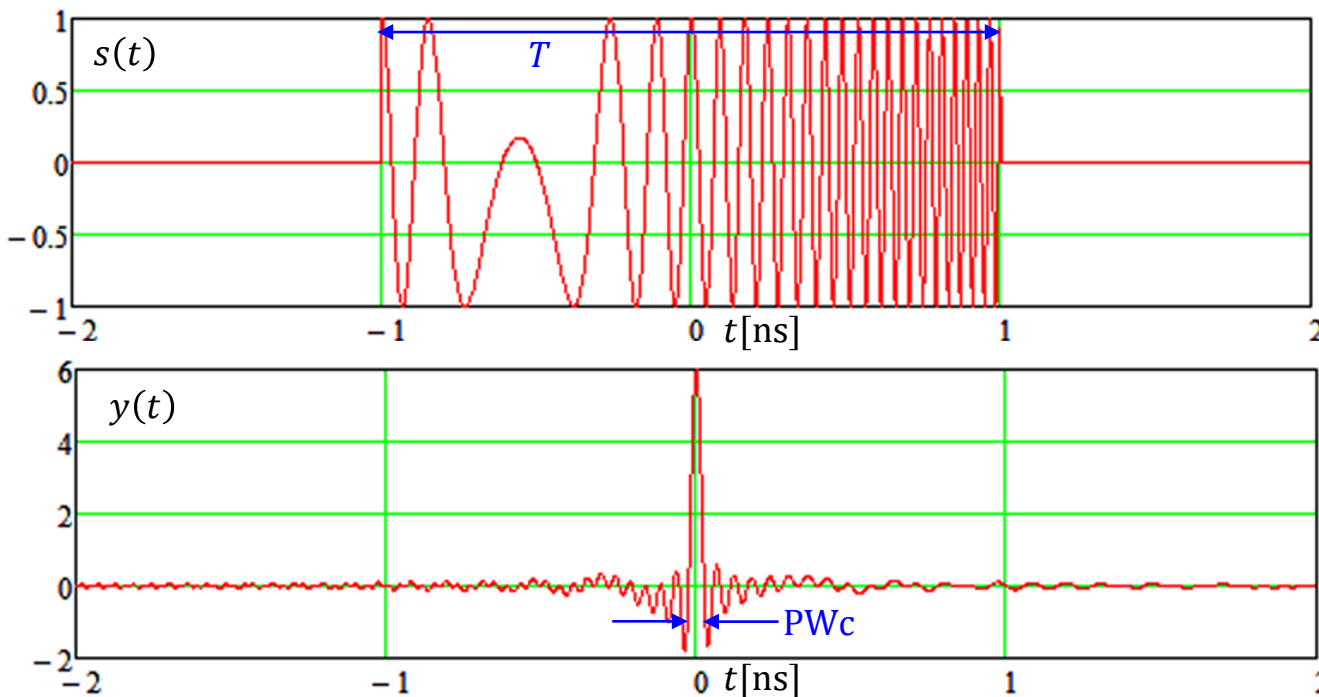
Para ajustar a amplitude de  $y_c(t)$  dentro de uma faixa de valores que não são excessivamente pequenos ou excessivamente grandes, vamos normalizar a amplitude de  $y_c(t)$  por um fator de escala  $\sqrt{BT}$ :

$$y_c(t) = \sqrt{BT} e^{j2\pi\left(f_c t - \frac{Bt^2}{2T}\right)} \operatorname{sinc}(\pi Bt) \quad (32)$$

## Sinais Chirp

**Exemplo 7:** Um sistema utiliza modulação PPM (*Pulse Position Modulation*) (ver [https://en.wikipedia.org/wiki/Pulse-position\\_modulation](https://en.wikipedia.org/wiki/Pulse-position_modulation)) em que, na sua forma mais simples, a posição no tempo do pulso transmitido determina a transmissão do bit "1" ou do bit "0" da sequência de bits a ser transmitida. Cada pulso transmitido pelo TX é um sinal *chirp*  $s(t) = \cos(2\pi f_0(t)t)$  modulado através de LFM (*Linear Frequency Modulation*), que varre a frequência  $f_0(t)$  do sinal  $s(t)$  no intervalo  $f_1 < f_0(t) < f_2$  durante o intervalo de tempo  $T = 2[\text{ns}]$ , sendo  $f_1 = 1.0 [\text{GHz}]$  e  $f_2 = 19 [\text{GHz}]$ . O RX detecta cada pulso *chirp* recebido através de um *matched-filter* cuja função de transferência é  $H(f) = e^{-j\pi \frac{(f-f_c)^2}{k}}$ , onde  $f_c = (f_1 + f_2)/2$  é a frequência central da banda  $B = f_2 - f_1$  de varredura linear da frequência instantânea do *chirp*  $s(t)$ . **Pede-se:** Plote o *chirp*  $s(t)$  transmitido pelo TX e a correspondente saída  $y(t)$  do *matched-filter* no RX no intervalo  $-T < t < T$ .

**Solução:** Do enunciado  $f_c = (f_1 + f_2)/2 = 10 [\text{GHz}]$   $B = f_2 - f_1 = 18[\text{GHz}]$  De (20):  $s(t) = \text{Re} \left\{ \text{Pulso} \left( \frac{t}{T} \right) e^{j2\pi \left( f_c t + \frac{B}{T} t^2 \right)} \right\}$   
 onde  $\text{Pulso}(x) = \begin{cases} 1.0, & |x| < 0.5 \\ 0.0, & x \geq 0.5 \end{cases}$ . De (32):  $y(t) = \text{Re}\{y_c(t)\} = \text{Re} \left\{ \sqrt{BT} e^{j2\pi \left( f_c t - \frac{Bt^2}{2T} \right)} \text{sinc}(\pi Bt) \right\}$



Note, portanto, que o pulso *chirp*  $s(t)$  transmitido pelo TX com uma duração  $T = 2[\text{ns}]$ , é convertido em um pulso  $y(t)$  estreito de largura  $PW_c = 0.05 [\text{ns}]$  na saída do *matched-filter* do RX, resultando em um **fator de compressão de pulso** dado por  $\rho = T/PW_c = 40$ .

Esta técnica de compressão de pulso através de um *matched-filter* pode ser usada para não somente aumentar a precisão do *range resolution* de um radar pulsado como também para reduzir o seu *minimum range*, conforme discutido no slide 22 (na solução do item (c) do Exemplo 1 do slide 20) e conforme discussão no próximo slide.

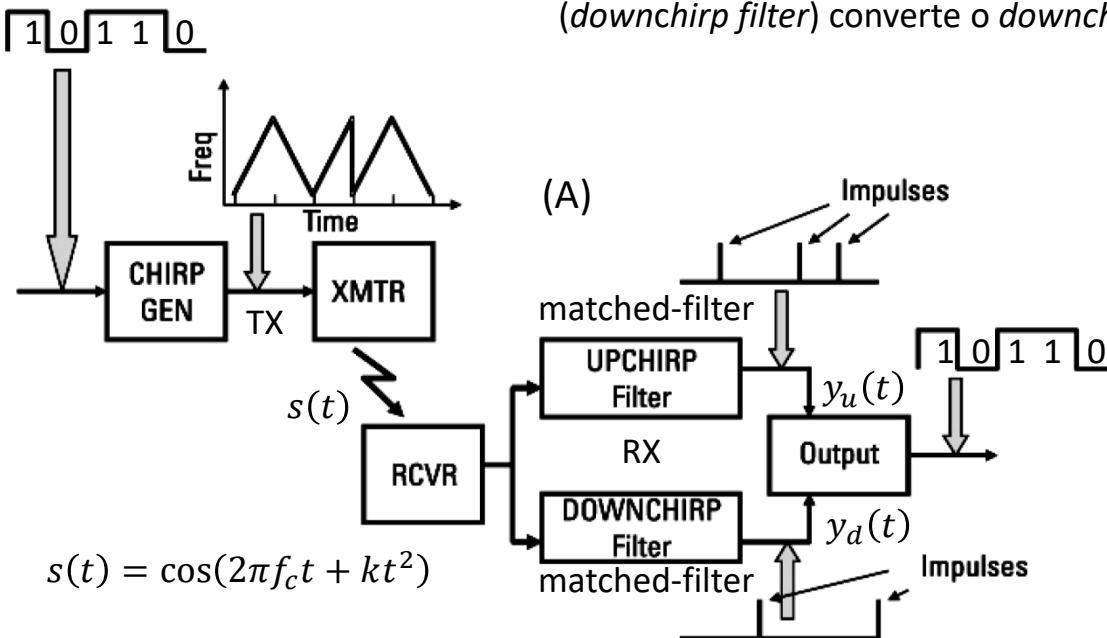


## Sinais Chirp

A geração de sinais LPI com a posição do pulso *chirp* determinando o valor do bit transmitido (PPM - *Pulse Position Modulation*), conforme Exemplo 7 no slide 70, é susceptível a erros devido à interferência intersimbólica (ISI – *Intersymbol Interference* – ver [https://en.wikipedia.org/wiki/Intersymbol\\_interference](https://en.wikipedia.org/wiki/Intersymbol_interference)) causada pelos efeitos de multipercurso no canal de transmissão entre TX e RX ([https://en.wikipedia.org/wiki/Multipath\\_propagation](https://en.wikipedia.org/wiki/Multipath_propagation)). Os múltiplos pulsos refletidos em múltiplos pontos de reflexão da onda EM no canal de transmissão (estruturas metálicas de edifícios, por exemplo) são recebidos com atrasos distintos e se superpõe aos pulsos transportados pela onda EM que se propaga no caminho direto, gerando ISI e degradando a inteligibilidade do sinal. Para efeito de contornar a suscetibilidade ao multipercurso da modulação PPM, uma técnica alternativa para efetuar o mapeamento “bit transmitido” → “pulso *chirp*” consiste em adotar dois *chirps*  $s(t) = \cos(2\pi f_c t + kt^2)$ , com a constante  $k \left[ \frac{\text{Hz}}{\text{s}} \right]$  que define a declividade da rampa de frequência sendo dada em função do valor do bit a ser transmitido, conforme (33) abaixo:

$$k = \begin{cases} -\frac{B}{T}, & \text{p/ bit "0"} \\ \frac{B}{T}, & \text{p/ bit "1"} \end{cases} \quad (33)$$

Conforme mostrado em (A), para representar o bit “1” um *chirp* é transmitido com frequência crescente e o correspondente *matched-filter* (*upchirp filter*) converte o *upchirp* em um impulso em sua saída. Para representar o bit “0” um *chirp* é transmitido com frequência decrescente e o correspondente *matched-filter* (*downchirp filter*) converte o *downchirp* em um impulso em sua saída.



Note em (A) que o *bit stream* de entrada é 10110. Assim, a saída  $y_u(t)$  do *upchirp filter* resulta em impulsos para o primeiro, terceiro e quarto bits, enquanto a saída  $y_d(t)$  do *downchirp filter* resulta em impulsos para o segundo e quinto bits. Os impulsos nas saídas  $y_u(t)$  e  $y_d(t)$  são digitalizados por respectivos conversores A/D no bloco “Output” e são convertidos em bits na lógica combinacional do bloco. Em não havendo excessivo multipercurso e/ou ruído aditivo no canal, a saída do bloco “Output” reproduz o *bit stream* original na entrada do TX.

**Exemplo 9:** O TX de um sistema de comunicação LPI transmite dois *chirps*  $s(t) = \cos(2\pi f_c t + kt^2)$ , um para cada valor de bit a ser transmitido, com a constante  $k \left[ \frac{\text{Hz}}{\text{s}} \right]$  definida em função do valor do bit:  $k = -B/T$  p/ o bit “0” e  $k = B/T$  p/ o bit “1”. Cada *chirp* é modulado através de LFM (*Linear Frequency Modulation*), que varre a frequência instantânea do sinal  $s(t)$  na banda  $B = f_2 - f_1$  no intervalo de tempo  $T = 20[\text{ns}]$ , sendo  $f_1 = 100 [\text{MHz}]$  e  $f_2 = 1.9 [\text{GHz}]$ . O RX detecta cada pulso *chirp* recebido (*upchirp* ↔ bit “1” e *downchirp* ↔ bit “0”) através de dois *matched-filters* cujas respectivas funções de transferência são dadas por  $H(f) = e^{-j\pi \frac{(f-f_c)^2}{k}}$ , onde  $k$  é definido em função do valor do bit conforme acima e  $f_c = (f_1 + f_2)/2$  é a frequência central da banda  $B$ . **Pede-se para o intervalo  $-T < t < T$ :** **(a)** Plote o *upchirp*  $s(t)$  transmitido pelo TX e a correspondente saída  $y_u(t)$  do *upchirp matched-filter* no RX em (A) no slide anterior. **(b)** Plote o *downchirp*  $s(t)$  transmitido pelo TX e a correspondente saída  $y_d(t)$  do *downchirp matched-filter* no RX em (A) no slide anterior. **(c)** Plote o *upchirp*  $s(t)$  transmitido pelo TX e a correspondente saída  $y_d(t)$  do *downchirp matched-filter* no RX em (A) no slide anterior.

**Solução:** Ver próximo slide.

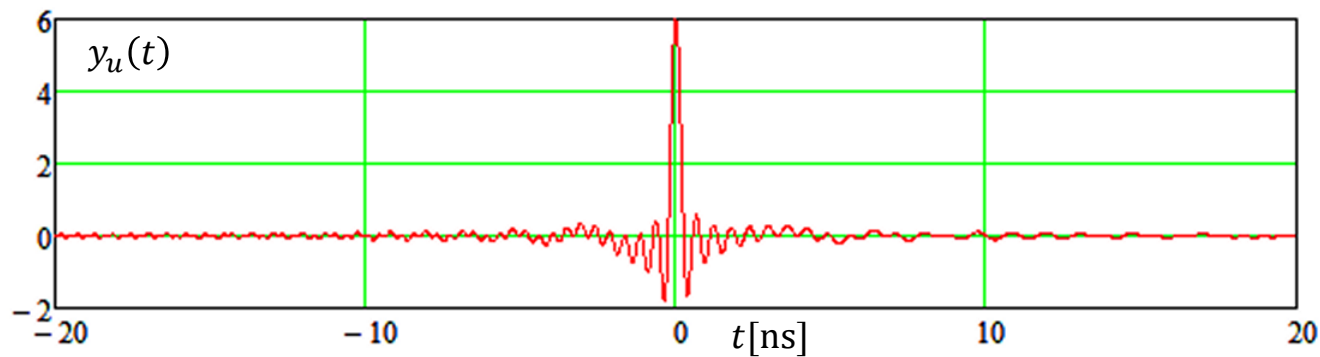
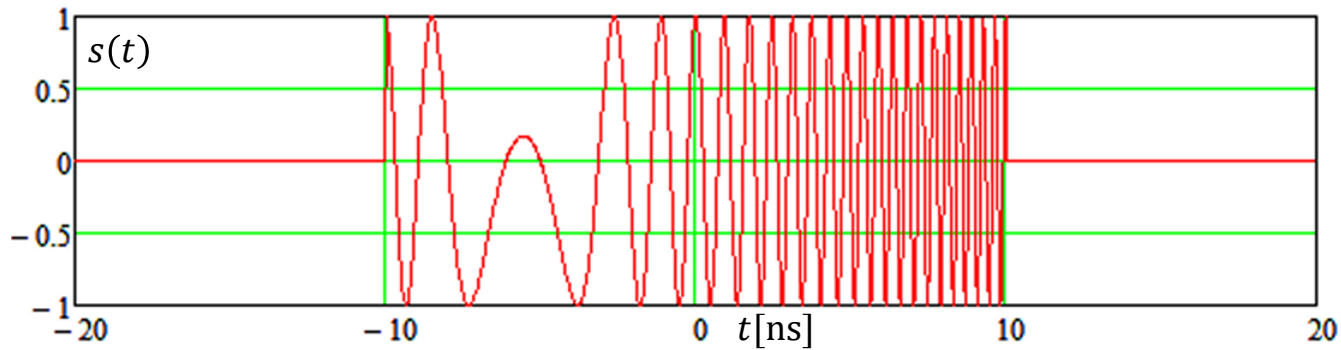


## Sinais Chirp

(a) Do enunciado  $f_c = (f_1 + f_2)/2 = 1$  [GHz]  $B = f_2 - f_1 = 1.8$ [GHz]

$$\text{De (20): } s(t) = \text{Re} \left\{ \text{Pulso} \left( \frac{t}{T} \right) e^{j2\pi \left( f_c t + \frac{B}{T} t^2 \right)} \right\} \text{ onde } \text{Pulso}(x) = \begin{cases} 1.0, & |x| < 0.5 \\ 0.0, & x \geq 0.5 \end{cases} .$$

$$\text{De (32): } y_u(t) = \text{Re} \left\{ \sqrt{BT} e^{j2\pi \left( f_c t - \frac{Bt^2}{2T} \right)} \text{sinc}(\pi Bt) \right\}$$

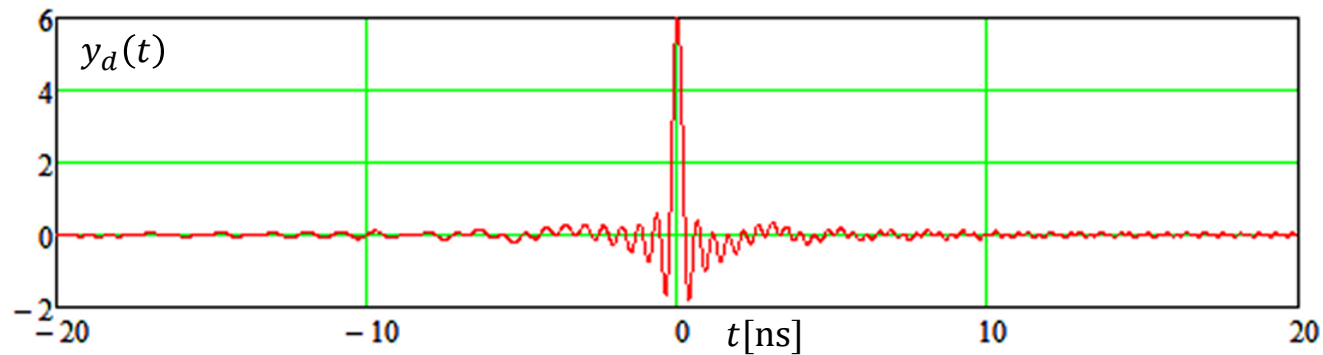
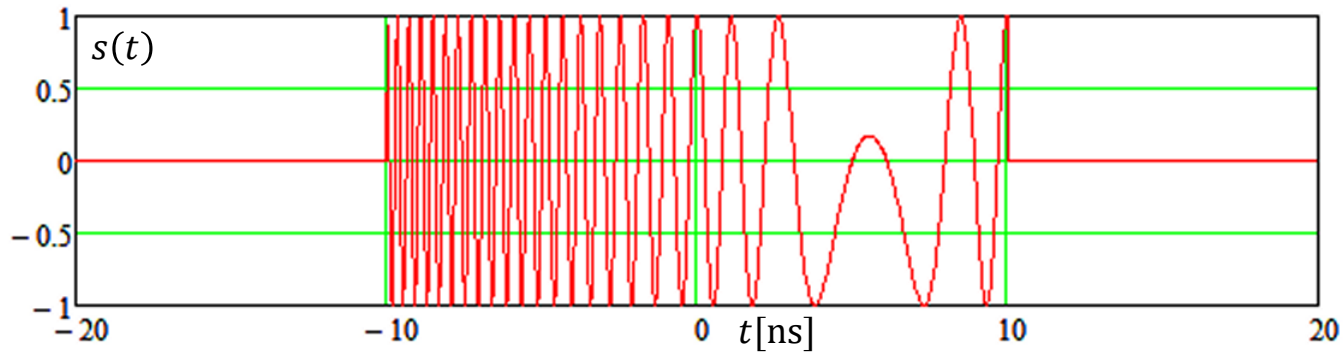


## Sinais Chirp

(b) De (20) e (32), trocando o sinal de  $B/T$  no argumento da exponencial (lembre que  $downchirp \leftrightarrow \text{bit "0"} \leftrightarrow k = -B/T$ ):

$$s(t) = \text{Re} \left\{ \text{Pulso} \left( \frac{t}{T} \right) e^{j2\pi \left( f_c t + \frac{-B}{T} t^2 \right)} \right\} \text{ onde } \text{Pulso}(x) = \begin{cases} 1.0, & |x| < 0.5 \\ 0.0, & x \geq 0.5 \end{cases} .$$

$$y_d(t) = \text{Re} \left\{ \sqrt{BT} e^{j2\pi \left( f_c t - \frac{Bt^2}{2T} \right)} \text{sinc}(\pi Bt) \right\}$$

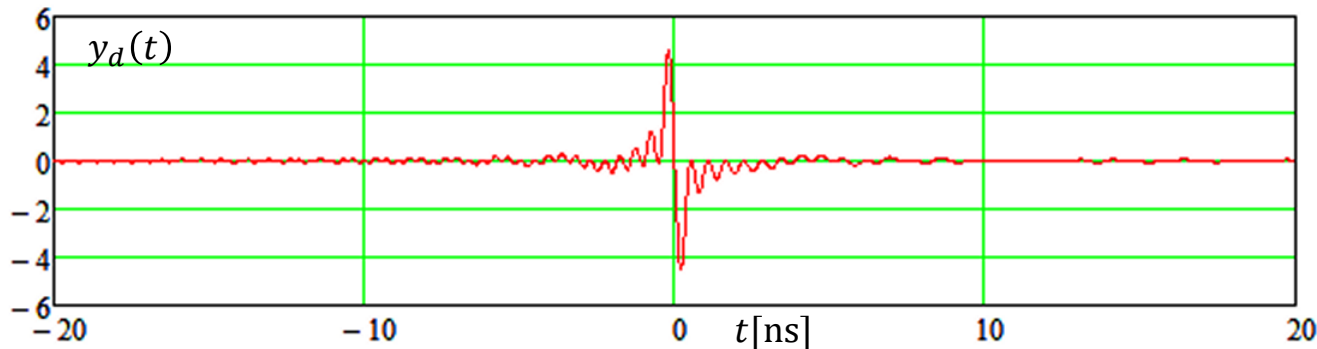
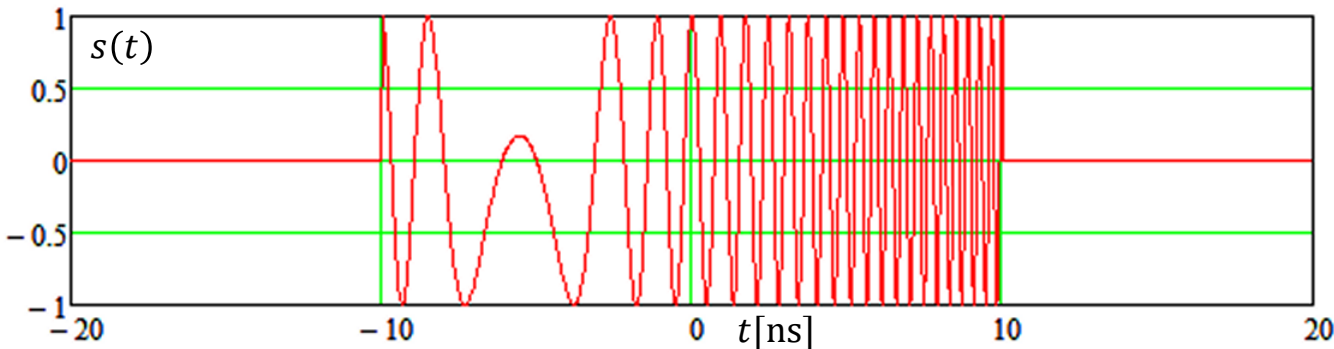


## Sinais Chirp

(c) De (20):  $s(t) = \text{Re} \left\{ \text{Pulso} \left( \frac{t}{T} \right) e^{j2\pi \left( f_c t + \frac{B}{T} t^2 \right)} \right\}$  onde  $\text{Pulso}(x) = \begin{cases} 1.0, & |x| < 0.5 \\ 0.0, & x \geq 0.5 \end{cases}$ .

Repetindo para  $k < 0$  ( $k < 0$  caracteriza um *downchirp matched-filter*) o desenvolvimento das equações (21) a (32) para a resposta ao impulso  $h(t)$  do *matched-filter* e para a saída  $y_c(t) = s_c(t) * h(t)$  do *matched-filter*, obtemos:

$$y_d(t) = \text{Re} \left\{ j\sqrt{BT} e^{j2\pi \left( f_c t - \frac{Bt^2}{2T} \right)} \text{sinc}(\pi Bt) \right\}$$



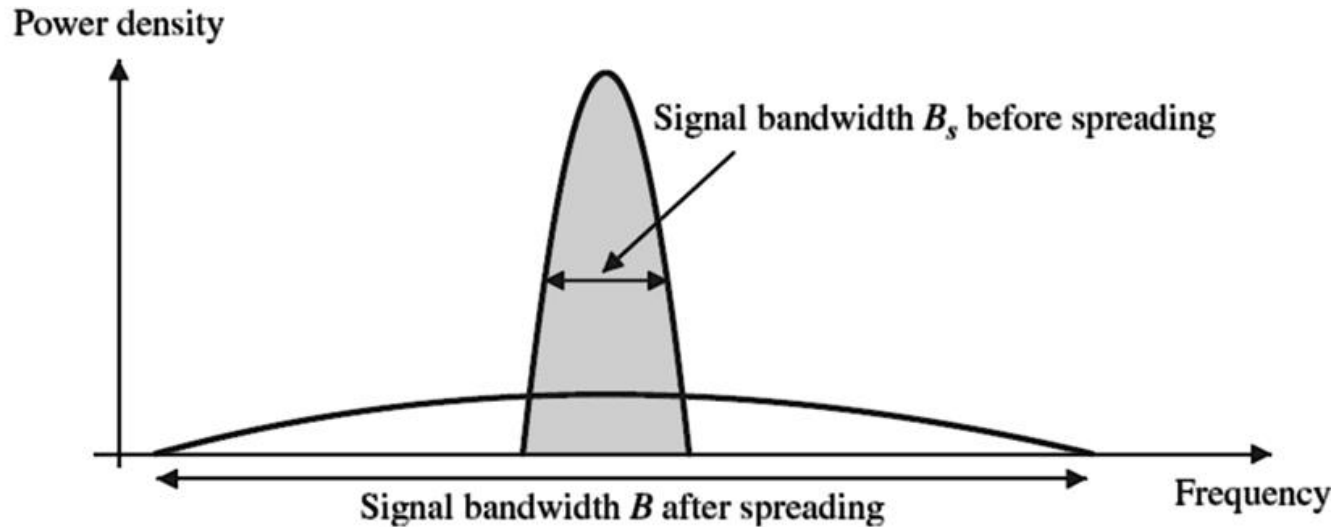
Note em (A) no slide 72 que os impulsos na saída  $y_u(t)$  do *upchirp filter* e na saída  $y_d(t)$  do *downchirp filter* são digitalizados por respectivos conversores A/D no bloco “Output” e são convertidos em bits na logica combinacional do bloco.

Ocorre que os conversores A/D amostram  $y_u(t)$  e  $y_d(t)$  em  $t = 0$ . Portanto, em  $t = 0$  a saída do A/D resulta em uma amostra de valor máximo para a situação em que o *chirp* é casado com o *matched-filter*, conforme valor  $y_u(t = 0) = 6$  obtido em (a) no slide 74 e  $y_d(t = 0) = 6$  obtido em (b) no slide 75. Em particular, note que a saída do A/D é uma amostra de valor zero em  $t = 0$  quando o *chirp* não é casado com o *matched-filter*, conforme valor  $y_d(t = 0) = 0$  no gráfico acima.

## Sinais *Direct Sequence Spread Spectrum* (DS-SS)

O princípio fundamental das técnicas de *Spread Spectrum* (SS) é transmitir informação através de sinais cuja largura da banda espectral do sinal transmitido no canal é muito maior do que a largura do sinal em banda-base que contém a informação a ser transmitida. Se a largura do espectro do sinal transmitido for muito grande, o espectro do sinal se assemelha ao espectro do ruído branco, que é descorrelacionado com qualquer função do domínio tempo exceto consigo mesmo. Sendo assim, um sistema SS se torna basicamente imune à interferência do sinal sobre instâncias dele mesmo que chegam atrasadas na antena do RX originadas por multipercurso no canal. O sinal é transmitido com uma largura de espectro  $B$  muito maior que a largura do espectro  $B_s$  do sinal em banda-base.

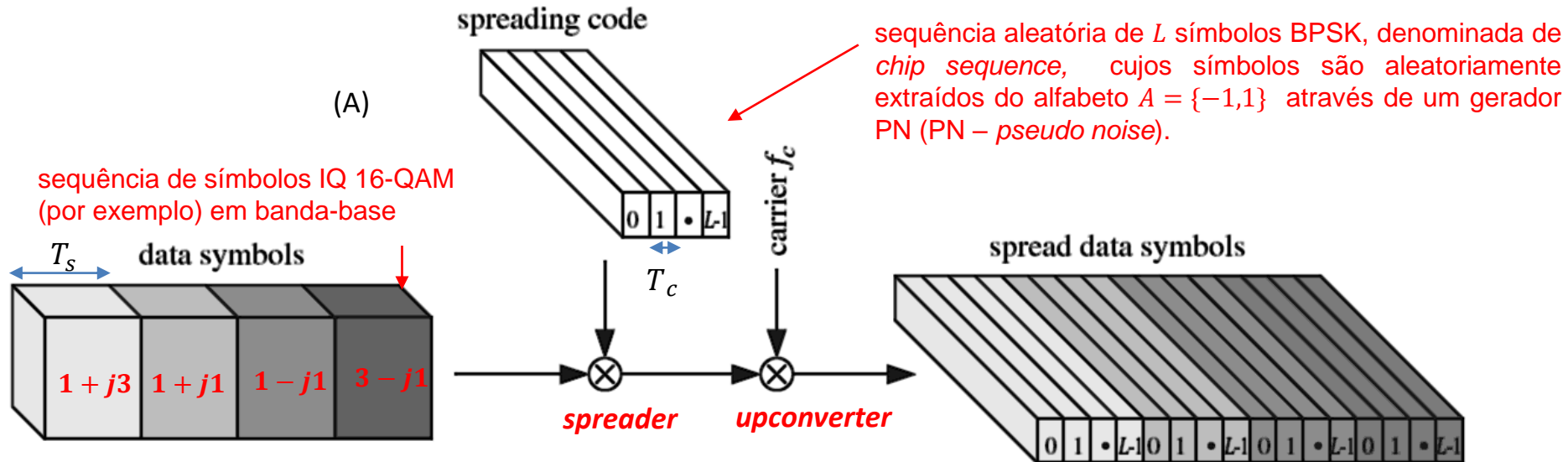
O **ganho de processamento** (*processing gain*) é definido por  $PG = B/B_s$ . Quanto maior for  $PG$ , menor a densidade de potência necessária para transmitir a informação e mais o sinal transmitido se assemelha a ruído branco. É usual valores de  $PG$  de algumas dezenas à várias centenas.



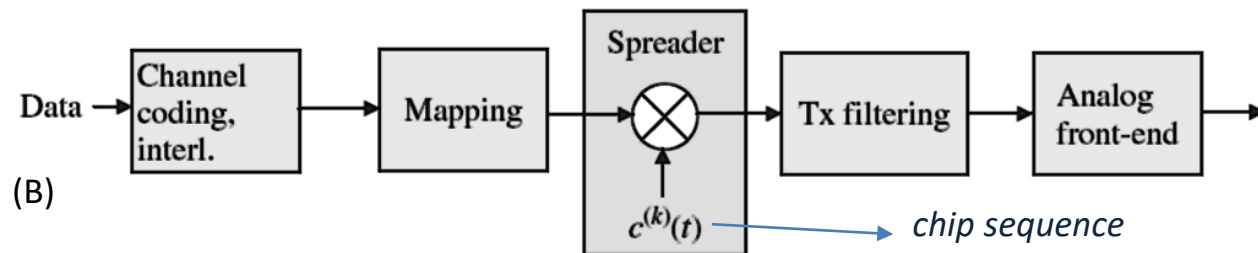
Power spectral density after direct sequence spreading

## Sinais Direct Sequence Spread Spectrum (DS-SS)

Dado o ganho de processamento  $PG$  de um sistema DS-SS, o processo de “espalhar” a largura do espectro  $B_s$  do sinal em banda-base ao longo de uma largura de espectro  $B = PG \cdot B_s$  muito maior que  $B_s$ , é denominado de **spreading**, e o bloco que executa a operação de **spreading** é denominado **spreader**, conforme mostrado em (A):



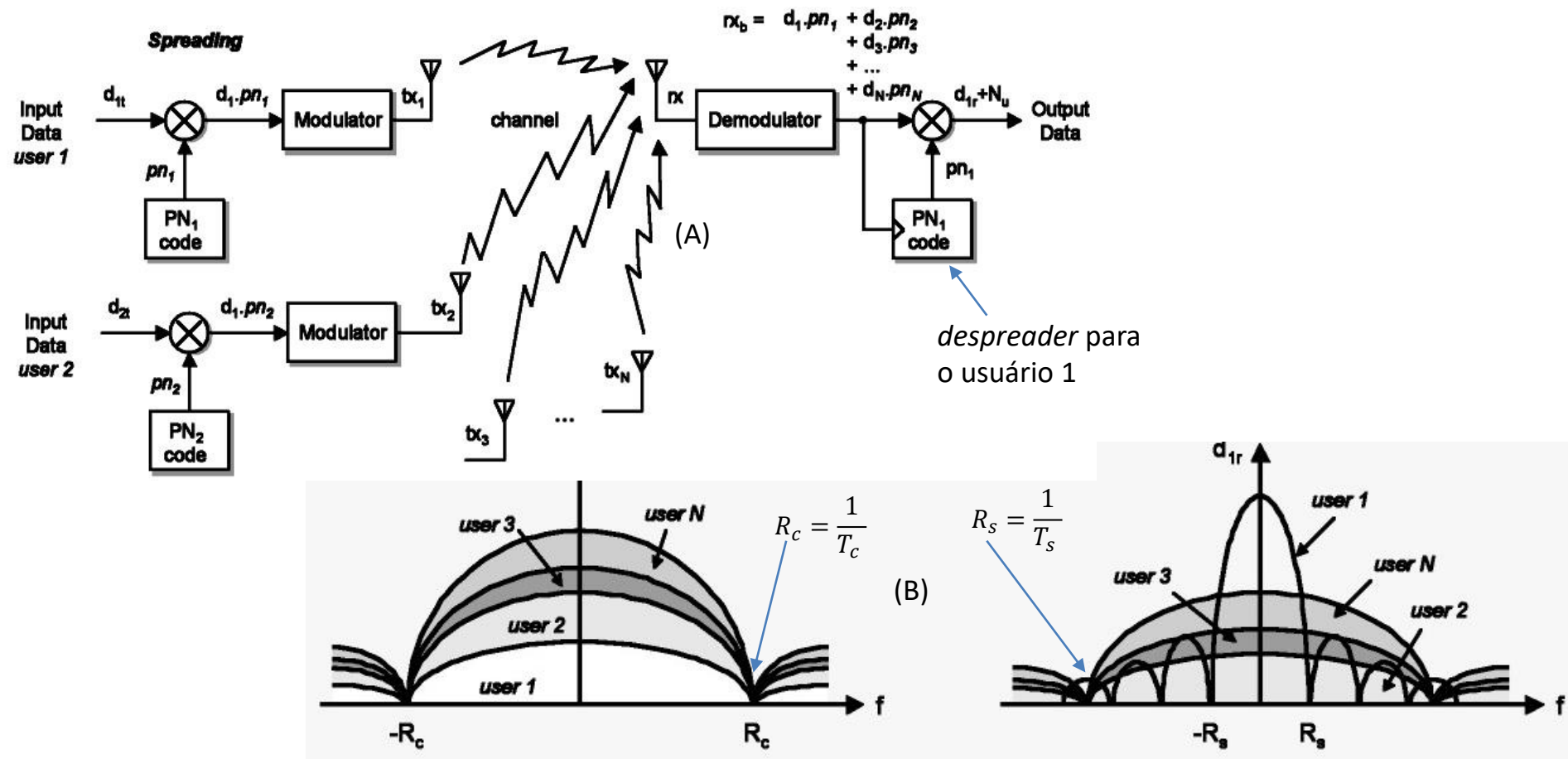
Para o *spreading* da sequência de símbolos IQ de duração  $T_s$  em banda-base, são utilizados códigos PN. Um código PN (PN – pseudo noise) implementa um sinal aleatório com espectro similar ao espectro do ruído branco. O espectro de uma sequência PN é semelhante ao de uma sequência aleatória de bits, mas é gerado de forma determinística. Ver [https://en.wikipedia.org/wiki/Pseudorandom\\_noise](https://en.wikipedia.org/wiki/Pseudorandom_noise). No âmbito da geração de sinais DS-SS, os códigos PN devem idealmente apresentar função de autocorrelação impulsiva e com função de correlação cruzada entre códigos a mais decorrelacionada possível, para evitar que o sinal de um usuário interfira nos demais usuários (o que separa os sinais de cada usuário é o código PN que espalha o espectro do sinal em banda-base de cada um deles). Um código PN gera uma sequência de símbolos BPSK, cada símbolo BPSK (denominado de *chip*) tendo uma duração  $T_c = T_s/PG$ , conforme mostrado em (A) acima. Em (B) abaixo é mostrado a localização do *spreader* no encadeamento de blocos de um TX DS-SS





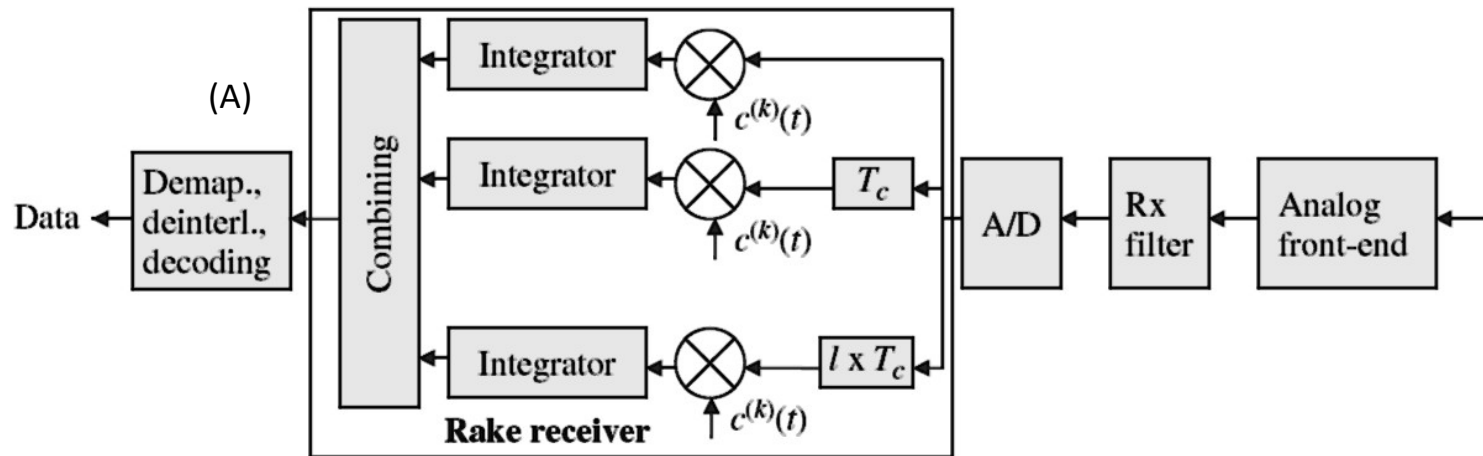
## Sinais Direct Sequence Spread Spectrum (DS-SS)

Para recuperar o sinal do usuário 1 recebido no RX juntamente com o sinal dos demais usuários, como exemplificado em (A) abaixo, o mesmo código PN<sub>1</sub> com o qual o sinal em banda-base do usuário 1 foi espalhado no TX, é aplicado a um correlador no RX e é correlacionado com o conjunto de sinais recebidos de todos os usuários. Este correlador, denominado de *despreader*, efetua o *despreading* do sinal do usuário 1, trazendo seu espectro de volta para banda-base, conforme mostrado em (B). O RX mantém em uma *lookup table* do seu hardware uma cópia dos códigos de cada usuário, p/ efeito de poder efetuar o *despreading*. Quanto mais longo for o código PN, mais semelhante a ruído branco o sinal se torna e mais imune a multipercurso o sistema se torna, no entanto mais crítica fica a sincronização de *clock* entre TX e RX.



## Sinais Direct Sequence Spread Spectrum (DS-SS)

Em (A) abaixo é mostrado o diagrama de blocos simplificado de um RX DS-SS. O sinal recebido é primeiramente amplificado no *front-end* e filtrado para contenção espectral de sinais fora da banda do canal e depois digitalizado no A/D cuja frequência de amostragem é  $\frac{1}{T_c}$ , sendo  $T_c$  a duração de um pulso BPSK do *chip sequence*. A seguir, um **rake receiver** realinha no tempo as instâncias da sequência originalmente transmitida que incidem na antena do RX defasadas entre si no tempo em consequência do multipercurso no canal. Note que as instâncias da sequência original recebidas não geram ISI, visto que são descorrelacionadas entre si porque são sinais *spread spectrum*. O *rake receiver* realinha no tempo as instâncias recebidas unicamente para somar construtivamente entre si as referidas instâncias, e assim aumentar o nível do sinal recebido.

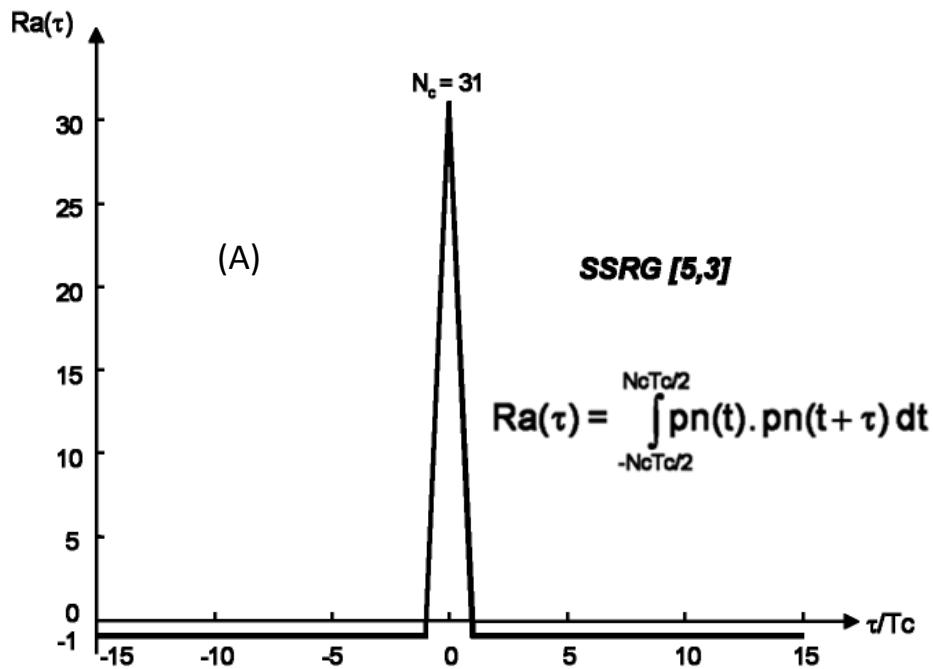


Cada braço do *rake receiver* (normalmente, são utilizados 3 ou 4 braços na prática) é um *despreader* (um correlator – multiplicador seguido de um integrador) que ajusta o atraso  $\ell \times T_c$  variando adaptativamente o respectivo índice  $\ell$  de modo aos sinais resultantes de todos os *despreaders* se somarem construtivamente no bloco “Combining”, maximizando a potência do sinal recebido. Note que o *despreader* de cada braço do *rake receiver* especificamente efetua o seguinte processo: cada sinal recebido de cada percurso no canal é atrasado de  $\ell \times T_c$  e correlacionado no correlator do *despreader* com a sequência PN  $c^{(k)}$  atribuída ao  $k$ -ésimo usuário. Após a correlação efetuada em cada *despreader*, as sequências são combinadas construtivamente e, finalmente, enviada ao *de-mapper* e aos códigos corretores de erro do decodificador de canal.

## Sinais Direct Sequence Spread Spectrum (DS-SS)

Um gerador de sequência PN para o processo de *spreading* do sinal *spread-spectrum* deve gerar uma sequência PN que possua as seguintes propriedades:

(I) A função de auto-correlação  $R_a(\tau)$  da sequência PN  $p_n(t)$  deve aproximar o formato impulsivo da função de correlação do ruído branco Gaussiano conforme mostrado em (A) abaixo.

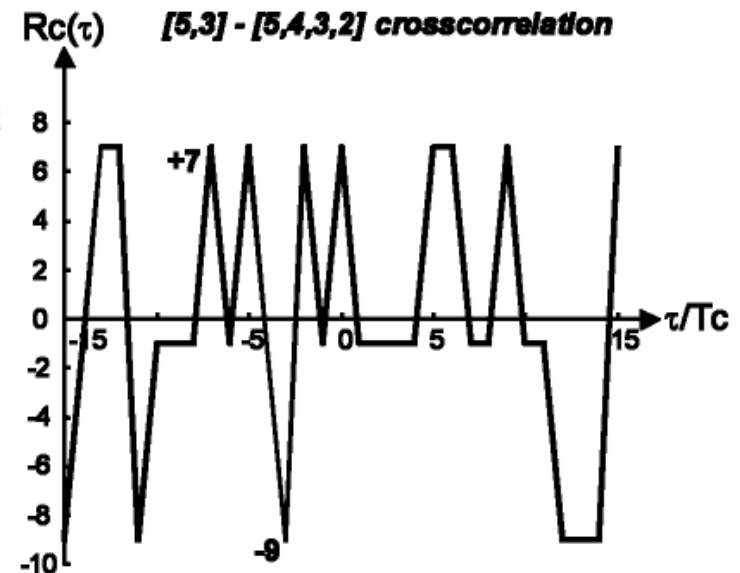
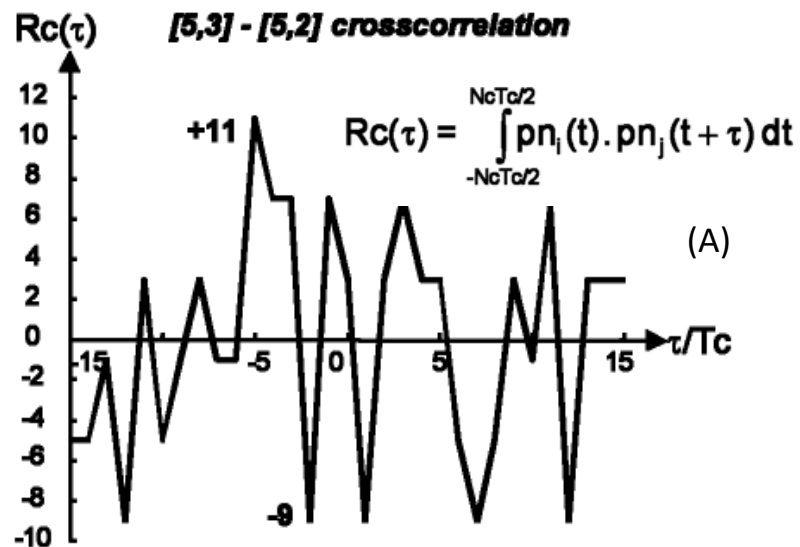


A razão para a exigência de que função de auto-correlação  $R_a(\tau)$  da sequência PN seja impulsiva, conforme mostrado em (A), é que quanto mais  $R_a(\tau)$  se assemelhar a um impulso mais o sinal DS-SS que se propaga no canal de transmissão se torna descorrelacionado com qualquer sinal do domínio tempo exceto consigo mesmo. Sendo assim, o sinal DS-SS é basicamente imune à interferência do sinal sobre instâncias dele mesmo que chegam atrasadas (ecos) na antena do RX originadas por multipercurso no canal. Mais importante ainda, quanto mais a função de auto-correlação  $R_a(\tau)$  se assemelhar a um impulso, mais imune se torna o sinal DS-SS à interferência (*jamming*) de qualquer outro sinal que não seja ele mesmo. **Note que quanto mais  $R_a(\tau)$  se assemelha a um impulso, maior será a largura  $B$  do espectro do sinal DS-SS e em consequência maior será o ganho de processamento  $PG = B/B_s$ .**

Portanto, quanto maior for o ganho de processamento  $PG$  do sinal DS-SS menor capacidade terá um sistema EW inimigo para efetuar *jamming* sobre o sinal DS-SS desejado recebido no RX, porque quanto maior for  $PG$  mais o sinal DS-SS se torna descorrelacionado com qualquer sinal do domínio tempo que não seja ele mesmo. A capacidade de um *jammer* é medida pelo  $J/S$  (*jamming-to-signal ratio*).  $J/S$  é a razão entre a potência do sinal do *jammer* medida na antena do RX que está sofrendo *jamming* e a potência do sinal desejado recebido medido na mesma antena. Dado um RX DS-SS, para cada tipo de sinal de *jamming* há um limiar de  $J/S$  a partir do qual o RX DS-SS fica impossibilitado de demodular o sinal DS-SS recebido desejado, em consequência do sinal indesejado de *jamming*. O aumento do ganho de processamento  $PG$  do sinal DS-SS aumenta proporcionalmente o limiar de  $J/S$  a partir do qual o RX DS-SS não consegue demodular o sinal, reduzindo a sensibilidade do RX DS-SS ao *jamming*.

## Sinais Direct Sequence Spread Spectrum (DS-SS)

(II) A função de correlação cruzada  $R_c(\tau)$  entre duas seqüências PN  $pn_i(t)$  e  $pn_j(t)$  deve idealmente resultar uma curva de valor próximo a zero ao longo do domínio  $\tau$ . A correlação cruzada é uma medida de similaridade no tempo entre dois códigos PN diferentes, cada um dos códigos usado para o *spreading* do sinal de dois usuários distintos. Quando a correlação cruzada  $R_c(\tau)$  é zero para todos os  $\tau$ , os códigos são chamados ortogonais. Na versão multiusuário do sistema DS-SS, o sistema DS-CDMA, (CDMA – *Code Division Multiple Access*), vários usuários ocupam a mesma largura de banda de RF e transmitem simultaneamente na mesma frequência e no mesmo local. Quando os códigos do usuário são ortogonais, não há interferência entre os usuários após o *despreading* no *rake receiver*, e a individualidade da comunicação de cada usuário é protegida. Na prática, os códigos não são perfeitamente ortogonais em consequência de a correlação cruzada entre códigos de usuário não ser zero, conforme mostrado em (A), introduzindo degradação no desempenho do sistema. Devido à ortogonalidade imperfeita entre os códigos de cada usuário, o sinal de um usuário é visto pelos demais usuários como um ruído interferente agregado ao sinal de interesse na saída do *despreader* do RX. Como a potência do ruído é aditiva, este efeito, denominado MAI (*multiple access interference*), acaba limitando o número máximo de usuários simultâneos. Quando um grande número de usuários, usando códigos diferentes, compartilha uma faixa de frequência comum (ambiente multiusuário), as seqüências PN atribuídas ao código de cada usuário devem ser cuidadosamente escolhidas para evitar interferência entre os mesmos.



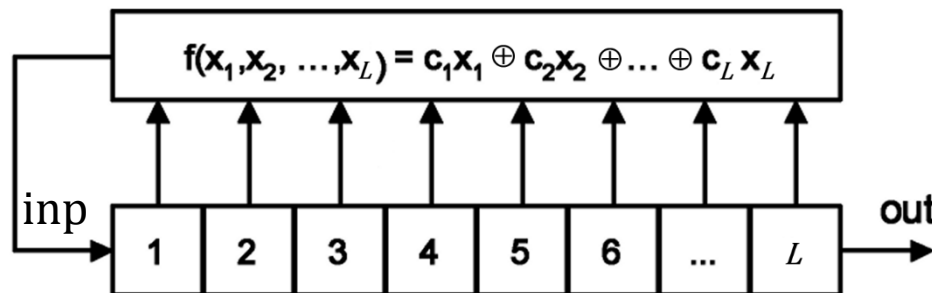
## Sinais Direct Sequence Spread Spectrum (DS-SS)

(III) **Nível DC do chip sequence:** A sequência dos  $L$  pulsos BPSK aleatoriamente extraídos do alfabeto  $A = \{-1, 1\}$  e que constituem o *chip sequence* (ver slide 78), deve apresentar uma componente DC residual cujo valor absoluto deve ser no máximo 1. Por exemplo, uma sequência com  $L = 7$  que atende a este critério é a sequência PN abaixo:

$$pn = [+1 +1 +1 -1 +1 -1 -1] \rightarrow \Sigma = +1$$

Note no slide 78 que o *upconverter* é o bloco seguinte ao *spreader* no fluxo de sinal. Se o nível DC residual do *chip sequence* não for zero, ou no máximo de valor absoluto 1, o espectro na saída do *upconverter* conterá uma portadora de frequência  $f_c$  e de amplitude proporcional ao nível DC residual do *chip sequence*. Esta portadora não transporta informação (é modulada por um nível DC) e consome inutilmente potência do HPA (*High Power Amplifier*) de RF (*Radio Frequency*) no *front-end* analógico na saída do TX. Esta é a razão da limitação do nível DC máximo do *chip sequence*.

Um código PN implementa um sinal aleatório com espectro similar ao espectro do ruído branco, mas é gerado de forma determinística. Um gerador PN que atende as propriedades (I), (II) e (III) é o gerador baseado em um arranjo particular de *shift-registers* (registradores de deslocamento - ver [http://www.fccdecastro.com.br/pdf/ED\\_C8.pdf](http://www.fccdecastro.com.br/pdf/ED_C8.pdf)), e é denominado de SSRG (*simple shift register generator*), conforme mostra a figura abaixo.



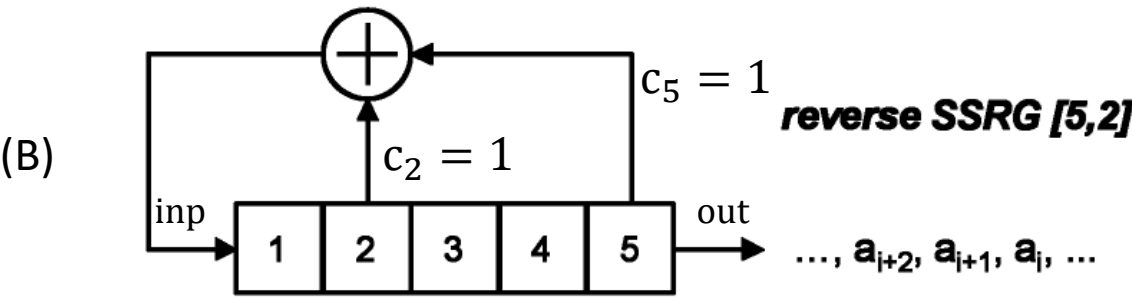
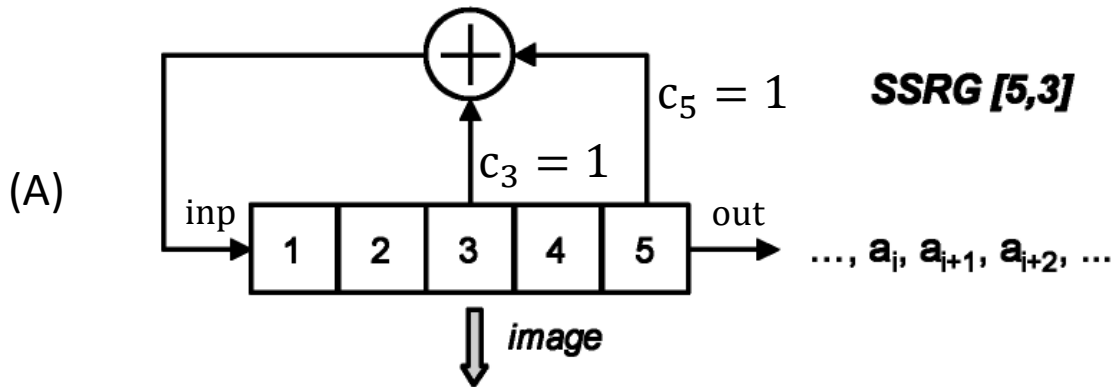
A sequência de bits na saída **out** é convertida na sequência de símbolos BPSK do *chip sequence* (e vice-versa) através da relação:

$$\text{BPSK}_i = \begin{cases} 1 & , \text{out}_i = 1 \\ -1 & , \text{out}_i = 0 \end{cases}$$

Um SSRG é uma fila FIFO de  $L$  *flip-flops* tipo D em que a saída Q de cada  $n$ -ésimo *flip-flop*,  $n = 1, 2, \dots, L$ , é atribuída à variável  $x_n$  respectiva. O conjunto de variáveis  $x_n$  é realimentado à entrada *inp* da FIFO através da lógica combinacional  $\text{inp} = c_1x_1 \oplus c_2x_2 \oplus \dots \oplus c_Lx_L$ , onde  $\oplus$  representa a operação XOR (exclusive – OR) e onde o valor lógico de  $c_n$  determina se a variável  $x_n$  é realimentada ou não à entrada *inp* ( $c_n = 0 \rightarrow$  desabilita realimentação de  $x_n$ ,  $c_n = 1 \rightarrow$  habilita realimentação de  $x_n$ ). O SSRG na figura acima é linear porque a função  $f(x_1, x_2, \dots, x_L) = c_1x_1 \oplus c_2x_2 \oplus \dots \oplus c_Lx_L$  que controla a realimentação é expressa como um soma módulo-2 (XOR).

## Sinais Direct Sequence Spread Spectrum (DS-SS)

A realimentação através da da função  $f(x_1, x_2 \dots, x_L) = c_1x_1 \oplus c_2x_2 \oplus \dots \oplus c_Lx_L$  faz com que um SSRG com  $L$  flip-flops produza uma sequência aleatória de bits em sua saída **out** com período  $N_c$ . A periodicidade  $N_c$  expressa o número de bits gerados na sequência resultante na saída **out** até a sequência começar a repetir a si mesma. O período  $N_c$  depende de  $L$ , depende da definição da função  $f(x_1, x_2 \dots, x_L) = c_1x_1 \oplus c_2x_2 \oplus \dots \oplus c_Lx_L$  e depende da inicialização (0 ou 1) de cada um dos  $L$  flip-flops do SSRG. **Quando o período  $N_c$  é o máximo que um SSRG pode gerar, i.e., quando  $N_c = 2^L - 1$ , a sequência PN é denominada *maximum length sequence* ou simplesmente *m-sequence*.** Uma *m-sequence* gerada a partir de um SSRG possui um número par de coeficientes  $c_n = 1$  em  $f(x_1, x_2 \dots, x_L) = c_1x_1 \oplus c_2x_2 \oplus \dots \oplus c_Lx_L$ , e os valores de  $n$  para os quais  $c_n = 1$  são dados na tabela no próximo slide. Esta tabela é obtida testando experimentalmente em um computador todas as possíveis combinações de  $c_n$  em  $f(x_1, x_2 \dots, x_L) = c_1x_1 \oplus c_2x_2 \oplus \dots \oplus c_Lx_L$  para que a condição  $N_c = 2^L - 1$  seja atingida. Note que  $c_L = 1$  em todos os casos da tabela, i.e. a saída do último flip-flop sempre é realimentada à entrada inp da SSRG.



Em (A) é mostrado um exemplo de SSRG com  $L = 5$  obtido da tabela no próximo slide.

Se um SSRG de  $L$  estágios ( $L$  *flip-flops*) tiver realimentação nos estágios  $L$ ,  $k$  e  $m$  e gerar na saída **out** a sequência  $\dots, a_i, a_{i+1}, a_{i+2}, \dots$  um SSRG com realimentação nos estágios  $L$ ,  $L - k$  e  $L - m$  gerará a sequência reversa  $\dots, a_{i+2}, a_{i+1}, a_i, \dots$ , conforme mostrado em (B).

A utilidade da sequência reversa é substituir o correlador no *despreader* do RX por um *matched-filter* cujos coeficientes são dados pelos bits da sequência reversa.

[5,2] = -1 -1 -1 -1 1 -1 1 -1 1 1 1 -1 1 1 -1 -1 1 1 -1 1 -1 -1 1

[5,3] = -1 -1 -1 -1 1 -1 -1 1 -1 1 1 1 1 1 -1 -1 1 1 -1 1 1 -1 1



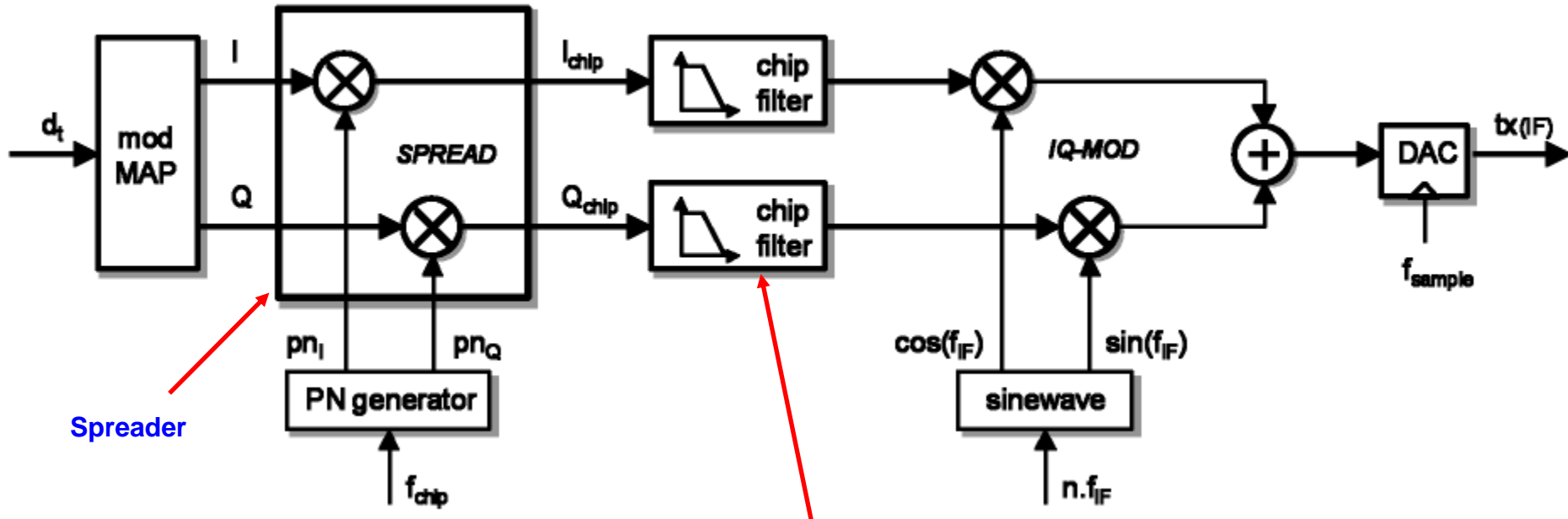
## Sinais *Direct Sequence Spread Spectrum* (DS-SS)

In the following table the feedback connections (even number) are tabulated for m-sequences generated with a linear SSRG (without image set).

L	$N_c=2^L-1$	Feedback Taps for m-sequences	# m-sequences
2	3	[2,1]	2
3	7	[3,1]	2
4	15	[4,1]	2
5	31	[5,3] [5,4,3,2] [5,4,2,1]	6
6	63	[6,1] [6,5,2,1] [6,5,3,2]	6
7	127	[7,1] [7,3] [7,3,2,1] [7,4,3,2] [7,6,4,2] [7,6,3,1] [7,6,5,2] [7,6,5,4,2,1] [7,5,4,3,2,1]	18
8	255	[8,4,3,2] [8,6,5,3] [8,6,5,2] [8,5,3,1] [8,6,5,1] [8,7,6,1] [8,7,6,5,2,1] [8,6,4,3,2,1]	16
9	511	[9,4] [9,6,4,3] [9,8,5,4] [9,8,4,1] [9,5,3,2] [9,8,6,5] [9,8,7,2] [9,6,5,4,2,1] [9,7,6,4,3,1] [9,8,7,6,5,3]	48
10	1023	[10,3] [10,8,3,2] [10,4,3,1] [10,8,5,1] [10,8,5,4] [10,9,4,1] [10,8,4,3] [10,5,3,2] [10,5,2,1] [10,9,4,2] [10,6,5,3,2,1] [10,9,8,6,3,2] [10,9,7,6,4,1] [10,7,6,4,2,1] [10,9,8,7,6,5,4,3] [10,8,7,6,5,4,3,1]	60
11	2047	[11,2] [11,8,5,2] [11,7,3,2] [11,5,3,2] [11,10,3,2] [11,6,5,1] [11,5,3,1] [11,9,4,1] [11,8,6,2] [11,9,8,3] [11,10,9,8,3,1]	176

For every set [L, k, ..., p] feedback taps listed in the table, there exists an image set (reverse set) of feedback taps [L, L-k, ..., L-p] that generates an identical sequence reversed in time.

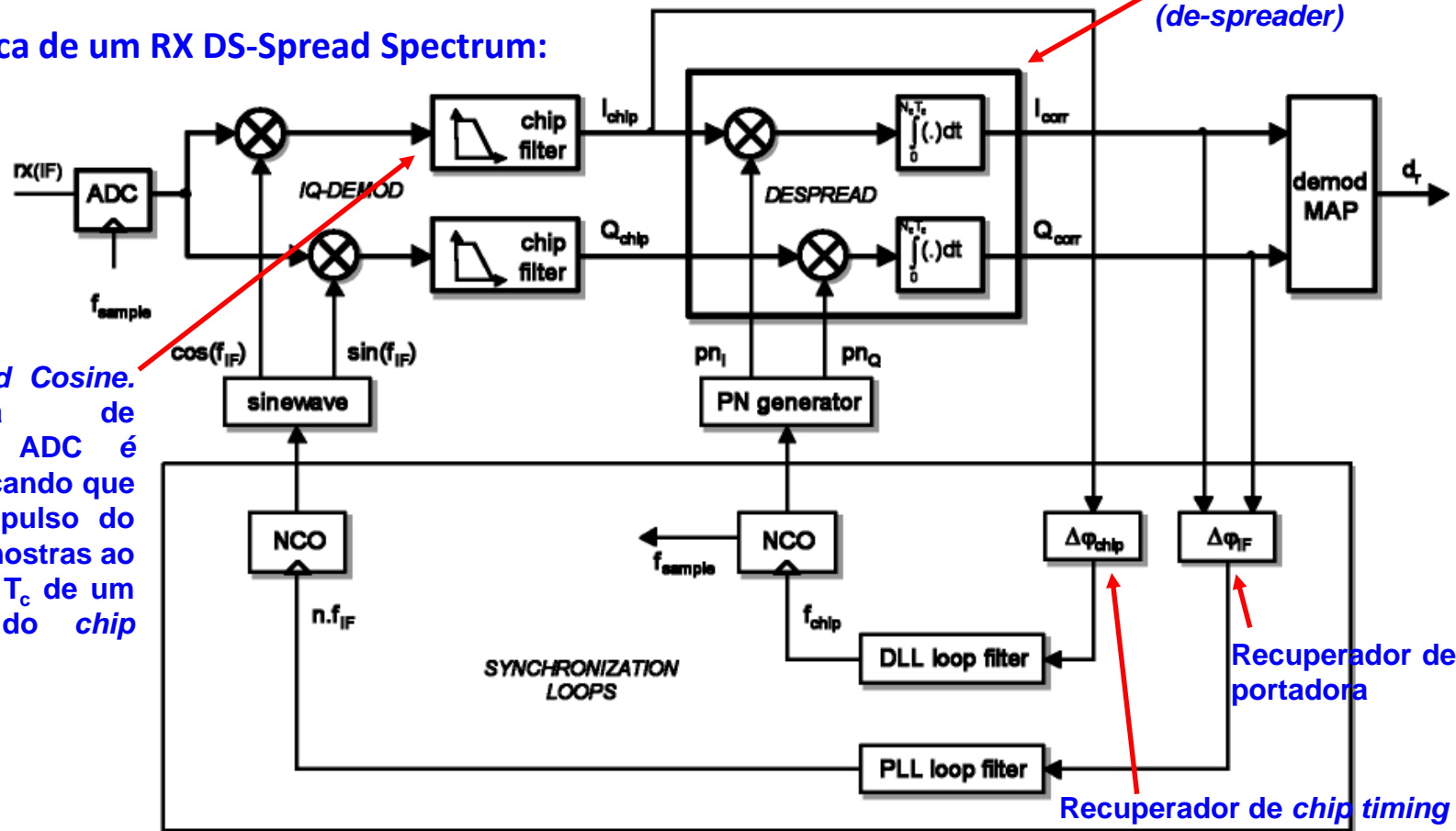
Arquitetura típica de um TX DS-Spread Spectrum:



Spreader

Filtro *Root Raised Cosine*. A frequência de amostragem do DAC é  $f_{\text{sample}} = k/T_c$ , implicando que a resposta ao impulso do *chip filter* tem  $k$  amostras ao longo da duração  $T_c$  de um símbolo BPSK do *chip sequence*.

Arquitetura típica de um RX DS-Spread Spectrum:



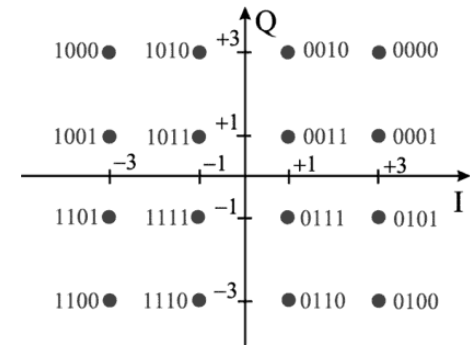
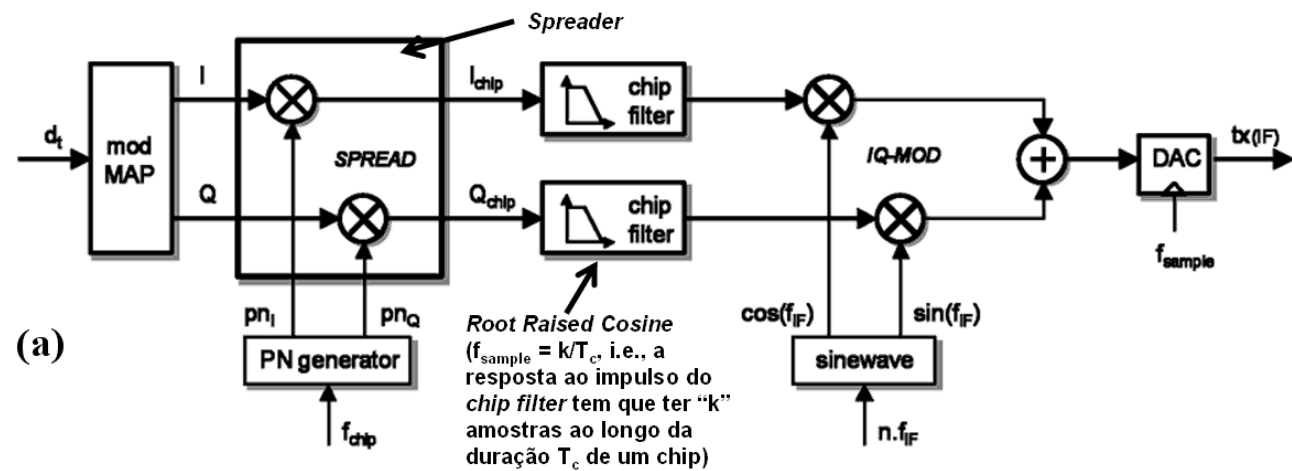
Filtro Root Raised Cosine. A frequência de amostragem do ADC é  $f_{\text{sample}} = k/T_c$ , implicando que a resposta ao impulso do chip filter tem  $k$  amostras ao longo da duração  $T_c$  de um símbolo BPSK do chip sequence.

The basic building blocks of a DS-SS (digital) receiver are:

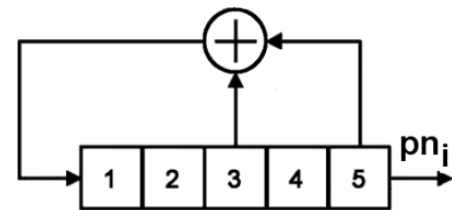
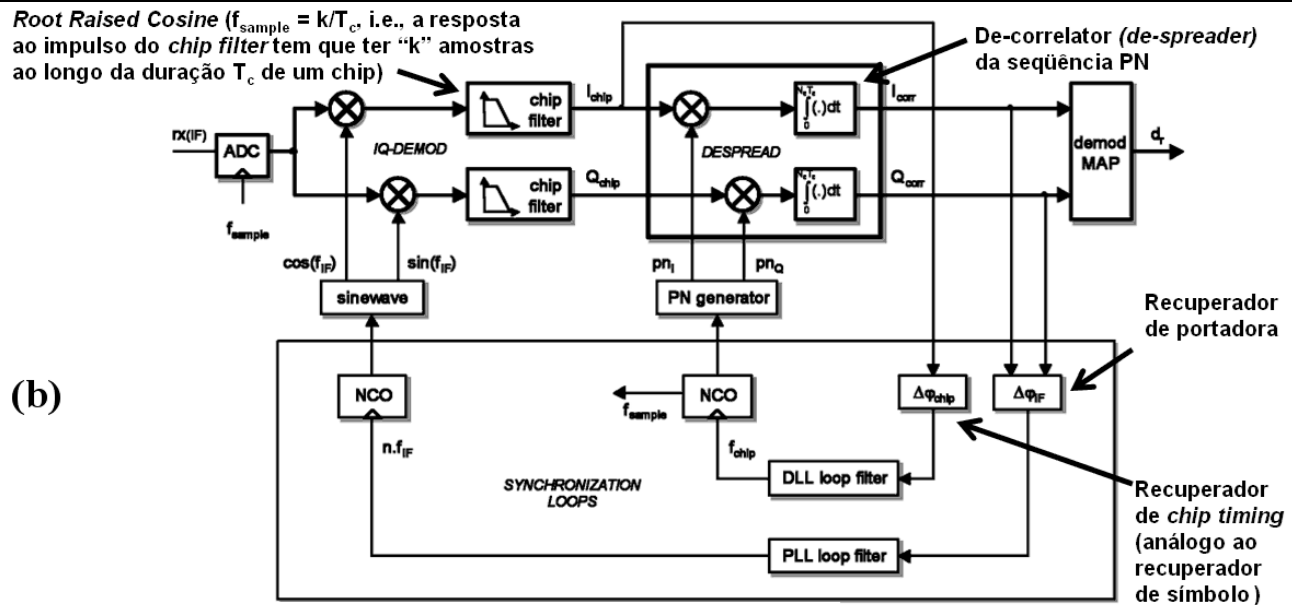
- coherent IQ vector-demodulator with waveform synthesizer (Direct Digital Synthesis) at the IF-carrier frequency ( $f_{IF}$ ) and chip matched filters (usually Square Root Raised Cosine)
- despreading (correlation of the received symbols with the locally generated PN-sequence(s)  $pn_I$  and  $pn_Q$ )
- decorrelated 'IQ to data' demodulator mapping
- synchronization loops for the IF-carrier ( $f_{IF}$ , phase error  $\Delta\phi_{IF}$  measured after despreading to reduce the influence of noise) and chip frequency ( $f_{chip}$ )

# Sinais Direct Sequence Spread Spectrum (DS-SS)

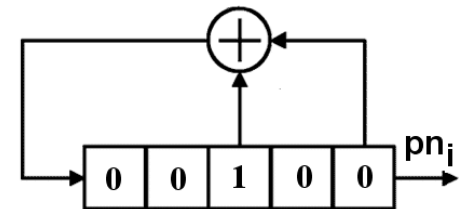
**Exemplo 10:** diagrama na Figura 1 abaixo mostra a etapa de modulação de um sistema DS-Spread Spectrum 16-QAM:



(c) mod e demod MAP



(d) PN generator SSRG[5,3] p/ a sequência de símbolos I. A cada novo símbolo I (e Q) o SSRG é inicializado conforme segue:



**Figura 1:** (a) TX DS-Spread Spectrum 16-QAM. (b) RX DS-Spread Spectrum 16-QAM (c) IQ mapper & de-mapper (d) “PN generator” usado no “Spreader” da sequência de símbolos I em (a).

## Sinais Direct Sequence Spread Spectrum (DS-SS)

O sistema utiliza  $N_C = 31$  chips por símbolo IQ e o “de-spreader” do RX é implementado por meio de um *matched-filter* para a seqüência de chips gerada no “spreader” do TX. Sabendo que o sistema não apresenta erros de sincronização nem no recuperador de portadora nem no recuperador de chip timing, pede-se:

- Determine o gráfico da seqüência  $pn_i$  na saída do “PN generator” na Figura 1 (a) p/ cada símbolo I na entrada do “Spreader” do TX.
- Determine o gráfico da seqüência  $pn_i$  reversa (imagem) da seqüência gerada em a), a ser utilizada no “de-spreader” do RX.
- Determine o balanceamento (nível DC) da seqüência  $pn_i$  gerada em a).
- Determine o gráfico da auto-correlação da seqüência de chips  $pn_i$  gerada no “Spreader” do TX.
- Determine o gráfico da correlação cruzada entre a seqüência de chips  $pn_i$  gerada no “Spreader” do TX e a a seqüência de chips  $pn_i$  gerada no “de-spreader” do RX.
- Dois símbolos consecutivos  $I_1$  e  $I_2$  são gerados no *mapper* do TX respectivamente pelas palavras binárias “1101” e “0111”. Assumindo que não haja multipercurso nem ruído no canal, determine a saída  $I_{corr}$  do “de-spreader” do RX para estas palavras binárias.

### Solução:

Do enunciado, é dado:

InitState := (0 0 1 0 0)<sup>T</sup> ← Estado inicial do SSRG[5,3]

$N_c := 31$  ← Numero de chips por símbolo IQ.

Idealmente  $N_c = 2^L - 1$ ,  $L$  é o tamanho do SSRG.

Ainda, do enunciado, os símbolos  $I_1$  e  $I_2$  são (vide *mapper* na Fig A) gerados pelas palavras binárias  $B_{10} := "1101"$  e  $B_{20} := "0111"$ , resultando nos seguintes valores para os símbolos  $I_1$  e  $I_2$ :

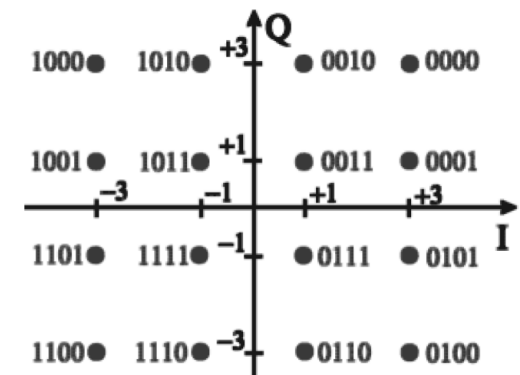


Fig A: *mapper*

$I1 = (-3)I2 = (1)$  ← O parêntese caracteriza que os símbolos são complexos  $I+jQ$ , e que estamos apenas utilizando a parte real  $I$  p/ efeito de simplificação.

Para gerar as seqüências de *chips* direta **pni53** usada no *spreader* do TX e a reversa **pni52** usada no *de-spreader* do RX, executa-se o seguinte procedimento para cada uma delas:

- 1- Inicializar o SSRG c/ o estado inicial  $\text{InitState}^T = (0 \ 0 \ 1 \ 0 \ 0)$ . Inicializar contador de *chips* em  $n=0$ .
- 2- Calcular a saída  $t$  da operação  $\oplus$ , conforme Fig B acima.
- 3- Armazenar o valor do bit mais à direita do SSRG da Fig B na FIFO (*buffer*) de saída  $\text{pn}_i$ .
- 4- *Shiftar* o SSRG um bit à direita.
- 5- Atribuir a saída  $t$  ao bit mais à esquerda do SSRG da Fig B.
- 6- Se  $n > N_c$  vá para o passo 7, caso contrário,  $n = n + 1$  e volta ao passo 2
- 7- Substituir todos os "0" por "-1" no *buffer* de saída  $\text{pn}_i$ . Fim do procedimento.

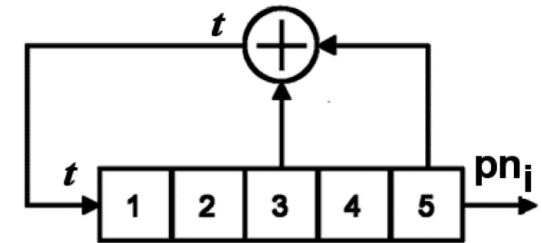
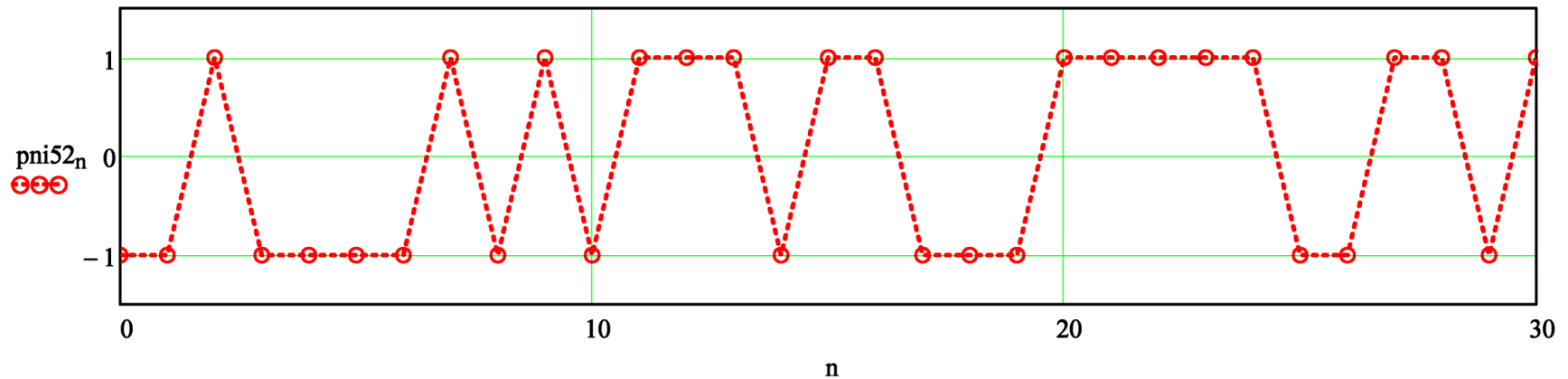
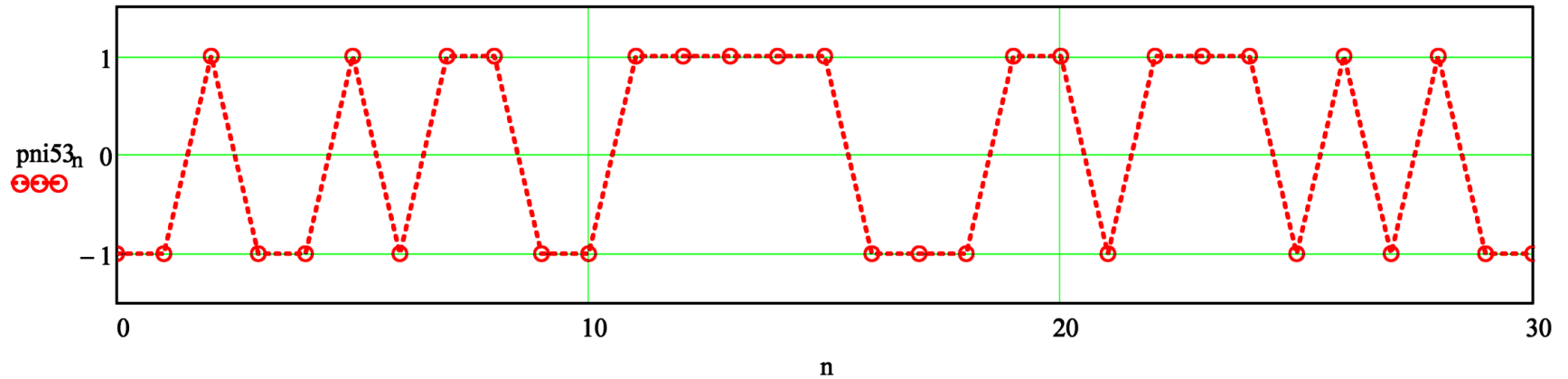


Fig B: SSRG[5,3]



**a&b)** Os gráficos da seqüências de *chips* direta e reversa assim geradas, resultam em:

$n := 0..N_c - 1$



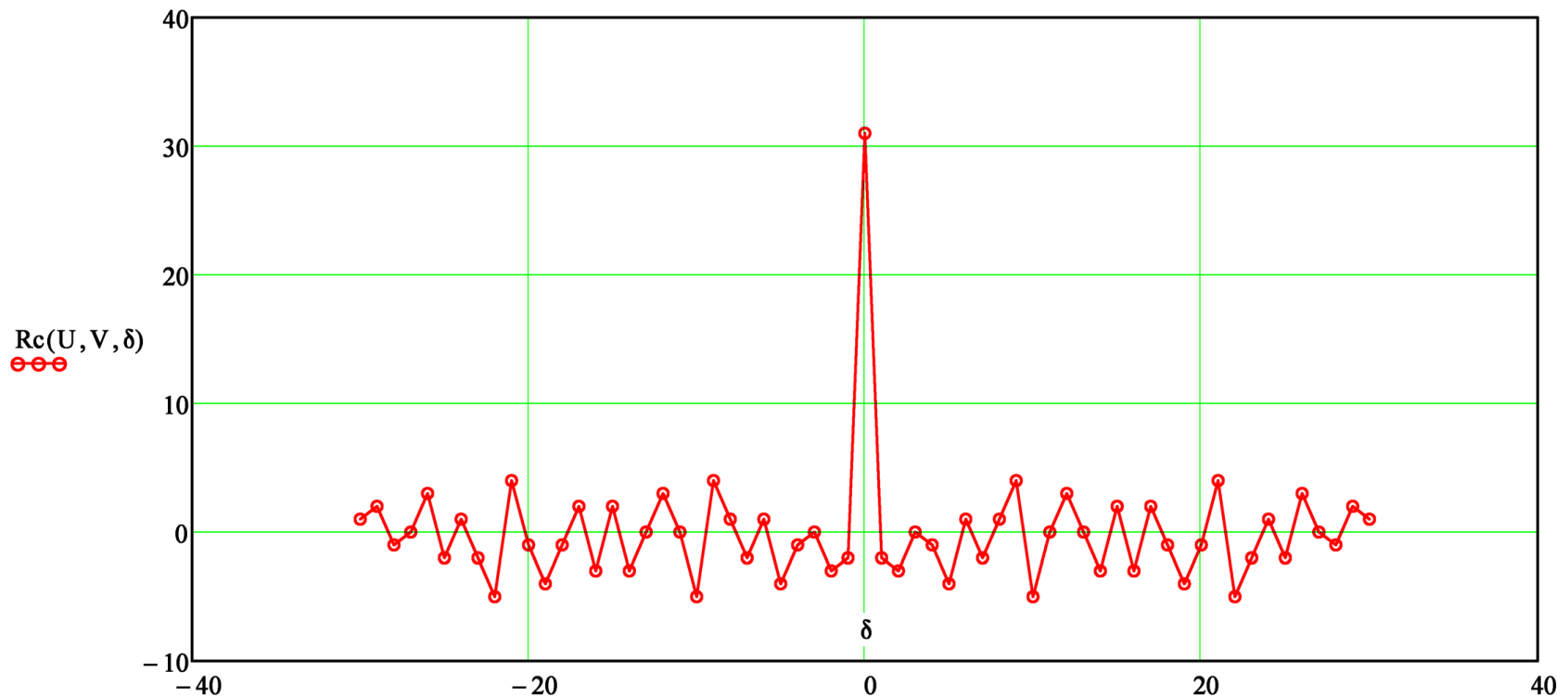
**c)** Nível DC:  $\sum p_{ni53} = 1$

**d)** A correlação  $R_c(\delta)$  entre duas seqüências U e V de mesmo número  $N_c = \text{length}(U) = \text{length}(V)$  de amostras é dada por:

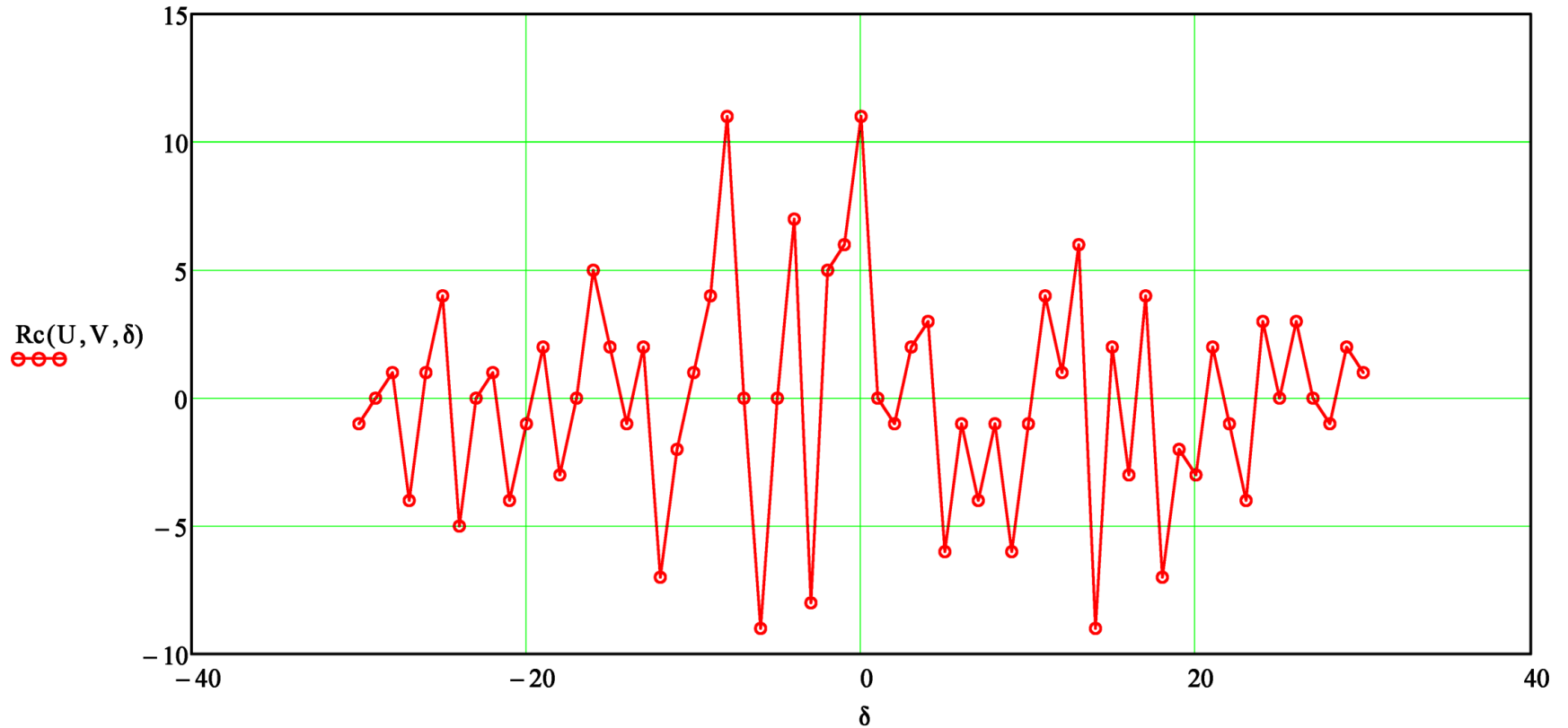
$$R_c(U, V, \delta) := \text{if} \left[ \begin{array}{l} \delta > 0, \\ \sum_{n=0}^{\text{length}(V)-1-\delta} (V_n \cdot U_{n+\delta}), \\ \sum_{n=0}^{\text{length}(U)-1+\delta} (U_n \cdot V_{n-\delta}) \end{array} \right] \quad (1)$$

sendo  $\delta := -(N_c - 1) .. (N_c - 1)$  os limites de deslocamento temporal entre U e V. Note que se  $\delta < 0$ , a equação (1) calcula a correlação fazendo V atrasado de  $\delta$  em relação a U e se  $\delta > 0$  equação (1) calcula a correlação fazendo U adiantado de  $\delta$  em relação a V.

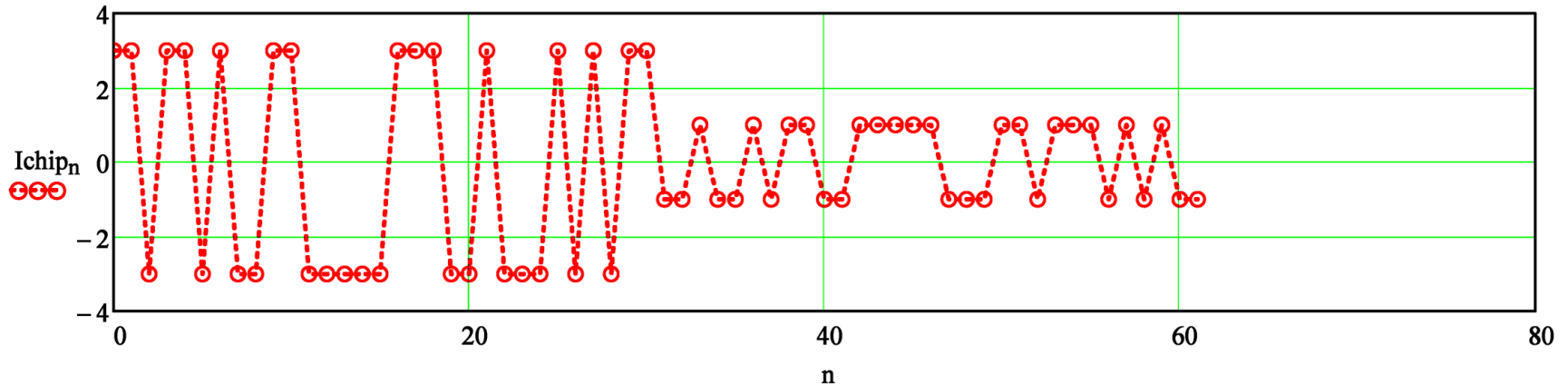
Seja  $U := \text{pni53}$  e seja  $V := U$ . Da equação (1), a função auto-correlação resulta em:



e) Da equação (1), com  $U := \text{pni53}$  e  $V := \text{pni52}$  a função de correlação cruzada resulta em:

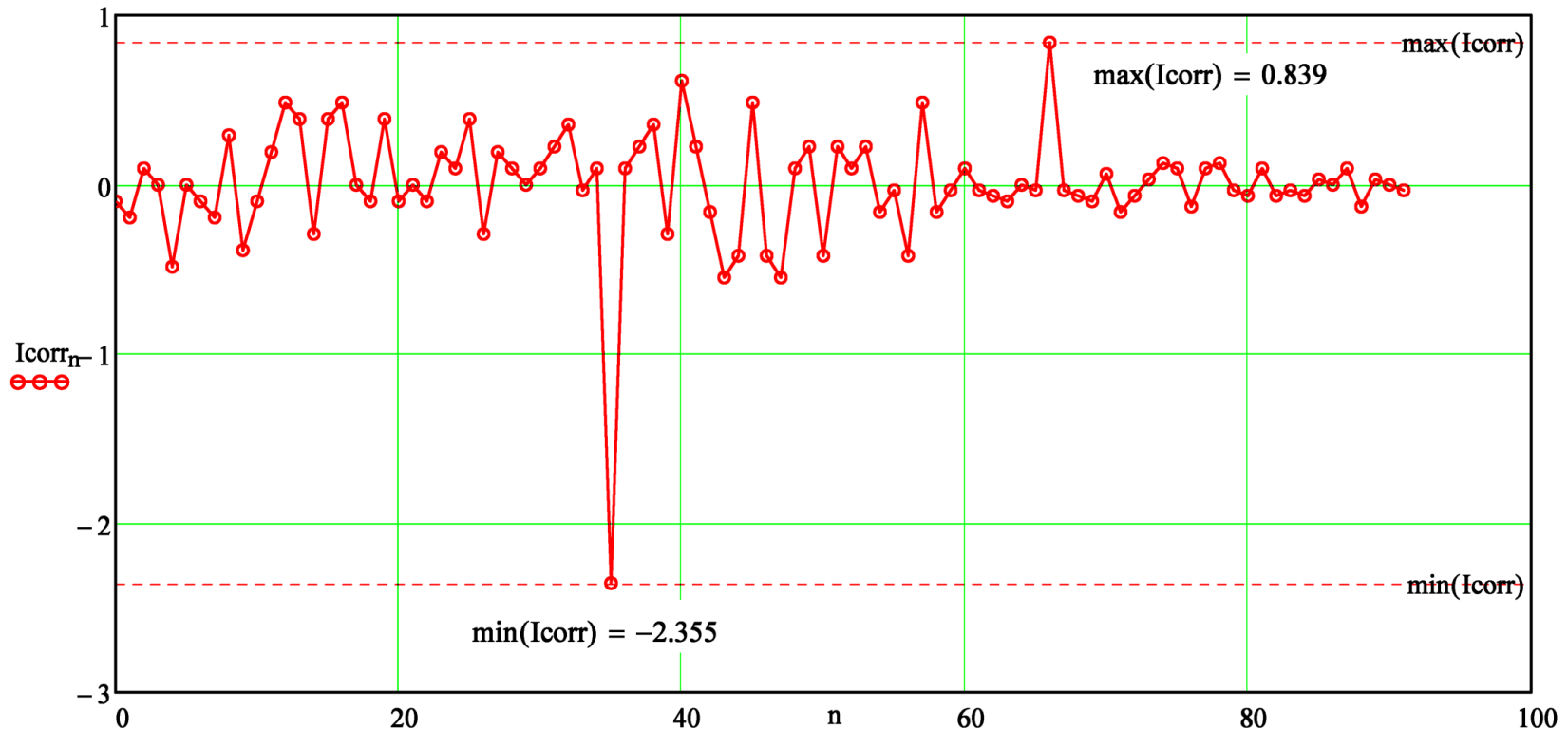


f) Primeiramente é necessário obter a seqüência  $I_{chip}$  na saída do “spreader” do TX, a qual, em não havendo ruído nem multipercurso no canal, é a própria seqüência  $I_{chip}$  na entrada do “de-spreader” do RX (ver Figura 1 do enunciado).  $I_{chip}$  é obtida do produto da  $p_{ni53}$  por  $I_1 = (-3)$  ao longo de  $N_c = 31$  chips concatenada com o produto da  $p_{ni53}$  por  $I_2 = (1)$  ao longo dos próximos  $N_c = 31$  chips. O gráfico da seqüência  $I_{chip}$  assim gerada, resulta em:



## Sinais Direct Sequence Spread Spectrum (DS-SS)

Do enunciado, o “*de-spreader*” do RX é implementado por meio de um *matched-filter* para a seqüência de *chips* gerada no “*spreader*” do TX. Portanto, a saída  $I_{\text{corr}}$  do “*de-spreader*” do RX é o resultado da **convolução** da seqüência  $I_{\text{chip}}$  na entrada do “*de-spreader*” com a resposta ao impulso do *matched-filter* dada pela seqüência reversa (imagem) **pni52**. Assim, efetuando a convolução entre as seqüências  $I_{\text{chip}}$  e **pni52** e normalizando pelo valor  $N_c = 31$ , obtém-se a saída  $I_{\text{corr}}$  do “*de-spreader*”:

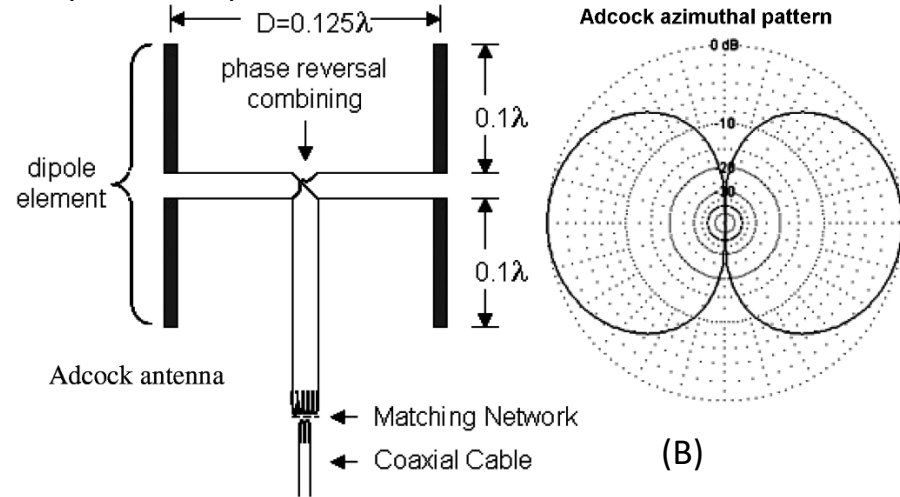
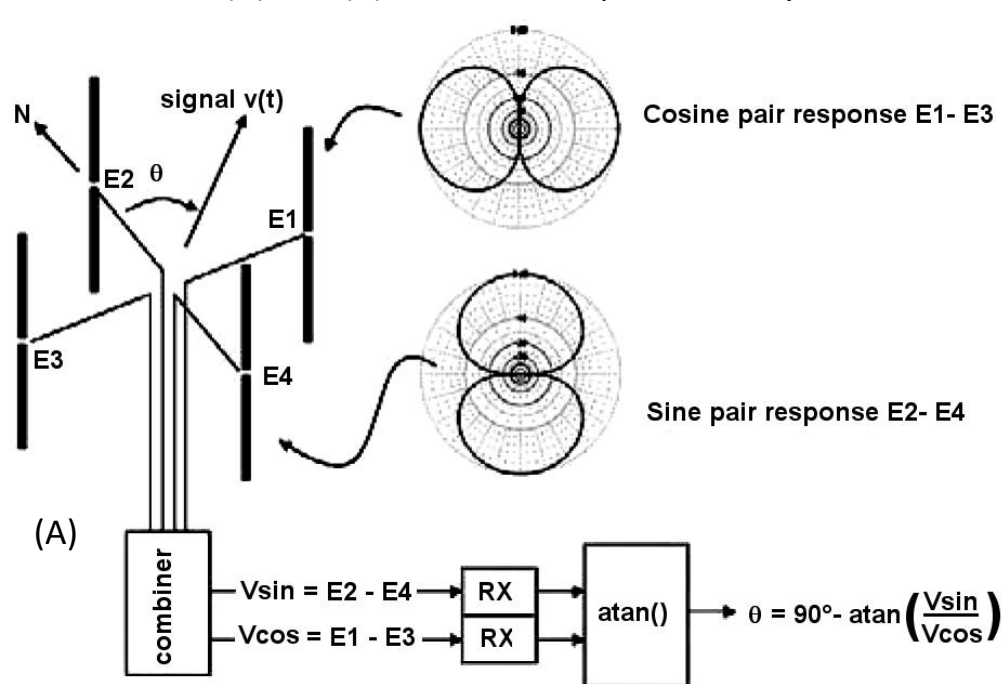


Note que o “*de-spreader*” recuperou uma aproximação dos símbolos  $I_1 = (-3)$  e  $I_2 = (1)$   
Quanto maior  $L$ , melhor a aproximação.

## Localização de emissores de radiação EM

Uma das ações mais cruciais em sistemas EW para ES (*Electronic Support*) é a localização de sinais irradiados por ameaças (*threats*). Uma vez conhecido os ângulos DOA (*Direction Of Arrival*) do sinal do TX inimigo que incide em duas ou mais estações receptoras, técnicas de triangulação podem ser aplicadas para localizar o TX, conforme visto no Exemplo 6 no slide 54. Triangulação é uma das abordagens mais usuais, embora não seja a técnica de maior precisão. A técnica TDOA (*Time Difference Of Arrival*), que discutiremos no slide 104, é uma das técnicas de maior precisão usualmente adotadas.

Há diversas técnicas para determinar os ângulos DOA do sinal do TX inimigo. No Cap II estudaremos os algoritmos MUSIC (*Multiple Signal Classification*) e ESPRIT (*Estimation of Signal Parameter via Rotational Invariance Technique*), com uma precisão melhor que  $0.1^{\circ(\text{rms})}$  na estimação do DOA. Uma técnica clássica é a técnica Watson-Watt (ver <http://www.fccdecastro.com.br/pdf/EWWBMDf.pdf>), que resulta em uma precisão melhor que  $2.5^{\circ(\text{rms})}$ . A técnica **Watson-Watt** determina o DOA  $\theta$  basicamente através de um esquema de comparação das amplitudes dos sinais de saída de dois *phased-arrays* Adcock (estudaremos *phased-arrays* no Cap II) dispostos ortogonalmente no espaço, conforme mostrado em (A). Em (B) é mostrado o *phased-array* Adcock formado por dois dipolos.

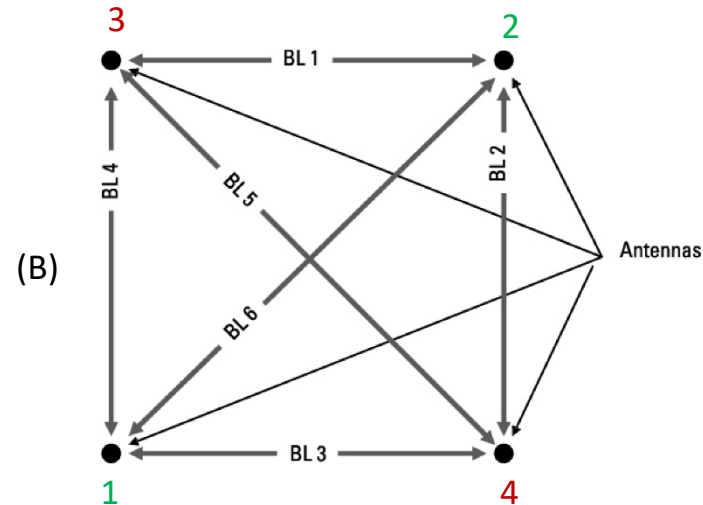
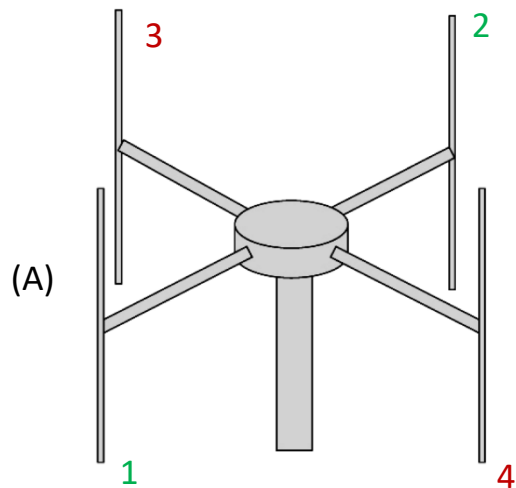


Note em (B) que a linha de transmissão do dipolo da direita tem seu terminais invertidos no ponto de alimentação do *array*, de modo que as tensões geradas são defasadas de  $180^{\circ}$ .



## Localização de emissores de radiação EM

Outra técnica usual para determinar o ângulo DOA do sinal do TX inimigo é a **radio-interferometria**, que resulta em uma precisão melhor que  $1.0^{\circ(\text{rms})}$ . A antena de um radio-interferômetro é um *array* de múltiplos pares de antenas. Cada par de antenas é interligado por uma reta fictícia denominada *baseline*. A precisão de um radio-interferômetro será tanto maior quanto maior for a *baseline* em relação ao comprimento de onda de operação  $\lambda = c/f$ , onde  $f$  é a frequência de operação e  $c = 3 \times 10^8$  [m/s] é a velocidade de propagação da onda EM. Quanto mais *baselines* tiver o sistema mais medidas de DOA podem ser efetuadas e correlacionadas entre si de modo a aumentar a precisão e minimizar os efeitos de multipercurso originados por reflexão da onda EM em estruturas constituídas de condutores elétricos (metal, água, etc ...) no caminho de propagação da onda.



Por exemplo, em (A) é mostrado a antena típica de um radio-interferômetro para a faixa de HF constituída por 4 dipolos verticais, cada par de dipolos formando uma *baseline*, de modo que este sistema opera com 6 *baselines* conforme mostrado em (B).

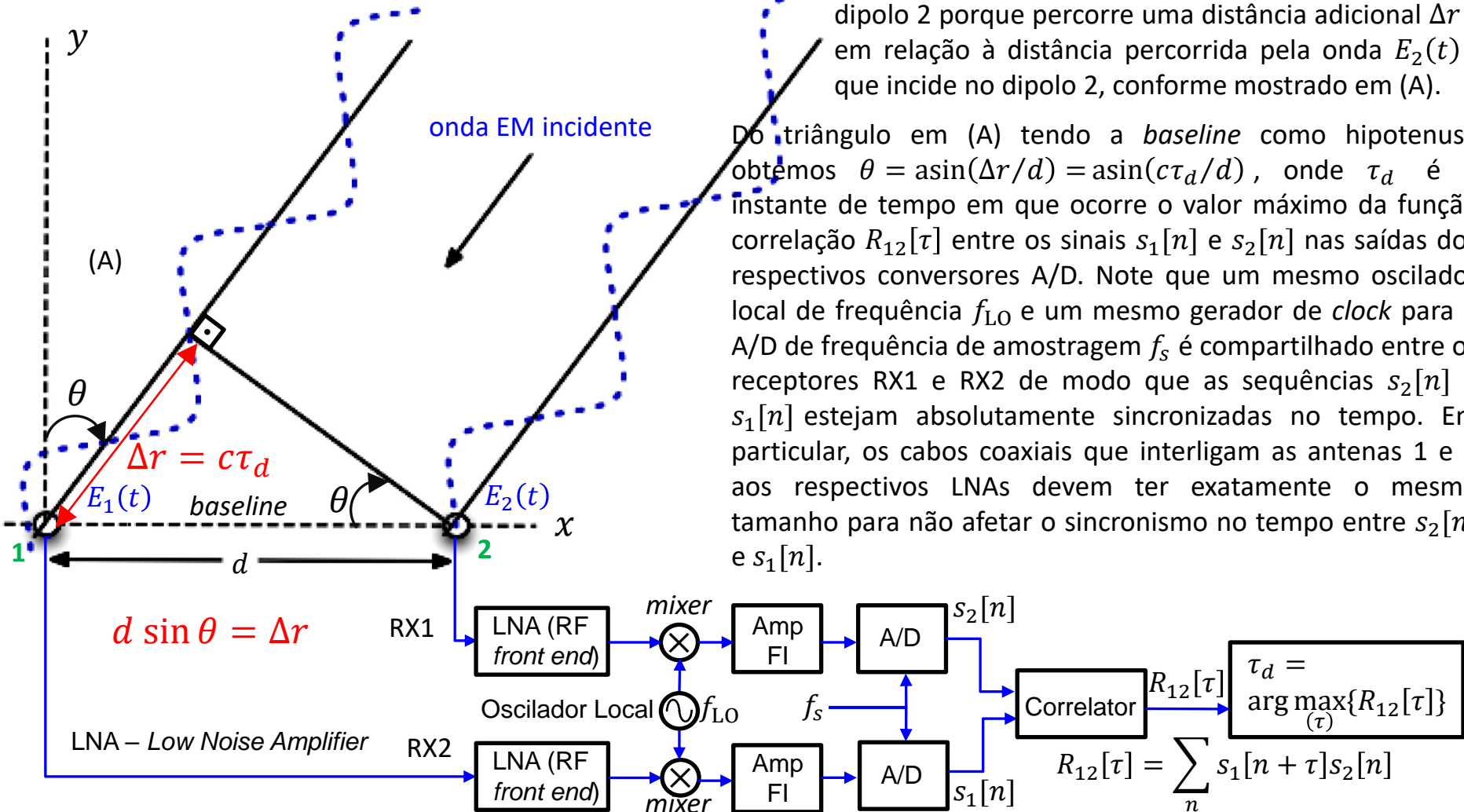
Independente do número de *baselines*, o elemento básico de um radio-interferômetro é a diferença de tempo da onda EM que incide em cada dipolo de cada par de dipolos interligado por uma *baseline*. Especificamente, a diferença de tempo entre as tensões resultantes respectivamente nos terminais dos dipolos 1 e 2 em (A) é uma medida do DOA no plano do azimute da onda EM que incide nos dois dipolos. Mesmo vale para todos os 6 pares de dipolos interligados pelas 6 respectivas *baselines* em (B).

## Localização de emissores de radiação EM

Dado que a diferença de tempo entre as tensões resultantes respectivamente nos terminais de dois dipolos do *array* é uma medida do DOA da onda EM incidente, passamos agora a analisar como a referida diferença de tempo é convertida em ângulo DOA. Em (A) abaixo são mostrados os dipolos 1 e 2 do diagrama em (A) no slide anterior e o processo determinação do ângulo de DOA  $\theta$  no plano do azimute da onda EM que incide nos dois dipolos.

A onda EM  $E_1(t)$  que incide no dipolo 1 está atrasada de  $\tau_d$  [s] da onda  $E_2(t)$  que incide no dipolo 2 porque percorre uma distância adicional  $\Delta r$  em relação à distância percorrida pela onda  $E_2(t)$  que incide no dipolo 2, conforme mostrado em (A).

Do triângulo em (A) tendo a *baseline* como hipotenusa obtemos  $\theta = \text{asin}(\Delta r/d) = \text{asin}(c\tau_d/d)$ , onde  $\tau_d$  é o instante de tempo em que ocorre o valor máximo da função correlação  $R_{12}[\tau]$  entre os sinais  $s_1[n]$  e  $s_2[n]$  nas saídas dos respectivos conversores A/D. Note que um mesmo oscilador local de frequência  $f_{LO}$  e um mesmo gerador de *clock* para o A/D de frequência de amostragem  $f_s$  é compartilhado entre os receptores RX1 e RX2 de modo que as sequências  $s_2[n]$  e  $s_1[n]$  estejam absolutamente sincronizadas no tempo. Em particular, os cabos coaxiais que interligam as antenas 1 e 2 aos respectivos LNAs devem ter exatamente o mesmo tamanho para não afetar o sincronismo no tempo entre  $s_2[n]$  e  $s_1[n]$ .



## Localização de emissores de radiação EM

**Exemplo 11:** A onda EM que incide no dipolo 2 em (A) no slide anterior é um pulso *chirp*  $E_2(t) = 1.0 \cos(2\pi f_0(t)t)$  modulado em LFM (*Linear Frequency Modulation*) que varre linearmente a frequência  $f_0(t)$  do sinal  $s_2(t)$  no intervalo  $f_1 < f_0(t) < f_2$  durante o intervalo de tempo  $T = 3[\mu\text{s}]$ , sendo  $f_1 = 50$  [MHz] e  $f_2 = 100$  [MHz]. A *baseline* entre as antenas 1 e 2 tem um tamanho  $d = 2$  [m] e a onda EM  $E_1(t)$  que incide no dipolo 1 está atrasada de  $\tau_d = 5$  [ns] da onda  $E_2(t)$  que incide no dipolo 2 em consequência da distância adicional  $\Delta r$  percorrida. Para minimizar a complexidade dos gráficos a serem gerados na solução deste exemplo, assuma que a frequência de amostragem  $f_s$  dos conversores A/D é suficientemente alta para que as sequências  $s_2[n]$  e  $s_1[n]$  em suas respectivas saídas sejam considerados sinais contínuos  $s_2(t)$  e  $s_1(t)$ . **Pede-se:** **(a)** Plote  $s_2(t)$  e  $s_1(t)$  no intervalo  $-T < t < T$ . **(b)** Plote  $s_2(t)$  e  $s_1(t)$  superpostos em um mesmo gráfico no intervalo  $-6\tau_d < t < 6\tau_d$  e identifique no gráfico o atraso  $\tau_d$  de  $s_1(t)$  em relação a  $s_2(t)$ . **(c)** Determine e plote a saída  $R_{12}(\tau)$  do bloco Correlator em (A) no slide anterior no intervalo  $-T < \tau < T$ . **(d)** Determine a saída  $R_{12}(\tau)$  do bloco Correlator em (A) no slide anterior no intervalo  $-T/10 < \tau < T/10$ , plote  $R_{12}(\tau)$  no intervalo  $-6\tau_d < t < 6\tau_d$  e verifique se o instante  $\tau$  que ocorre o máximo de  $R_{12}(\tau)$  corresponde ao atraso  $\tau_d$  de  $s_1(t)$  em relação a  $s_2(t)$ . **(e)** Determine o ângulo DOA no plano do azimute (=ângulo  $\theta$  em (A) no slide anterior) para a onda EM que incide no *array* de antenas do interferômetro.

O *script* do software MathCad utilizado como auxílio na solução deste exemplo está disponível em <http://www.fccdecastro.com.br/ZIP/E11S99.zip>.

**Solução:** **(a)** Do enunciado

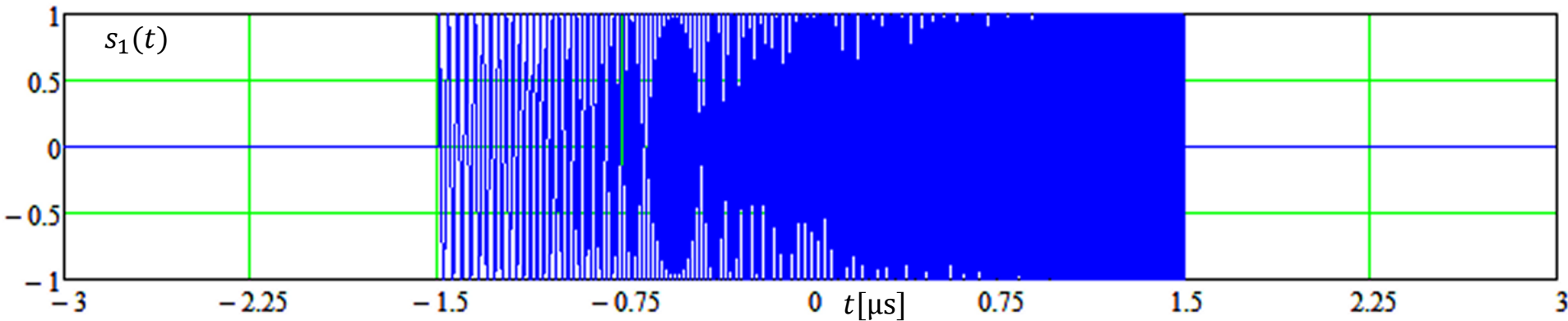
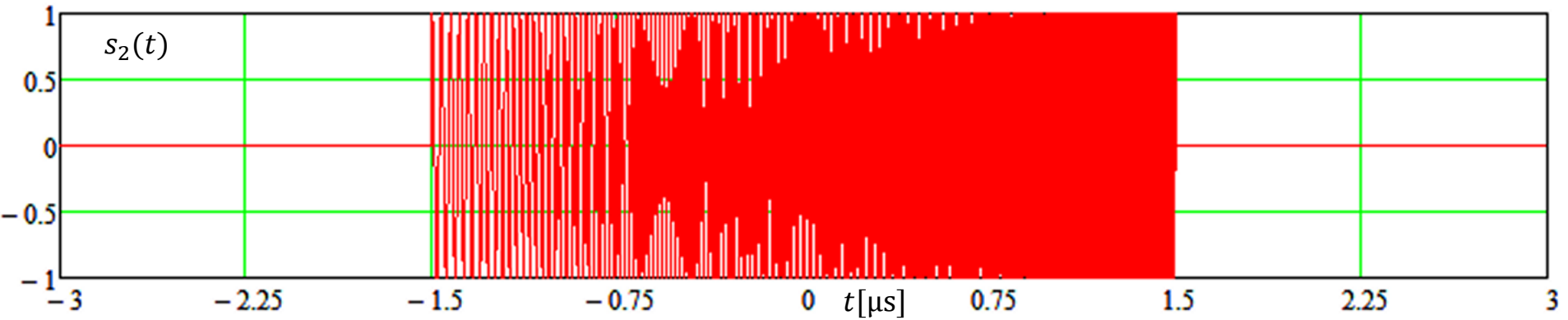
$$f_c = (f_1 + f_2)/2 = 75 \text{ [MHz]}$$

$$B = f_2 - f_1 = 50 \text{ [MHz]}$$

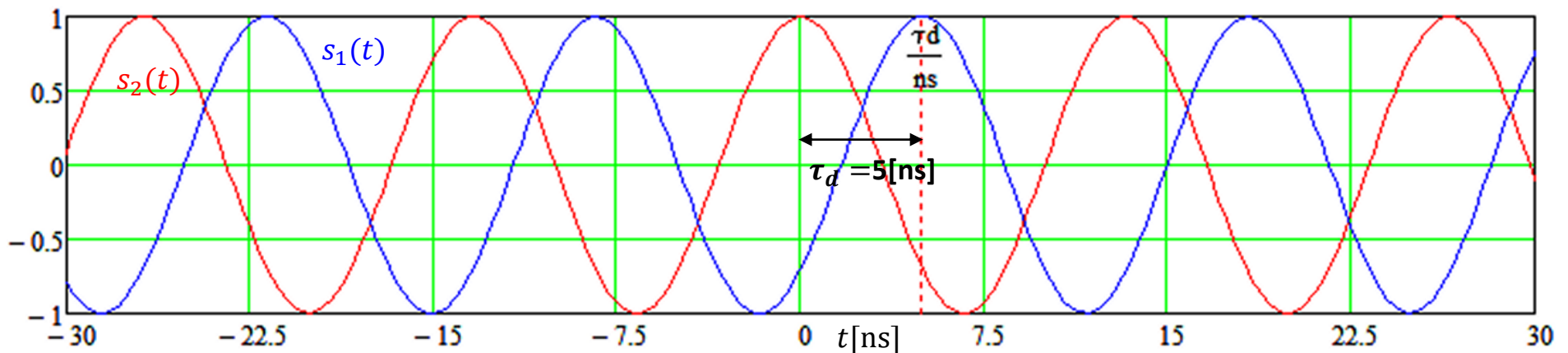
$$\text{De (20): } s_2(t) = \text{Re} \left\{ \text{Pulso} \left( \frac{t}{T} \right) e^{j2\pi \left( f_c t + \frac{B}{T} t^2 \right)} \right\} \quad \text{onde } \text{Pulso}(x) = \begin{cases} 1.0, & |x| < 0.5 \\ 0.0, & x \geq 0.5 \end{cases} .$$

$$s_1(t) = s_2(t - \tau_d)$$

## Localização de emissores de radiação EM



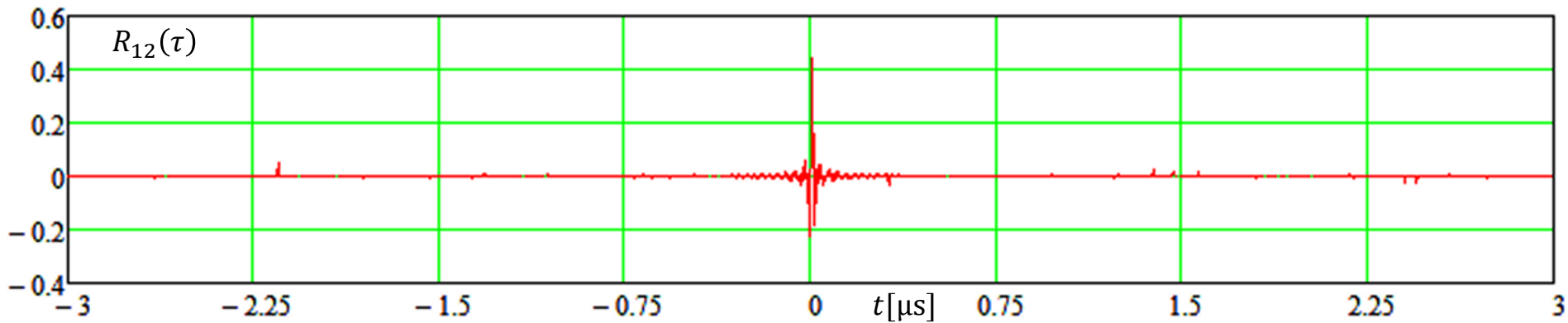
(b) Plotando  $s_2(t)$  e  $s_1(t)$  no intervalo  $-6\tau_d < t < 6\tau_d$  e identificando o atraso  $\tau_d$  de  $s_1(t)$  em relação a  $s_2(t)$ :



## Localização de emissores de radiação EM

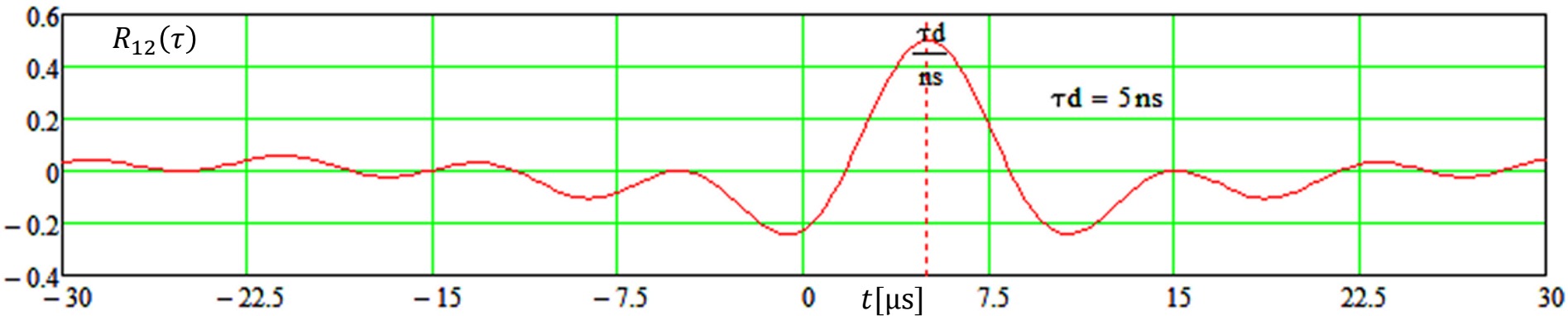
(c) É dado no enunciado que a frequência de amostragem  $f_s$  dos conversores A/D é suficientemente alta para que as sequências  $s_2[n]$  e  $s_1[n]$  em suas respectivas saídas sejam considerados sinais contínuos  $s_2(t)$  e  $s_1(t)$ . Então a correlação discreta se torna uma correlação contínua:

$$R_{12}(\tau) = \frac{1}{T} \int_{-T}^T s_1(t + \tau) s_2(t) dt$$



## Localização de emissores de radiação EM

(d) Determinando  $R_{12}(\tau)$  no intervalo  $-T/10 < \tau < T/10$ , plotando  $R_{12}(\tau)$  no intervalo  $-6\tau_d < t < 6\tau_d$  e identificando o atraso  $\tau_d$  como sendo o instante em que ocorre o máximo de  $R_{12}(\tau)$ , i.e.,  $\tau_d = \arg \max_{(\tau)} \{R_{12}(\tau)\}$ :



Note, portanto, que o sistema determina o atraso  $\tau_d$  de  $s_1(t)$  em relação a  $s_2(t)$  como sendo o instante em que ocorre o máximo de  $R_{12}(\tau)$ , i.e.,  $\tau_d = \arg \max_{(\tau)} \{R_{12}(\tau)\}$ .

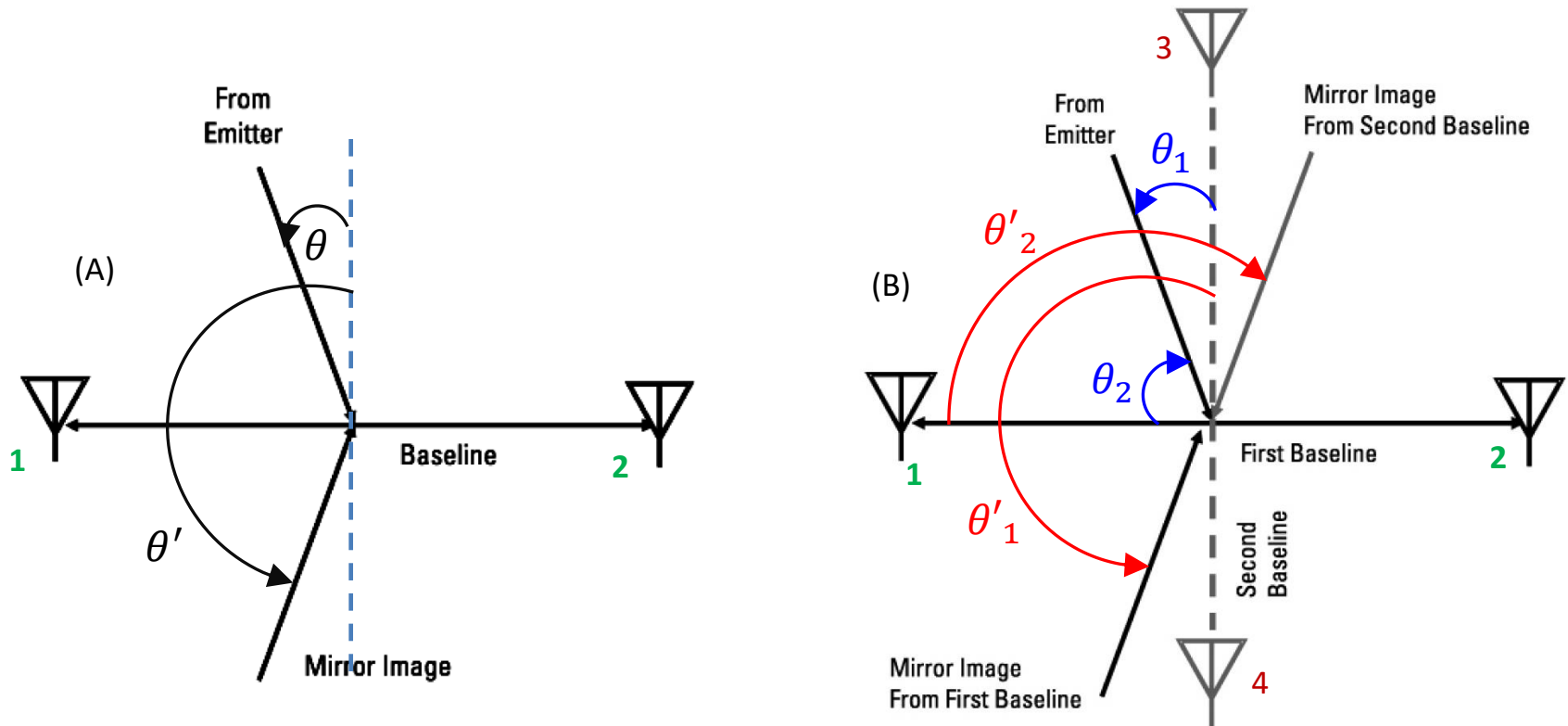
(e) Uma vez obtido o atraso  $\tau_d$  de  $s_1(t)$  em relação a  $s_2(t)$  através de  $\tau_d = \arg \max_{(\tau)} \{R_{12}(\tau)\}$ , o ângulo DOA no plano do azimute (=ângulo  $\theta$ ) para a onda EM que incide no *array* de antenas do interferômetro é dado por:

$$\theta = \text{asin}(c\tau_d/d) = 48.6^\circ$$



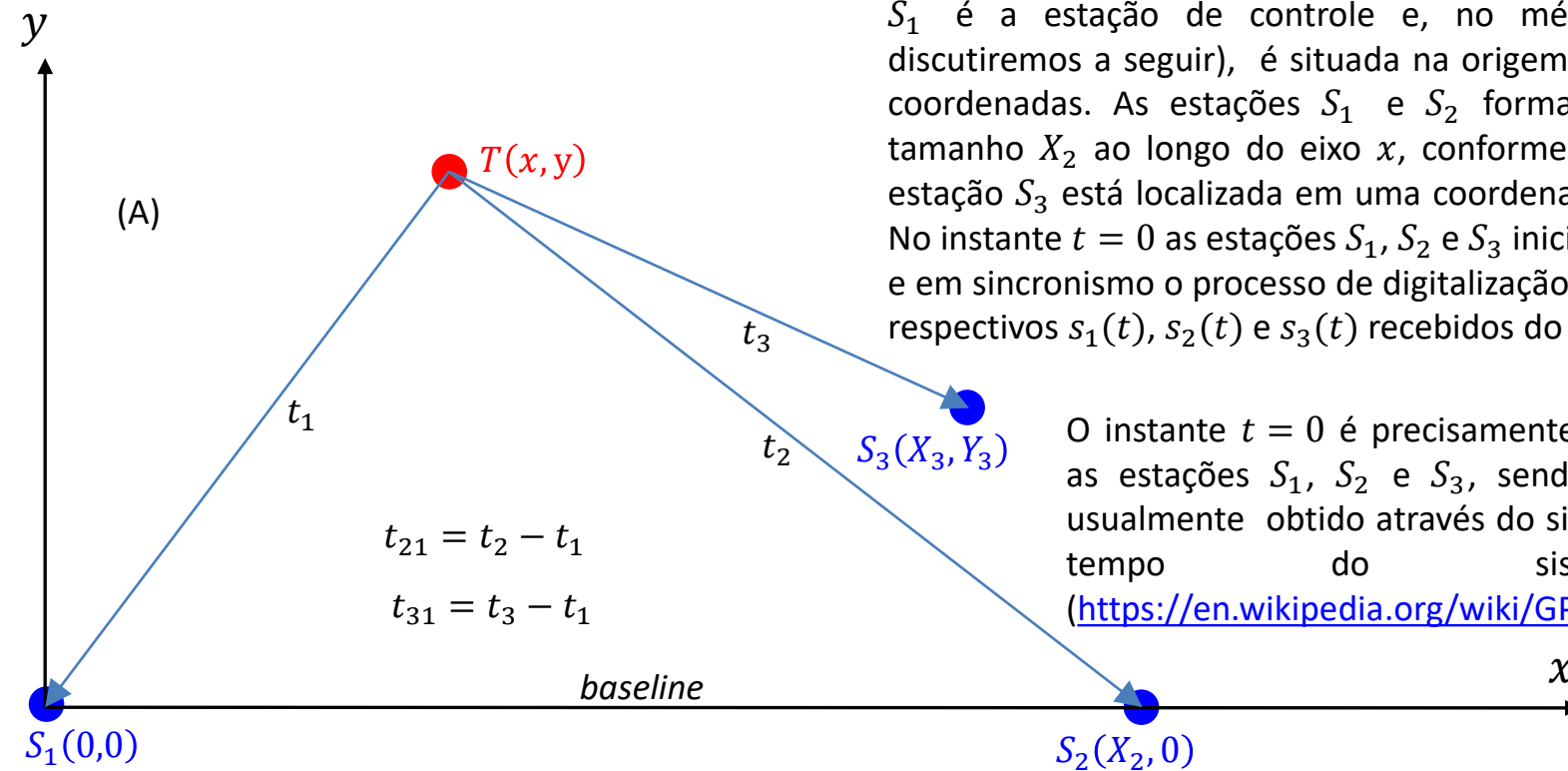
## Localização de emissores de radiação EM

Como o padrão de irradiação do *array* dos dipolos 1 e 2 cobre 360° no plano de azimute, um interferômetro com uma única *baseline* apresenta uma ambiguidade *front-back*, conforme mostrado em (A). Note que ambos sinais “From Emitter” e “Mirror Image” que incidem no *array* respectivamente nos ângulos DOA  $\theta$  e  $\theta'$  gerariam o mesmo atraso  $\tau_d$  na saída do bloco Correlator em (A) no slide 98. Esta ambiguidade é resolvida conforme mostrado em (B), em que a medida dos ângulos DOA  $\theta$  e  $\theta'$  é adicionalmente efetuada através de uma segunda *baseline*, estabelecida entre os dipolos 3 e 4. Os DOAs corretos ( $\theta_1$  e  $\theta_2$  em (B)) resultam no mesmo vetor de direção nas duas medições, enquanto os DOAs ambíguos ( $\theta'_1$  e  $\theta'_2$  em (B)) resultam em vetores de direção díspares.



## TDOA - Time Difference of Arrival

TDOA é uma técnica de alta precisão que determina as coordenadas  $(x, y)$  de um TX inimigo  $T$ , sem depender de triangulação ou ângulos DOA. São necessárias 3 estações RX  $S_1$ ,  $S_2$  e  $S_3$  que recebem a onda EM irradiada pelo TX  $T$ , conforme (A) abaixo. A onda EM demora respectivamente  $t_1$ ,  $t_2$  e  $t_3$  para se propagar do TX  $T$  até as estações  $S_1$ ,  $S_2$  e  $S_3$ .



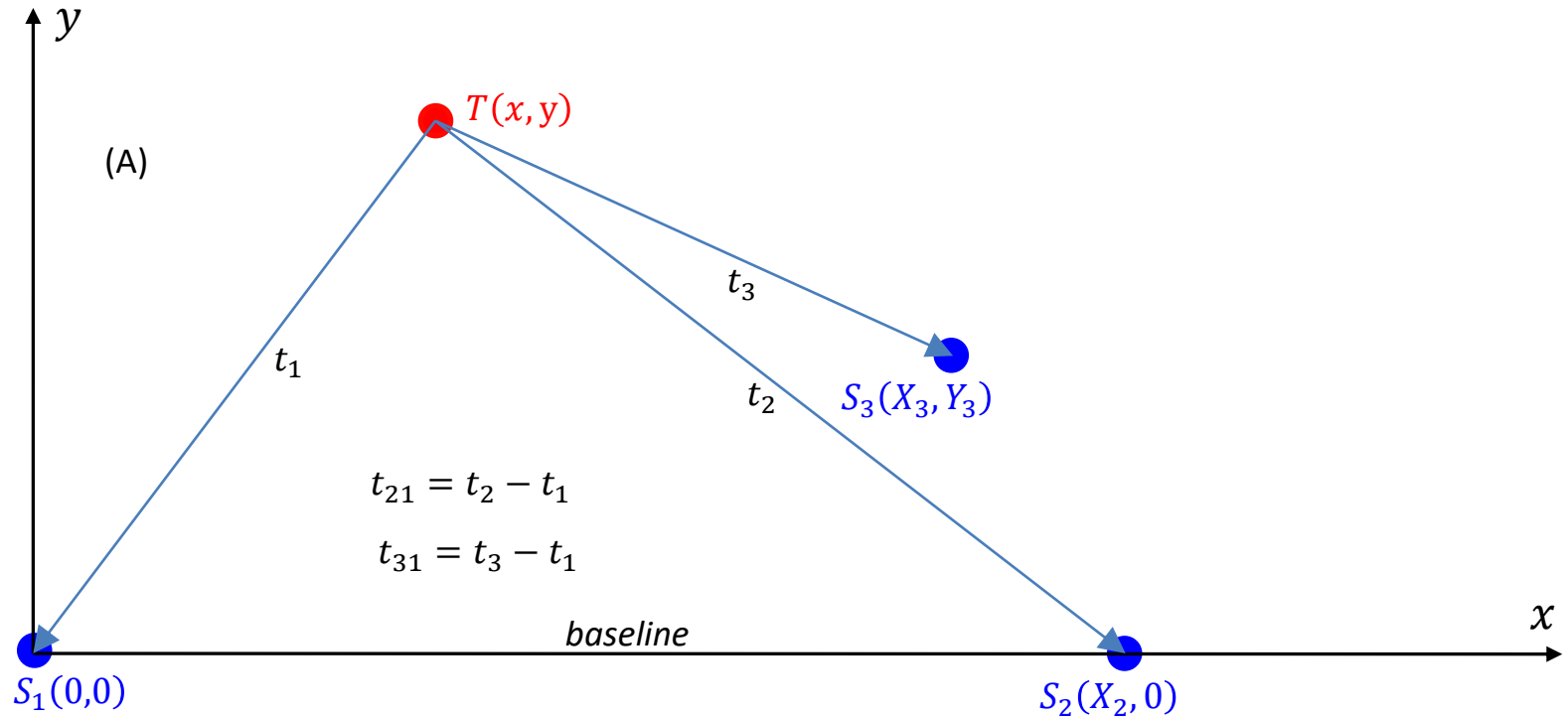
$S_1$  é a estação de controle e, no método de Fang (que discutiremos a seguir), é situada na origem  $(x, y)$  do sistema de coordenadas. As estações  $S_1$  e  $S_2$  formam uma *baseline* de tamanho  $X_2$  ao longo do eixo  $x$ , conforme mostrado em (A). A estação  $S_3$  está localizada em uma coordenada  $(X_3, Y_3)$  qualquer. No instante  $t = 0$  as estações  $S_1$ ,  $S_2$  e  $S_3$  iniciam simultaneamente e em sincronismo o processo de digitalização e gravação dos sinais respectivos  $s_1(t)$ ,  $s_2(t)$  e  $s_3(t)$  recebidos do TX inimigo  $T$ .

O instante  $t = 0$  é precisamente sincronizado entre as estações  $S_1$ ,  $S_2$  e  $S_3$ , sendo este sincronismo usualmente obtido através do sinal de referência de tempo do sistema GPS ([https://en.wikipedia.org/wiki/GPS\\_signals#Time](https://en.wikipedia.org/wiki/GPS_signals#Time)).

As estações  $S_2$  e  $S_3$  enviam para a estação de controle  $S_1$  os respectivos sinais  $s_2(t)$  e  $s_3(t)$  que foram por elas digitalizados e gravados a partir do instante  $t = 0$ . O envio é usualmente feito por um enlace de microondas encriptado. Daí, a estação de controle  $S_1$  determina a correlação  $R_{12}(\tau)$  entre  $s_1(t)$  e  $s_2(t)$  e determina a correlação  $R_{13}(\tau)$  entre  $s_1(t)$  e  $s_3(t)$ , conforme vimos no Exemplo 11 do slide 99. Obtidos  $R_{12}(\tau)$  e  $R_{13}(\tau)$  a estação  $S_1$  determina as diferenças de tempo  $t_{21} = t_2 - t_1$  e  $t_{31} = t_3 - t_1$  através de  $t_{21} = \arg \max_{(\tau)} \{R_{12}(\tau)\}$  e  $t_{31} = \arg \max_{(\tau)} \{R_{13}(\tau)\}$ , conforme visto no Exemplo 11. Obtidas as diferenças  $t_{21}$  e  $t_{31}$  do tempo de propagação da onda EM, há vários métodos para determinar as coordenadas  $(x, y)$  do TX inimigo  $T$  (ver <http://www.fccdecastro.com.br/pdf/HPLEMPE.pdf>). Neste estudo adotaremos o método de Fang (ver <http://www.fccdecastro.com.br/pdf/SSHRPF.pdf>), conforme veremos no exemplo do próximo slide.

## TDOA - Time Difference Of Arrival

**Exemplo 12:** A estação de controle  $S_1$  do sistema TDOA em (A) abaixo determinou  $t_{21} = \arg \max_{(\tau)} \{R_{12}(\tau)\} = 9.017 [\mu\text{s}]$  e  $t_{31} = \arg \max_{(\tau)} \{R_{13}(\tau)\} = -4.431 [\mu\text{s}]$ . A estação  $S_2$  está distante da estação  $S_1$  de  $X_2 = 14.54 [\text{Km}]$ . A estação  $S_3$  está localizada na coordenada  $(X_3, Y_3) = (12.25, 3.99) [\text{Km}]$ .



Sabendo que as estações  $S_1$ ,  $S_2$  e  $S_3$  estão sincronizadas através do sinal de referência de tempo do sistema GPS, use o método de Fang (ver <http://www.fccdecastro.com.br/pdf/HPLEMPE.pdf> e <http://www.fccdecastro.com.br/pdf/SSHRPF.pdf>) para determinar as coordenadas  $(x, y)$  do TX inimigo  $T$ .

## TDOA - Time Difference Of Arrival

Solução:

$$t_{21} := t_2 - t_1 = 9.017 \cdot \mu\text{s} \quad \rightarrow \quad R_{21} := c \cdot t_{21} = 2.703 \cdot \text{km}$$

$$X_2 := 14.54 \text{ km}$$

$$t_{31} := t_3 - t_1 = -4.431 \cdot \mu\text{s} \quad \rightarrow \quad R_{31} := c \cdot t_{31} = -1.328 \cdot \text{km}$$

$$X_3 := 12.25 \text{ km} \quad Y_3 := 3.99 \text{ km}$$

$$c = 2.9979246 \times 10^8 \frac{\text{m}}{\text{s}}$$

$$g_- := \frac{R_{31} \cdot \left( \frac{X_2}{R_{21}} \right) - X_3}{Y_3} = -4.861$$

$$h := \frac{X_3^2 + Y_3^2 - R_{31}^2 + R_{31} \cdot R_{21} \cdot \left[ 1 - \left( \frac{X_2}{R_{21}} \right)^2 \right]}{2 \cdot Y_3} = 33.148 \text{ km}$$

$$d := \left[ 1 - \left( \frac{X_2}{R_{21}} \right)^2 + g_-^2 \right] = 4.304$$

$$e_- := X_2 \cdot \left[ 1 - \left( \frac{X_2}{R_{21}} \right)^2 \right] - 2 \cdot g_- \cdot h = -83.883 \text{ km}$$

$$f := \frac{R_{21}^2}{4} \cdot \left[ 1 - \left( \frac{X_2}{R_{21}} \right)^2 \right]^2 - h^2 = 326.53 \text{ km}^2$$

$$x := \frac{-e_- - \sqrt{e_-^2 - 4 \cdot d \cdot f}}{2 \cdot d} = 5.375 \cdot \text{km}$$

$$y := g_- \cdot x + h = 7.02 \cdot \text{km}$$

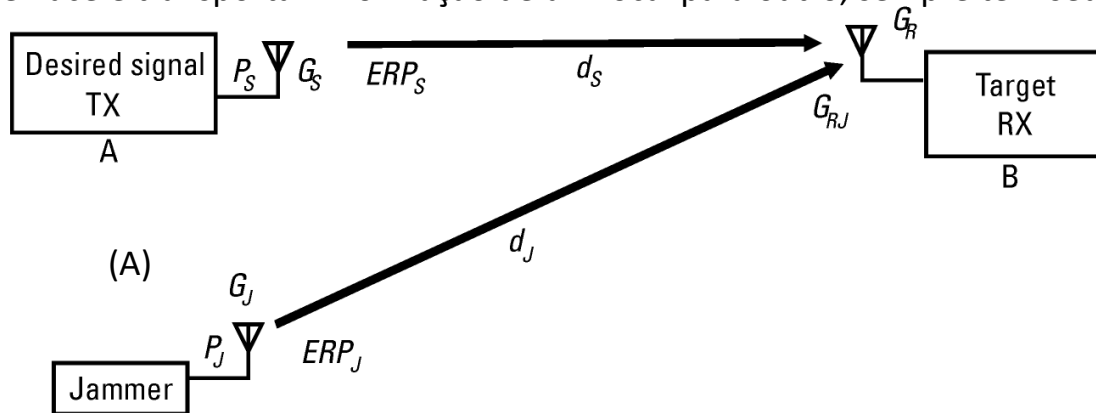
## TDOA - *Time Difference Of Arrival*

FDOA (*Frequency Difference Of Arrival* - ver <https://en.wikipedia.org/wiki/FDOA>) é uma técnica de alta precisão alternativa/complementar à TDOA. No entanto FDOA tem a desvantagem operacional de exigir que as estações RX estejam em movimento para efeito de gerar desvio Doppler, o que nem sempre é possível em um cenário operacional de EW.

## Jamming

Neste capítulo estudaremos o processo de *jamming*, ou simplesmente *jamming*, de enlaces de comunicações. O *jamming* de sistemas de radar será estudado no Cap 3 desta disciplina.

O objetivo básico do *jamming* de enlaces de comunicação é impedir a transferência de informação. Os requisitos para o *jamming* de enlaces dependem da modulação do sinal, da geometria do enlace, dos parâmetros (padrão de irradiação e polarização) das antenas envolvidas na dada geometria, da potência do sinal transmitido pelo TX do enlace e da potência transmitida pelo TX do *jammer*. Em (A) é mostrado o diagrama da geometria típica para o *jamming* de um enlace A→B de comunicação, onde no local A está situado o TX do enlace e onde no local B está situado o RX do enlace. Note que um radar típico tem o TX e o RX a ele associado ambos situados no mesmo local. Já um enlace de comunicação, dado que a função do enlace é transportar informação de um local para outro, sempre tem seu RX situado em um local diferente daquele do TX.

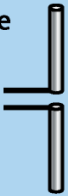

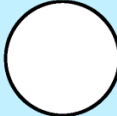
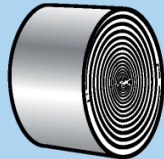
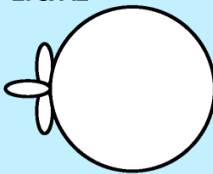
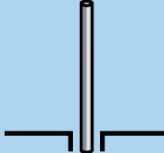


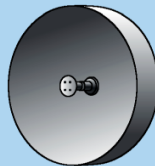


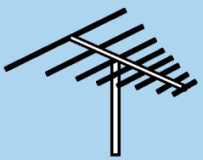
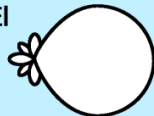





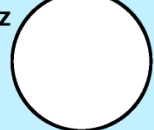
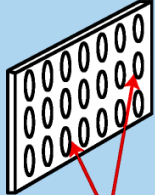


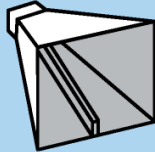




Note que o *jamming* é efetuado sobre o RX do enlace em (A), e não sobre o TX. Um enlace é, em geral, estabelecido através de transceptores localizados nas extremidades do enlace (cada um incluindo o TX e o RX para viabilizar comunicação bidirecional), mas em (A) apenas o RX (*target* – alvo) no local B está sofrendo *jamming* pelo sinal do *jammer*.

Se dois transceptores estiverem em uso e quisermos efetuar o *jamming* do enlace na outra direção (direção B→A) o *jammer* deverá apontar o *boresight* (direção de maior ganho de irradiação) do padrão de irradiação de seu *array* de antenas (estudaremos *arrays* no Cap 2 desta disciplina) para o local A de modo a focalizar a energia da onda EM irradiada no local onde encontra-se situado o RX. Ainda, o *jammer* deve ajustar a polarização de sua antena de modo que a polarização da onda EM irradiada seja compatível com a polarização da antena do RX do enlace, caso contrário o *jamming* será inefetivo. Neste contexto, quanto mais diretivo for o padrão de irradiação da antena do RX do enlace e quanto mais específica for sua polarização menores serão as chances de sucesso do *jammer*. A máxima chance de sucesso do *jamming* ocorre na situação em que a onda EM irradiada pelo *jammer* incide na antena RX do enlace na direção do *boresight* do padrão de irradiação da antena RX ou na situação em que a antena do RX do enlace tem um padrão de irradiação omnidirecional. A tabela no próximo slide mostra diversos tipos usuais de antenas para EW, seu ganho e *beamwidth* no *boresight* e polarização, entre outros parâmetros.

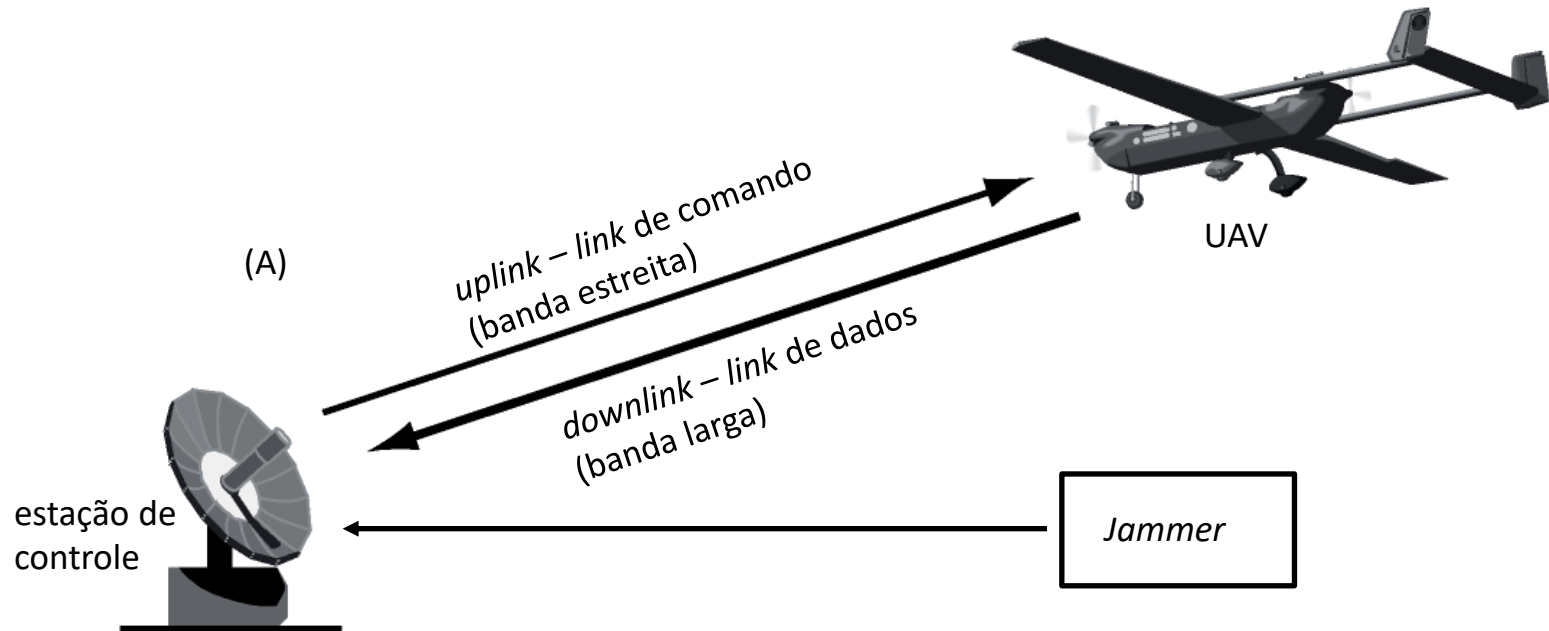


# A Sampling of Typical EW Antenna Types, Patterns, and Specifications

Antenna Type	Pattern	Typical Specifications	Antenna Type	Pattern	Typical Specifications
<b>Dipole</b> 	EI  Az 	<b>Polarization:</b> Aligned with element orientation <b>Beamwidth:</b> 80° x 360° <b>Gain:</b> 2 dB <b>Bandwidth:</b> 10% <b>Frequency Range:</b> Zero through $\mu\text{W}$	<b>Cavity-backed Spiral</b> 	EI & Az 	<b>Polarization:</b> R & L Circular <b>Beamwidth:</b> 60° x 60° <b>Gain:</b> -15 dB (min freq); +3 dB (max freq) <b>Bandwidth:</b> 9 to 1 <b>Frequency Range:</b> UHF through $\mu\text{W}$
<b>Monopole</b> 	EI  Az 	<b>Polarization:</b> Vertical <b>Beamwidth:</b> 45° x 360° <b>Gain:</b> 5 dB <b>Bandwidth:</b> 10% <b>Frequency Range:</b> HF through UHF	<b>Splash Plate</b> 	EI  Az 	<b>Polarization:</b> Any <b>Beamwidth:</b> 20° x 20° <b>Gain:</b> 20 dB <b>Bandwidth:</b> <b>Frequency Range:</b> $\mu\text{W}$
<b>Log Periodic</b> 	EI  Az 	<b>Polarization:</b> Vertical or Horizontal <b>Beamwidth:</b> 80° x 60° <b>Gain:</b> 6 to 8 dB <b>Bandwidth:</b> 10 to 1 <b>Frequency Range:</b> HF through $\mu\text{W}$	<b>Parabolic Dish</b> 	EI & Az 	<b>Polarization:</b> Depends on feed <b>Beamwidth:</b> 0.5° to 30° <b>Gain:</b> 10 to 55 dB <b>Bandwidth:</b> Depends on feed <b>Frequency Range:</b> UHF through $\mu\text{W}$
<b>Biconical</b> 	EI  Az 	<b>Polarization:</b> Vertical <b>Beamwidth:</b> 20° to 100° x 360° <b>Gain:</b> 0 to 4 dB <b>Bandwidth:</b> 4 to 1 <b>Frequency Range:</b> UHF through mmw	<b>Phased Array</b> 	EI  Az 	<b>Polarization:</b> Depends on feed <b>Beamwidth:</b> 0.5° to 30° <b>Gain:</b> 10 to 40 dB <b>Bandwidth:</b> Depends on elements <b>Frequency Range:</b> VHF through $\mu\text{W}$
<b>Horn</b> 	EI  Az 	<b>Polarization:</b> Linear <b>Beamwidth:</b> 40° x 40° <b>Gain:</b> 5 to 10 dB <b>Bandwidth:</b> 4 to 1 <b>Frequency Range:</b> VHF through mmw			

## Jamming

O *jamming* do enlace de UAVs (*Unmanned Aerial Vehicle*) é uma ação de EA de particular importância em um cenário operacional de EW. Em (A) é mostrada uma geometria típica para o *jamming* do *downlink* de um UAV militar. Note que neste caso não há transceptores – a comunicação é unidirecional. Novamente, note em (A) que o RX da estação de controle é quem está sofrendo *jamming*. Ver também <https://www.thesignaljammer.com/blog/how-a-drone-jammer-can-help-with-security/> e <https://www.thesignaljammer.com/blog/everything-you-need-to-know-about-drone-jammers/>.



## Jamming-to-Signal Ratio – $J/S$

O processo de *jamming* de um enlace de comunicações inimigo é considerado eficaz quando o fluxo de informações entre TX e RX do enlace é efetivamente interrompido. O mecanismo pelo qual um *jammer* interfere no enlace de comunicação é através da injeção de um sinal disruptivo no RX alvo simultaneamente com quaisquer sinais desejados que estão sendo recebidos pelo RX inimigo. O sinal disruptivo deve ser suficientemente intenso para que o RX fique impossibilitado de demodular a informação recebida com a necessária inteligibilidade. A razão entre a potência  $J$  do sinal de *jamming* e a potência  $S$  do sinal desejado (sendo  $J$  e  $S$  medidos nas vizinhanças do RX alvo) é denominada de *jamming-to-signal ratio* ( $J/S$ ).  $J/S$  é comumente dado em [dB], i.e.,  $J/S = 10 \log\left(\frac{J}{S}\right)$  [dB].

O valor mínimo de  $J/S$  requerido para o *jamming* efetivo do enlace inimigo depende da modulação transmitida. No entanto, a determinação do  $J/S$  independe da modulação e é dada por:

$$J/S = ERP_J - ERP_S - L_J + L_S + G_{RJ} - G_R \quad (34)$$

onde  $J/S$  é a razão entre a potência  $J$  do sinal de *jamming* e a potência  $S$  do sinal desejado (sendo  $J$  e  $S$  medidos nas vizinhanças do RX alvo) em [dB]

$ERP_J = P_J + G_J$  é a potência efetiva irradiada pelo TX do *jammer* em [dBm], onde  $P_J$  é a potência do TX do *jammer* em [dBm] e onde  $G_J$  é o ganho em [dBi] na direção do *boresight* da antena do TX do *jammer*. Ver diagrama (A) no slide 108.

**Nota:** Uma potência  $P$  expressa em [W] é expressa em [dBm] através de  $P[\text{dBm}] = 10 \log(P[\text{W}]/(10^{-3}))$  (35)

$ERP_S = P_S + G_S$  é a potência efetiva irradiada pelo TX do enlace em [dBm], onde  $P_S$  é a potência do TX do enlace em [dBm] e onde  $G_S$  é o ganho em [dBi] na direção do *boresight* da antena do TX do enlace. Ver diagrama (A) no slide 108.

$L_J$  é perda de potência em [dB] no caminho de propagação  $d_J$  da onda EM irradiada pelo *jammer* até o local do RX do enlace. Por exemplo, em (A) no slide 108 se houver linha de visada direta entre a antena do *jammer* e a antena do RX do enlace e se não houver ocorrência de multipercurso, então  $L_J = 32.44 + 20 \log(d_J) + 20 \log(f)$ , onde  $d_J$  é a distância entre o *jammer* e o RX do enlace em [Km] e  $f$  em [MHz] é a frequência de operação do enlace (ver [https://en.wikipedia.org/wiki/Free-space\\_path\\_loss](https://en.wikipedia.org/wiki/Free-space_path_loss)).

$L_S$  é perda de potência em [dB] no caminho de propagação  $d_S$  da onda EM irradiada pelo TX até o local do RX do enlace (ver (A) no slide 108).

$G_{RJ}$  é o ganho da antena RX na direção do *jammer* em [dBi].

$G_R$  é o ganho da antena RX na direção do TX do enlace em [dBi].

As perdas de propagação  $L_J$  e  $L_S$  dependem da situação operacional. A situação mais simples e usual é a operação sob linha de visada sem multipercurso (ver [https://en.wikipedia.org/wiki/Free-space\\_path\\_loss](https://en.wikipedia.org/wiki/Free-space_path_loss)). No entanto há inúmeros cenários de operação, e cada cenário demanda uma abordagem específica para determinar as perdas de propagação (ver [https://en.wikipedia.org/wiki/Radio\\_propagation](https://en.wikipedia.org/wiki/Radio_propagation)).

Uma aproximação usual em EA, em particular para *Stand-in Jamming* (ver próximo slide) em ambiente urbano e para enlaces em terreno tropical úmido, é o cenário de propagação sob multipercurso gerado por um único ponto de reflexão no canal entre TX e RX. Neste caso a perda de propagação em [dB] pode ser aproximada por  $L = 120 + 40 \log(d) - 20 \log(h_T) - 20 \log(h_R)$ , onde  $d$  é a distância entre a antena do TX (do enlace ou do *jammer*) e a antena do RX do enlace em [Km],  $h_T$  é a altura do solo da antena do TX em [m] e  $h_R$  é a altura do solo da antena do RX em [m] (ver [https://en.wikipedia.org/wiki/Two-ray\\_ground-reflection\\_model](https://en.wikipedia.org/wiki/Two-ray_ground-reflection_model) )

Se há obstrução no caminho de propagação será necessário verificar a liberação (*clearance*) da 1ª zona de Fresnel ([https://en.wikipedia.org/wiki/Fresnel\\_zone#Clearance](https://en.wikipedia.org/wiki/Fresnel_zone#Clearance)). Em não havendo *clearance* suficiente da 1ª zona de Fresnel será necessário modelar a atenuação da obstrução. Obstruções geradas por objetos difratores do tipo gume de faca (*knife edge*) são modeladas pelos métodos de Bullington, Epstein-Peterson ou Deygout (ver <http://www.wirelesscommunication.nl/reference/chaptr03/diffrac.htm> ).

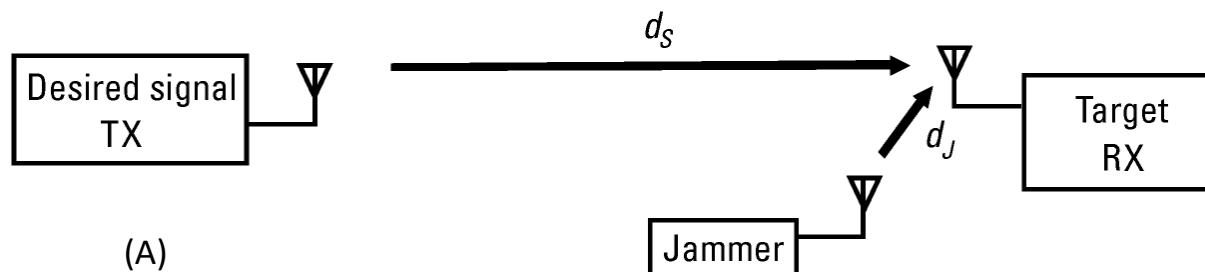
## Stand-In Jamming

*Stand-in Jamming* é uma geometria em que o *jammer* é posicionado próximo ao RX alvo, conforme mostrado em (A) abaixo. A redução da distância  $d_j$  do *jammer* ao RX alvo aumenta o  $J/S$  pelo quadrado da redução da distância.

Para um dado  $J/S$  necessário para efetivamente interromper o fluxo de informações entre TX e RX do enlace inimigo, esta técnica permite que seja utilizada menor potência no TX do *jammer*, mantendo o valor de  $J/S$  obtido no RX do enlace. Uma vantagem adicional é que os RXs de facções amigas - que estão presumivelmente muito mais distantes do *jammer* do que o RX inimigo alvo - não sofrerão efeitos do *jamming*. Isso evita o fratricídio (*jamming* não intencional das comunicações de facções amigas).

Técnicas de *Stand-in Jamming* incluem *emplaced jammers* (<https://fas.org/man/dod-101/sys/land/docs/960800-kornuta.htm>), *payloads* de UAVs específicos para *jamming* (<https://www.c4isrnet.com/newsletters/unmanned-systems/2018/11/16/russian-drones-can-jam-cell-phones-60-miles-away/>), *jammers* transportados por aeronaves (<https://worldofweapon.wordpress.com/2017/04/22/us-navy-next-generation-jammer-threatens-to-blind-chinas-a2ad-network-in-south-china-sea/>) e *jammers* levados às vizinhanças do alvo através de projéteis de artilharia (<https://www.samel90.com/en/products/category/jammer-solutions-military-equipment-surveillance-systems/artillery-jammers>).

O *Stand-in Jamming* pode ser particularmente vantajoso contra sinais LPI do tipo DS-SS, sinais que apresentam baixa suscetibilidade ao *jamming* em consequência da necessidade do *jammer* gerar no RX um  $J/S$  suficientemente alto para superar o ganho de processamento do RX DS-SS, conforme já discutido no slide 81. O maior  $J/S$  resultante da geometria *Stand-in Jamming* pode superar o ganho de processamento do RX DS-SS e o *jammer* pode efetivamente conseguir interromper o fluxo de informações entre TX e RX do enlace inimigo.



## Jamming de enlaces analógicos e digitais

Para efetuar o *jamming* de enlaces analógicos, em particular os enlaces que transportam sinal de voz, é necessário uma razão  $J/S$  de pelo menos 10 [dB] com *duty cycle* 100% no TX do *jammer* (i.e., sem interrupção). Isso ocorre porque o operador humano do enlace tem uma capacidade cognitiva adaptativa, inferindo pelo contexto os trechos da informação de voz que foram degradados pelo *jammer*. Mesmo em enlaces analógicos de vídeo este comportamento está presente, dada a capacidade do operador humano em inferir partes do vídeo que foram corrompidas pelo sinal do *jammer*. Isso é particularmente verdadeiro na comunicação militar tática, onde as informações críticas são enviadas em formatos padronizados que facilitam a inferência. Exemplos disto são o padrão de escrita em 5 parágrafos das ordens de operações (ver [https://en.wikipedia.org/wiki/Five\\_paragraph\\_order](https://en.wikipedia.org/wiki/Five_paragraph_order) e as páginas 2-9 e E-1 de <https://bdex.eb.mil.br/jspui/bitstream/123456789/4025/1/EB60-ME-13.301%20TRABALHO%20DE%20COMANDO%202%20C%AA%20Edi%20C%3%A7%20C%3%A3o%202019.pdf> ) e o alfabeto fonético militar (ver [https://pt.wikipedia.org/wiki/Alfabeto\\_fon%C3%A9tico\\_da\\_OTAN](https://pt.wikipedia.org/wiki/Alfabeto_fon%C3%A9tico_da_OTAN) ).

No caso do *jamming* de enlaces digitais, o sinal do *jammer* interfere no sinal desejado causando a disrupção do RX do enlace da facção inimiga através do aumento significativo da taxa de erro de bits (BER - *Bit Error Rate* – [https://en.wikipedia.org/wiki/Bit\\_error\\_rate](https://en.wikipedia.org/wiki/Bit_error_rate) ) na saída do *de-mapper* do demodulador digital do RX (ver slides 19 e 20 de [http://www.fccdecastro.com.br/pdf/T2\\_Aula10&11\\_22042020.pdf](http://www.fccdecastro.com.br/pdf/T2_Aula10&11_22042020.pdf) ). A partir de um determinado número máximo de bits errados contíguos na sequência de bits na saída do *de-mapper* fica inviabilizada a correção dos bits errados pelo código corretor de erro no decodificador de canal do RX digital (ver [http://www.fccdecastro.com.br/pdf/T2\\_Aula7\\_01042020.pdf](http://www.fccdecastro.com.br/pdf/T2_Aula7_01042020.pdf), [http://www.fccdecastro.com.br/pdf/T2\\_Aula8\\_03042020.pdf](http://www.fccdecastro.com.br/pdf/T2_Aula8_03042020.pdf) e [http://www.fccdecastro.com.br/pdf/T2\\_Aula9\\_15042020.pdf](http://www.fccdecastro.com.br/pdf/T2_Aula9_15042020.pdf) ).

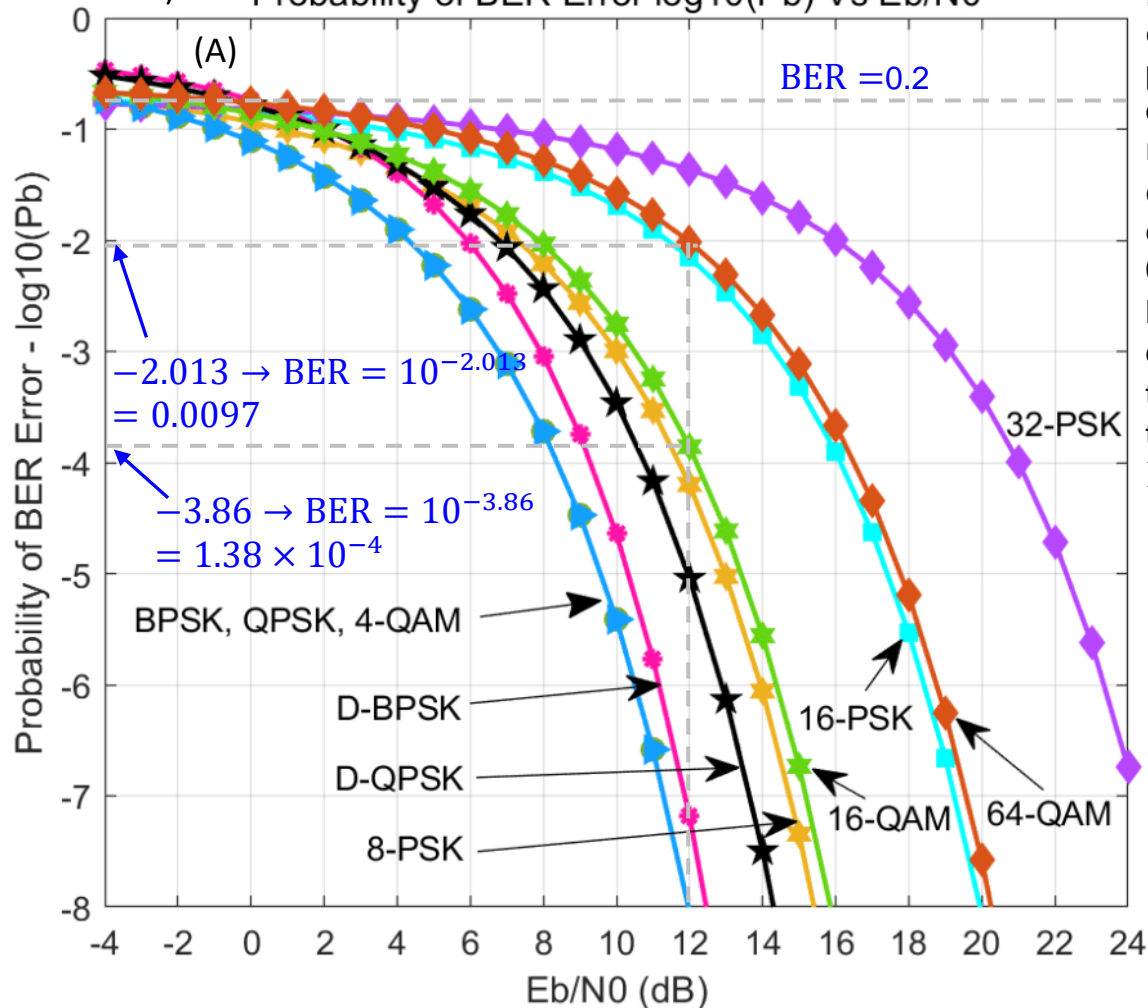
O limiar de  $J/S$  a partir do qual ocorre a falha do código corretor de erro no RX inimigo é o nível mínimo de  $J/S$  em que começa o *jamming* efetivo do enlace. A disrupção completa do RX do enlace ocorrerá em um nível maior de  $J/S$  , acima do limiar mínimo de  $J/S$ , situação em que o grande número de bits errados na saída do decodificador de canal torna ininteligível a informação transportada pelo sinal desejado recebido no RX do enlace. Estes dois limiares de  $J/S$  dependem basicamente do tipo de modulação digital adotada e do tipo de código corretor de erro adotado no enlace, ambos determinando a curva de desempenho  $BER \times Eb/No$  do enlace, sendo  $Eb/No$  a relação sinal-ruído por bit transportado pela modulação digital. Assumindo um *noise figure* ideal de 0 [dB] no *front-end* analógico do RX ([https://en.wikipedia.org/wiki/Noise\\_figure](https://en.wikipedia.org/wiki/Noise_figure) ), a relação entre o  $Eb/No$  na entrada do *de-mapper* e a SNR (*signal to noise ratio*) medida na entrada do *front-end* analógico do RX (denominada  $C/N$  – *carrier to noise ratio* ) é dada por  $C/N = Eb/No \times BitRate/BW$ , onde  $BitRate$  é a taxa de transmissão no canal em [bps] e  $BW$  é a banda de passagem do filtro do amplificador de FI do RX em [Hz] (<https://en.wikipedia.org/wiki/Eb/No>).



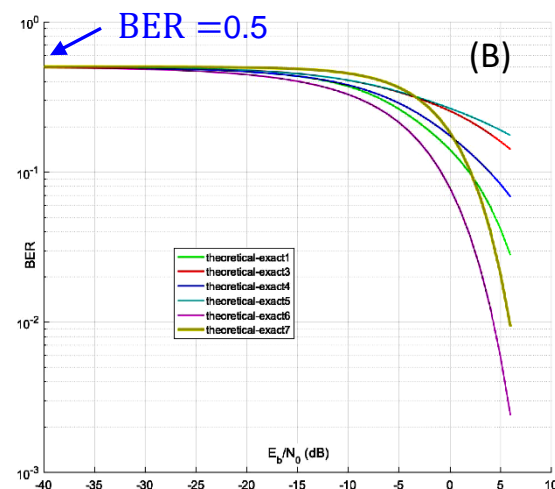
## Jamming de enlaces analógicos e digitais

O gráfico em (A) abaixo, gerado pelo script Matlab no Apêndice A (alternativamente pode ser gerado pelo BERTool/BERAnalyzer do Matlab - <https://www.mathworks.com/help/comm/ref/beranalyzer-app.html> ) mostra a BER na saída do *de-mapper* do RX (sem considerar os códigos corretores de erro) para diversas modulações digitais usuais, em função da relação sinal ruído  $E_b/N_0$ . Por exemplo, para uma relação sinal-ruído  $E_b/N_0 = 12$  [dB] a modulação 16-QAM apresenta  $BER = 1.38 \times 10^{-4}$  (138 bits errados na saída do *de-mapper* a cada 1 milhão de bits recebidos) e a modulação 64-QAM apresenta  $BER = 10^{-2.013} = 0.0097$  (9700 bits errados na saída do *de-mapper* a cada 1 milhão de bits recebidos).

Probability of BER Error  $\log_{10}(P_b)$  Vs  $E_b/N_0$



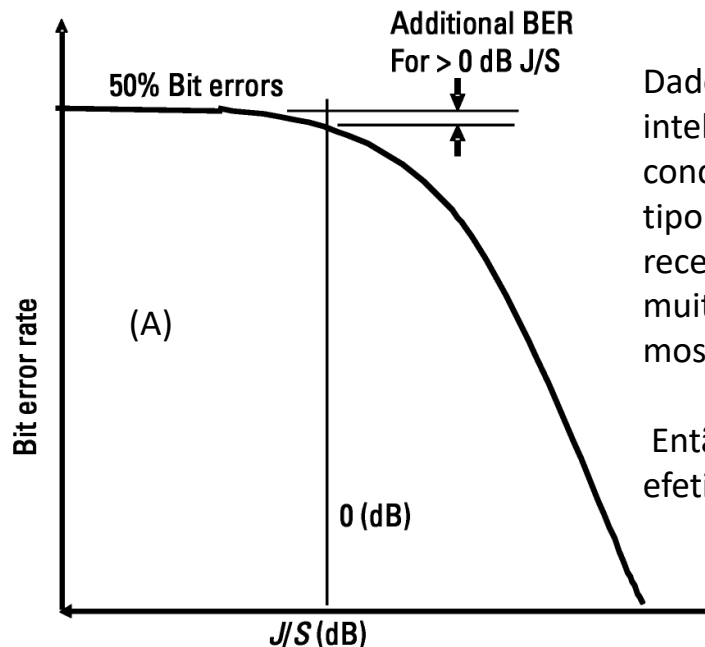
Portanto um enlace que utiliza modulação 64-QAM é mais “frágil” ao ruído do que um enlace 16-QAM porque 64-QAM resulta BER não nula com um nível de ruído menor do que é necessário para 16-QAM resultar BER não nula. Consequentemente o nível de  $J/S$  necessário para efetuar o *jamming* de um enlace 16-QAM será maior de que para um enlace 64-QAM. Note em (A) que há uma relação não linear entre a relação sinal-ruído  $E_b/N_0$  na entrada do *de-mapper* do RX e a BER na sua saída. Note também que à medida em que  $E_b/N_0$  é reduzido todas as curvas de BER convergem para o valor  $BER = 0.5$ , conforme mostrado em (B):



## Jamming de enlaces analógicos e digitais

Note também em (A) do slide anterior que todas as curvas resultam em uma taxa de erro de bits  $BER \cong 0.2$  para  $E_b/N_0 = 0$  [dB], BER que não é muito diferente do valor limite de  $BER = 0.5$  obtido para  $E_b/N_0 = -40$  [dB] ou menor, conforme mostrado em (B) do slide anterior. Isso significa que, independentemente do tipo de modulação usada, comparando as situações  $E_b/N_0 = 0$  [dB] e  $E_b/N_0 = -40$  [dB] para, por exemplo, 1024 bits recebidos (apenas 128 bytes recebidos – um único *frame* de qualquer sistema de comunicação usual é maior que 128 bytes – ver próximo slide), teremos 205 bits errados para  $E_b/N_0 = 0$  [dB] e 512 bits errados para  $E_b/N_0 = -40$  [dB]. Estes apenas 307 bits adicionais a serem corrigidos pelo código corretor de erro do RX para  $E_b/N_0 = -40$  [dB] não farão muita diferença na capacidade de correção do código corretor porque, para uma BER tão alta quanto 0.2 ou quanto 0.5 o código corretor já estará operando além do limite da sua capacidade de correção de blocos de bits errados que ocorrem de forma sequencialmente contígua.

Por exemplo, consideremos um código corretor de erro Reed-Solomon  $RS(n = 204, k = 188, t = 8)$  (ver [https://en.wikipedia.org/wiki/Reed%E2%80%93Solomon\\_error\\_correction](https://en.wikipedia.org/wiki/Reed%E2%80%93Solomon_error_correction)), que é um código largamente utilizado em sistemas sem fio. Este código é capaz de corrigir  $0.5 \times (n - k) \times t = 0.5 \times (204 - 188) \times 8 = 64$  bits errados consecutivos, e portanto não é capaz de corrigir os 205 bits errados para  $E_b/N_0 = 0$  [dB] nem tampouco os 512 bits errados para  $E_b/N_0 = -40$  [dB]. Ou seja, para  $E_b/N_0 = 0$  [dB] ( $BER = 0.2$ ) qualquer código corretor de erro já deixou de ser efetivo.



Dado que o efeito do *jamming* é o mesmo do ruído (a degradação da inteligibilidade do sinal desejado pela adição de um sinal indesejado), mesma conclusão pode ser inferida para o processo de *jamming*: Independentemente do tipo de modulação usada, se o nível do sinal do *jammer* for igual ao nível do sinal recebido pela antena do RX ( $J/S = 0$  [dB]), a BER no RX inimigo não aumentará muito mais se aumentarmos o  $J/S$  para valores acima de 0 [dB], conforme mostrado em (A).

Então  $J/S = 0$  [dB] é considerado o limiar mínimo para que o *jamming* ocorra efetivamente.

## Jamming de enlaces analógicos e digitais

Com relação ao *duty-cycle* do TX do *jammer*, um sinal digital é considerado ininteligível se  $1/3 = 33.3\%$  da duração de cada *frame* de dados transmitido for completamente degradado pelo sinal do *jammer* (ver [https://en.wikipedia.org/wiki/Frame\\_\(networking\)](https://en.wikipedia.org/wiki/Frame_(networking)) e [https://en.wikipedia.org/wiki/Data\\_transmission](https://en.wikipedia.org/wiki/Data_transmission) ). Este valor  $33.3\%$  foi determinado experimentalmente da observação da operação de enlaces digitais. Isso significa que o TX do *jammer* pode usar um *duty-cycle* de  $1/3$  com uma duração de cada ciclo de *jamming* sendo aproximadamente igual a duração do *frame* do enlace digital, desde que a potência do TX do *jammer* resulte em no mínimo  $J/S = 0$  [dB] na antena do RX do enlace inimigo.

Note que quanto menor o *duty-cycle* no TX do *jammer* menor será a potência necessária para alimentar o TX, o que pode ser um requisito crucial para a autonomia da bateria de unidades móveis no âmbito de *Stand-in Jamming* (ver slide 113).

Quando o TX e o RX do enlace inimigo adota códigos corretores que incluem *interleaver* (ver <https://www.gaussianwaves.com/2010/10/interleavers-and-deinterleavers-2/>, <https://www.gaussianwaves.com/2010/10/block-interleaver-design-for-rs-codes-2/>) e/ou modulação que inclua *interleaver* (ver slides 100 a 102 de [http://www.fccdecastro.com.br/pdf/T2\\_Aulas21a26\\_26062020.pdf](http://www.fccdecastro.com.br/pdf/T2_Aulas21a26_26062020.pdf) ) será necessário aumentar o *duty-cycle* do TX do *jammer* para pelo menos  $1/2$ , e tanto mais será necessário aumentar o *duty-cycle* quanto maior for a profundidade do *buffer* do *interleaver*.

## Jamming de sinais Spread Spectrum (SS)

Conforme discutimos no Cap 1.3, sinais LPI espalham pseudo-aleatoriamente sua energia em uma banda de frequência  $B$  bem maior do que a banda necessária  $B_s$  para transportar do TX ao RX a informação desejada, sendo a relação entre  $B$  e  $B_s$  dada pelo ganho de processamento do sinal SS, i.e.,  $PG = 10 \log(B/B_s)$  [dB] ([https://en.wikipedia.org/wiki/Process\\_gain](https://en.wikipedia.org/wiki/Process_gain)). O *despreader* no RX do enlace (ver slides 79 e 80), que é sincronizado e casado com o *spreader* do TX do enlace (ver slide 78), recupera o espectro em banda-base de largura  $B_s$  do sinal de informação originalmente transmitido pelo TX, e, portanto, recupera o sinal de informação originalmente transmitido no domínio tempo. Portanto, um *jammer* terá que gerar um J/S capaz de superar o ganho de processamento  $PG$ , o que é algo não trivial de ser realizado. Por exemplo, para um sistema DS-SS com ganho de processamento de 20 [dB] e modulação BPSK será necessário aumentar o J/S em aproximadamente 8.1 [dB] (i.e., implica aumentar 6.5 vezes a potência do TX do *jammer* – e esta abordagem “força bruta” nem sempre é viável em um cenário de EW).

Conforme vimos no Cap 1.3 há três tipos básicos de sinais LPI e todos eles se baseiam em espalhamento espectral: *Frequency hopping*, *Chirp* e *Direct sequence*. Estes três sinais LPI basicamente espalham pseudo-aleatoriamente o espectro do sinal de informação ao longo de uma banda de frequência  $B$  bem maior do que a banda necessária  $B_s$  para transportar do TX ao RX a informação desejada. No entanto, a natureza da distribuição de potência versus frequência versus tempo para cada tipo de sinal e os parâmetros da modulação em banda-base (ainda sem o efeito do espalhamento espectral), determina para cada um destes três sinais LPI uma vulnerabilidade diferente em presença de *jamming*.

Neste contexto, consideremos um sistema SS com ganho de processamento  $PG = 10 \log(B/B_s)$ , sistema que demanda um mínimo valor de relação sinal ruído  $SNR_{\min}$  em [dB] na entrada do *de-mapper*, valor abaixo do qual a BER resulta não nula na saída do *de-mapper* (uma BER maior que  $1 \times 10^{-8}$  é considerada não nula, para fins práticos). Vamos supor que tenhamos determinado a geometria necessária do cenário de *jamming* para que se obtenha  $J/S = 0$  [dB] na antena do RX do enlace inimigo, sendo  $J/S = ERP_J - ERP_S - L_J + L_S + G_{RJ} - G_R$  obtido através de (34). Nesta situação, o  $J/S = 0$  [dB] não será suficiente para efetuar o *jamming* do enlace SS com eficácia, e será necessário adicionar uma margem de folga  $M_J = PG - SNR_{\min}$  ao J/S calculado por (34), denominada *jamming margin*, de modo a levar em consideração o ganho de processamento  $PG$  resultante do espalhamento espectral bem como levar em consideração a fragilidade da modulação digital ao ruído (e conseqüentemente ao *jamming*) medida pela  $SNR_{\min}$  da modulação, conforme exemplo no próximo slide.

## Jamming de sinais Spread Spectrum (SS)

**Exemplo 13:** Seja um enlace SS com  $PG = 30$  [dB] que adota como modulação em banda-base (i.e., antes do *spreader* do TX) a modulação 64-QAM e opcionalmente a modulação 16-QAM. **Pede-se:** Determine para **(a)** 64-QAM e **(b)** 16-QAM o *jamming margin* em [dB] a ser adicionado ao limiar mínimo  $J/S = 0$  [dB] de modo que o *jamming* do RX do enlace SS seja efetuado eficazmente. **(c)** Analise qual encaminhamento para uma efetiva ação de *jamming* do enlace SS em questão.

**Solução:** Do gráfico em (A) no slide 115 note que para  $BER = 1 \times 10^{-8}$  (BER considerada nula) a modulação 64-QAM demanda  $E_b/N_0 = 20.27$  [dB] ou menor enquanto que a modulação 16-QAM demanda  $E_b/N_0 = 15.87$  [dB] ou menor.

Precisamos converter  $E_b/N_0$  em  $E_s/N_0$  na entrada do *de-mapper* através de  $E_s/N_0 = E_b/N_0 + 10 \log(\log_2(M))$  (ver <https://en.wikipedia.org/wiki/Eb/NO>), onde  $M$  refere-se à " $M$ "-QAM e  $E_s/N_0$  é a  $SNR_{\min}$  necessária para que a modulação " $M$ "-QAM opere sob  $BER = 1 \times 10^{-8}$  ou menor na saída do *de-mapper*. Dai, para 64-QAM obtemos  $SNR_{\min} 64QAM = 20.27[\text{dB}] + 10 \log(\log_2(64)) = 28.1$  [dB] e para 16-QAM obtemos  $SNR_{\min} 16QAM = 15.87[\text{dB}] + 10 \log(\log_2(16)) = 21.9$  [dB].

**(a)** O *jamming margin* para 64-QAM resulta  $M_J 64QAM = PG - SNR_{\min} 64QAM = 30$  [dB]  $- 28.1$  [dB] =  $1.9$  [dB]

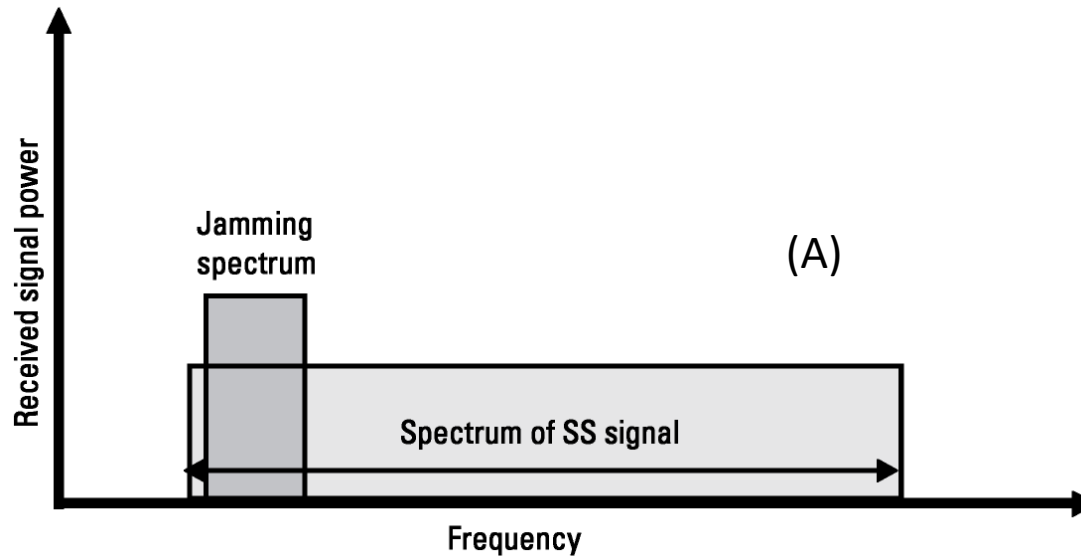
**(b)** O *jamming margin* para 16-QAM resulta  $M_J 16QAM = PG - SNR_{\min} 16QAM = 30$  [dB]  $- 21.9$  [dB] =  $8.1$  [dB]

**(c)** Note, portanto, que o TX do *jammer* para o enlace 64-QAM precisará aumentar sua potência de apenas  $1.9$  [dB] ou reduzir a distância do *jammer* até o RX do enlace SS, ou uma combinação das duas ações desde que o  $J/S$  na antena do RX do enlace SS resulte em no mínimo  $J/S = 1.9$  [dB].

Já o TX do *jammer* para o enlace 16-QAM precisará aumentar sua potência de  $8.1$  [dB] (aumentar a potência em 6.5 vezes) ou reduzir significativamente a distância do *jammer* até o RX do enlace SS (*Stand-In Jamming* – slide 113) de modo que o  $J/S$  na antena do RX do enlace SS resulte em no mínimo  $J/S = 8.1$  [dB]. Dado que um aumento 6.5 vezes na potência do TX do *jammer* pode não ser factível, a melhor solução será efetuar o *Stand-In Jamming*.

## Jamming em banda parcial (*partial band jamming* – PBJ)

PBJ é uma técnica de *jamming* que otimiza o desempenho do *jammer* em relação a sinais SS. Como o nome indica, o PBJ efetua o *jamming* em apenas parte da banda do espectro do sinal SS conforme mostrado em (A):



Conforme discutido no slide 117, a potência do TX do *jammer* deve ser suficiente para que se consiga  $J/S = 0$  [dB] nas vizinhanças do RX inimigo mas o *duty-cycle* do TX do *jammer* pode ser de apenas  $1/3 = 33.3\%$  para que o sinal digital seja considerado ininteligível. Mesma regra pode ser aplicada ao *duty-cycle* no domínio frequência, i.e., o sinal do *jammer* não necessita varrer todo o espectro do sinal SS, bastando interferir apenas uma parte do espectro (em geral,  $1/3$  da totalidade do espectro ou menos), desde que mantido  $J/S = 0$  [dB] em cada frequência interferida.



## Jamming de sinais Frequency Hopping (FH)

Consideremos a situação em que um sinal de *jamming* de onda contínua (CW – *continuous wave*) com uma frequência fixa  $f_c$  (sendo, portanto, um sinal de banda estreita) é transmitido pelo TX do *jammer* na direção do RX de um enlace FH. O RX do enlace salta de frequência em frequência e somente será interferido pelo sinal do *jammer* quando um dos saltos em frequência coincidir com  $f_c$ , situação operacional que reduz significativamente a eficácia do *jamming*.

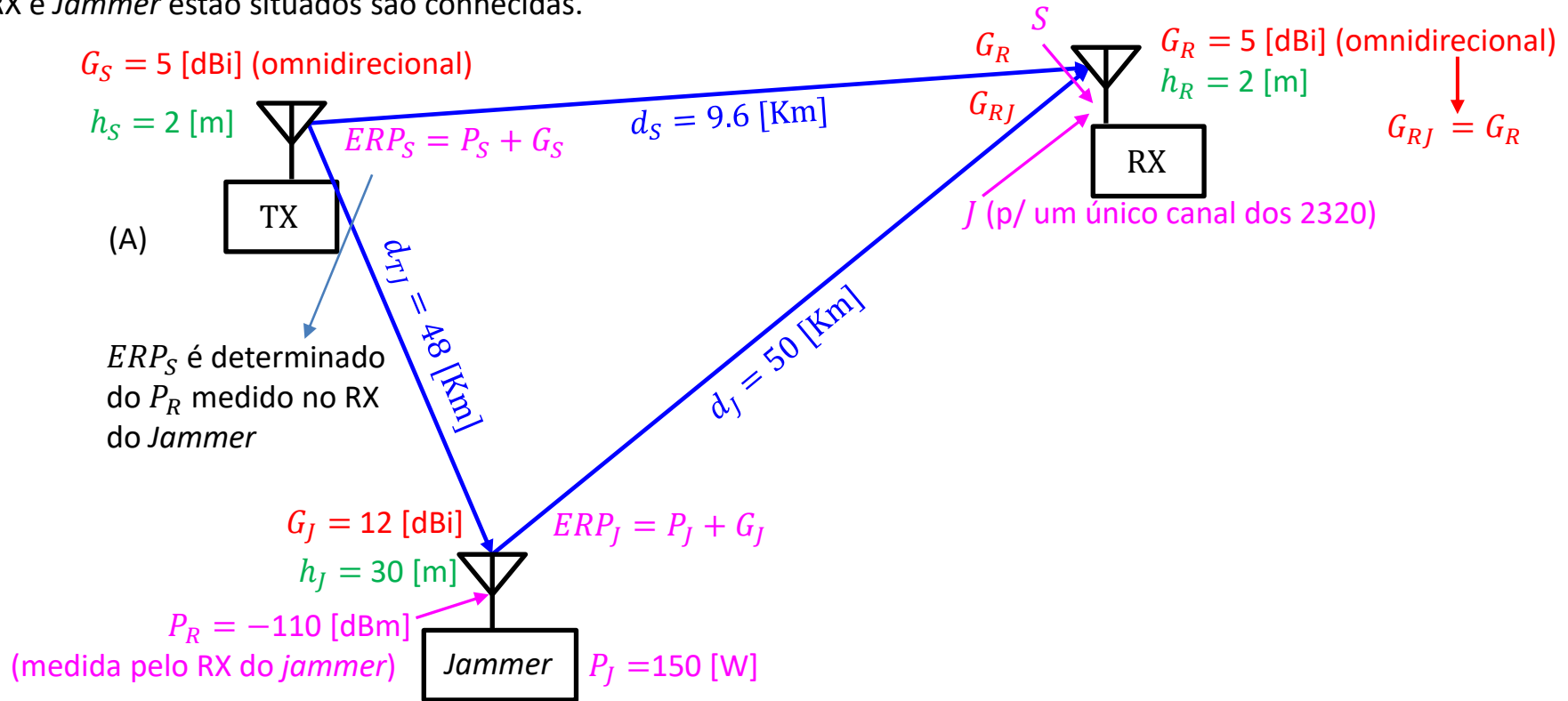
Por exemplo, o clássico sistema Jaguar V (<http://www.fccdecastro.com.br/pdf/JAGUARV.pdf>) opera sob um *hopping range* (ver slide 57) de 58MHz (de 30MHz a 88 MHz), com um máximo de 2320 canais de 25 kHz nesta faixa. O sistema é configurável para 256 e 512 canais de 25KHz, reduzindo respectivamente o *hopping range* para 6.4MHz e 12.8MHz, possibilitando assim evitar a interferência de enlaces de facções amigas. Note que o maior ganho de processamento é obtido com o máximo *hopping range* de 58 MHz :  $PG = 10 \log(58[\text{MHz}]/25[\text{KHz}]) = 33.7$  [dB].

Se um sinal de *jamming* CW for apontado para a antena do RX do sistema Jaguar V (que salta aleatoriamente ao longo dos 2320 canais de 25 kHz distribuídos na faixa entre 30 e 88 MHz), o RX “verá” o sinal de interferência apenas  $100/2320=0.043\%$  do tempo, e portanto apenas 0.043% do *frame* de dados do sistema será interferido (bem distante dos 33.3% usualmente necessário para *jamming* efetivo). Alternativamente, podemos interpretar desta forma: Se o sinal de *jamming* for distribuído por 2320 frequências de canal, o J/S por canal será reduzido de  $PG = 10 \log(2320/1) = 33.7$  [dB], o que reduziria significativamente a eficácia do *jamming*.

Uma possível solução para minimizar a ineficácia do *jamming* devido ao ganho de processamento  $PG$  consiste em adotar a técnica PBJ (*Partial Band Jamming*) conforme discutimos no slide anterior, interferindo em  $1/3 = 33.3\%$  dos canais do *hopping range* sob  $J/S = 0$  [dB] e que analisaremos no exemplo do próximo slide. Alternativamente podemos utilizar a técnica *folower jamming*, que discutiremos adiante neste capítulo.

## Jamming de sinais Frequency Hopping (FH)

**Exemplo 14:** Um sistema FH inimigo opera sob um *hopping range* de 58MHz (de 30MHz a 88 MHz), com  $N_{ch} = 2320$  canais de  $BW = 25$  kHz nesta faixa. Em (A) é mostrado a geometria do cenário de *jamming* para este sistema. As coordenadas onde TX, RX e *Jammer* estão situados são conhecidas.



A potência  $P_J = 150$  [W] é a potência de saída do TX do *jammer*. As antenas têm respectivas alturas  $h$  em relação ao solo e apresentam respectivos ganhos  $G$  na direção do *boresight* de seu diagrama de irradiação. Note que as antenas do TX e do RX do enlace são omnidirecionais no plano do azimute (ver slide 51), de modo que  $G_{RJ} = G_R$  para a antena do RX, sendo  $G_{RJ}$  o ganho da antena RX na direção do *jammer*. O *search receiver* do *jammer* (ver slides 11 e 25) mediu uma potência  $P_R = -110$  [dBm] para o sinal recebido do TX do enlace. Não há obstrução significativa entre as antenas, no entanto o solo é tropical úmido e deve-se esperar desvanecimento por multipercurso em consequência da reflexão no solo condutor da onda EM irradiada pelas respectivas antenas. **Pede-se:** Para a geometria dada em (A) determine a largura da banda parcial  $PB$  para que a mesma seja interferida pelo sinal do *jammer* sob  $J/S = 0$  [dB] e com *duty cycle* de pelo menos 33.3%.

Convertendo a potência do TX do jammer de [W] p/ [dBm]:

$$P_J := 10 \cdot \log\left(\frac{P_J}{1\text{mW}}\right) = 51.8 \text{ [dBm]}$$

Perda de propagação no trajeto TX-Jammer:

$$L_{TJ} := 120 + 40 \cdot \log(d_{TJ}) - 20 \cdot \log(h_S) - 20 \cdot \log(h_J) = 151.7 \text{ [dB]}$$

Potência efetivamente irradiada pela antena do TX do enlace na direção do RX do enlace:

$$ERP_s := P_R - G_J + L_{TJ} = 29.7 \text{ [dBm]}$$

Perda de propagação no trajeto TX-RX do enlace (ver slide 112):

$$L_S := 120 + 40 \cdot \log(d_S) - 20 \cdot \log(h_S) - 20 \cdot \log(h_R) = 147.2 \text{ [dB]}$$

Potência do sinal desejado recebido nos terminais da antena do RX do enlace:

$$S := ERP_s - L_S + G_R = -112.6 \text{ [dBm]}$$

Perda de propagação no trajeto TX do jammer - RX do enlace (ver slide 112):

$$L_J := 120 + 40 \cdot \log(d_J) - 20 \cdot \log(h_J) - 20 \cdot \log(h_R) = 152.4 \text{ [dB]}$$

Potência efetivamente irradiada pela antena do TX do jammer na direção do RX do enlace:

$$ERP_J := P_J + G_J = 63.8 \text{ [dBm]}$$

Potência do sinal do jammer recebido nos terminais da antena do RX do enlace:

$$J := ERP_J - L_J + G_{RJ} = -83.6 \text{ [dBm]}$$

J/S resultante para um único canal de  $BW = 25 \cdot \text{KHz}$  dentre a totalidade de  $N_{ch} = 2320$  canais:

$$J_S := J - S = 28.9 \text{ [dB]}$$

## Jamming de sinais Frequency Hopping (FH)

O J/S para um único canal resultou  $J\_S = 28.9$  [dB], mas precisamos de apenas  $J\_S = 0$  [dB] por canal. Então, para reduzir o J\_S para 0 [dB] por canal podemos distribuir a potência J do jammer entre apenas  $\rho$  canais dos  $N_{ch} = 2320$  canais totais, onde

$$\rho := \text{round}\left(10^{\frac{J\_S}{10}}\right) = 781 \quad \rightarrow \quad \rho = 781 \text{ é o fator inteiro pelo qual deveríamos dividir a potência J do jammer em um único canal para que se obtenha } J\_S=0 \text{ [dB]. Equivalentemente, } \rho = 781 \text{ é o número de canais que devemos varrer sob } J\_S = 28.9 \text{ [dB], distribuindo assim a potência J do jammer entre os canais para que, na média, se obtenha } J\_S=0 \text{ [dB].}$$

Com isto, estamos implementando a técnica PBJ (*partial band jamming*). O hopping range é  $HR := BW \cdot N_{ch} = 58 \cdot \text{MHz}$ , e a largura da banda parcial interferida pelo jammer é  $PB := \rho \cdot BW = 19.5 \cdot \text{MHz}$ .

O duty cycle  $\delta$  do PBJ para  $J/S = 0$  [dB] por canal na banda  $PB = 19.5 \cdot \text{MHz}$  é obtido de:

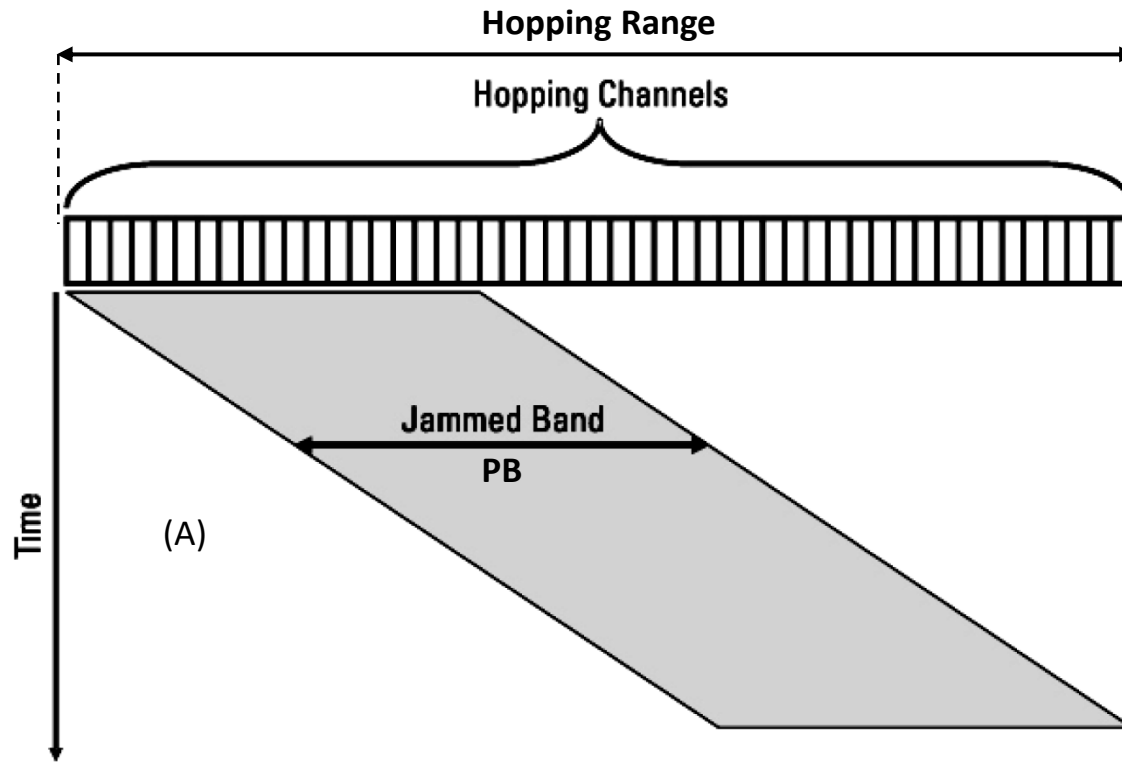
$$\delta := 100 \cdot \frac{\rho}{N_{ch}} = 33.66 \%$$

que resulta maior do que o duty cycle 33.3% sob  $J/S = 0$  [dB], que é a regra prática recomendada para PBJ.

A geometria proposta no enunciado para o *partial band jamming* do TX do enlace é, portanto, válida (pode acontecer em determinadas situações táticas que as possíveis geometrias não atendam a condição duty cycle 33.3% sob  $J/S = 0$  [dB]).

## Jamming de sinais Frequency Hopping (FH)

O **swept spot jamming** é uma variante da técnica *partial band* em que o sinal de *jamming* cobre a banda parcial PB do *hopping range*, conforme mostrado em (A), mas a medida que o tempo transcorre, a banda parcial é deslocada sobre toda a faixa do *hopping range*. O **swept spot jamming** é usual em dispositivos para *Stand-in Jamming* (ver slide 113), obtendo-se um significativo aumento da eficácia do *jamming*.

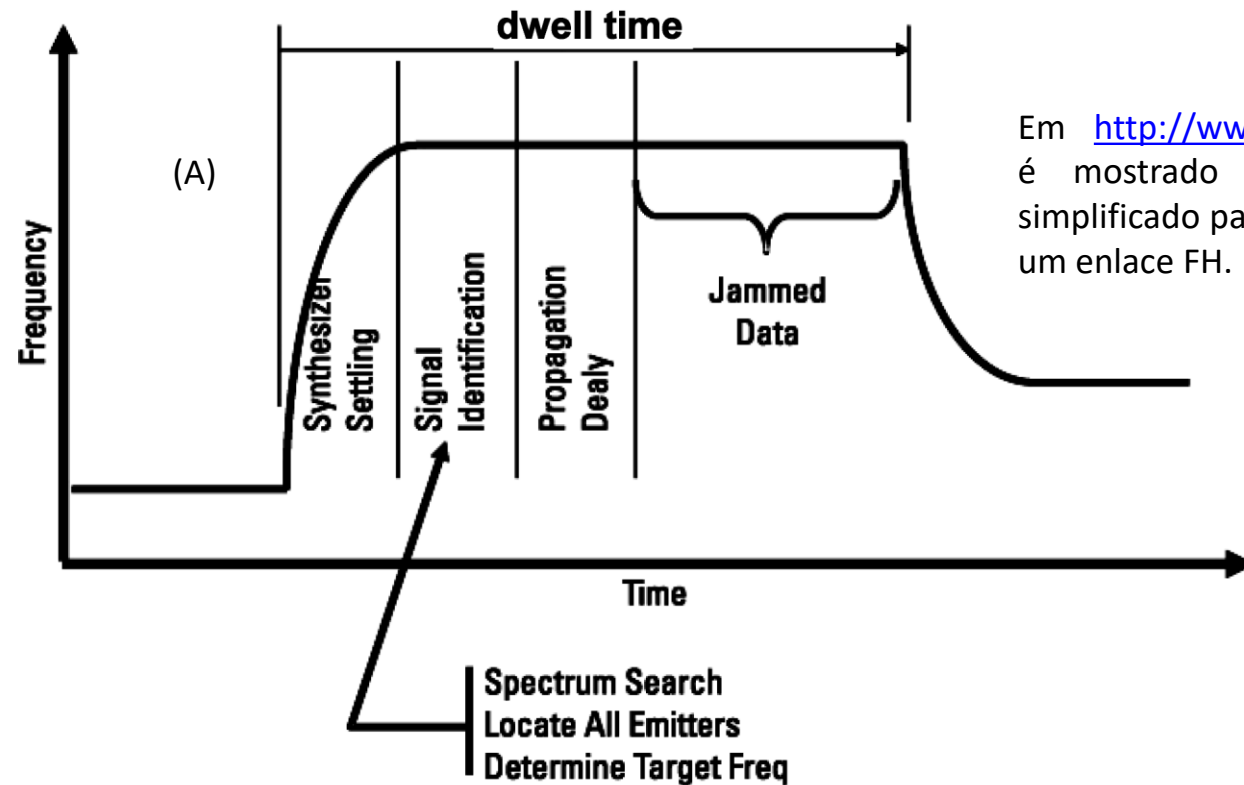


## Jamming de sinais Frequency Hopping (FH)

O **follower jamming** determina preliminarmente em uma fração do *dwell time* (ver slide 57) para qual frequência  $f_x$  um enlace FH inimigo saltou em um determinado instante. Imediatamente a seguir o TX do *jammer* é sintonizado em  $f_x$  e o enlace inimigo é interferido na frequência  $f_x$  durante o tempo restante do *dwell time*. A cada *hop* (salto) do enlace FH o procedimento é repetido pelo *jammer*.

A eficácia de um *follower jammer* é dependente da rapidez que o *search receiver* do *jammer* (ver slides 11 e 25) é capaz de determinar para qual frequência  $f_x$  o enlace FH inimigo salta a cada instante. Para *slow hoppers* (ver slides 58 a 60) é possível usar análise espectral via FFT (*Fast Fourier Transform*), no entanto para *fast hoppers* é usual adotar um banco de filtros sintonizados (ver Figura 3 de <http://www.fccdecastro.com.br/pdf/FJCFHSS.pdf>).

Em (A) é mostrado o diagrama de temporização típico para um *follower jammer*, e como se nota, somente metade do *dwell time* é interferido.



Em <http://www.fccdecastro.com.br/pdf/SIFHCSFJ.pdf> é mostrado o diagrama de blocos funcional simplificado para um *follower jammer* interferindo em um enlace FH.



## Jamming de sinais Chirp

Nos slides 61 a 63 discutimos a curva frequência versus tempo para sinais *chirp* (*Wide Linear Sweep* e *Chirp on Each Bit*). O padrão de varredura em frequência é rápido e aleatório de modo que o sinal *chirp* não pode ser “visto” por um RX que não esteja sincronizado com o padrão de varredura em frequência do TX do enlace. O instante de início de cada ciclo de varredura em frequência também pode ser aleatório e/ou a declividade da curva de varredura em frequência pode ser não linear para dificultar eventual tentativa de sincronização de parte de um RX receptor hostil com o TX do enlace.

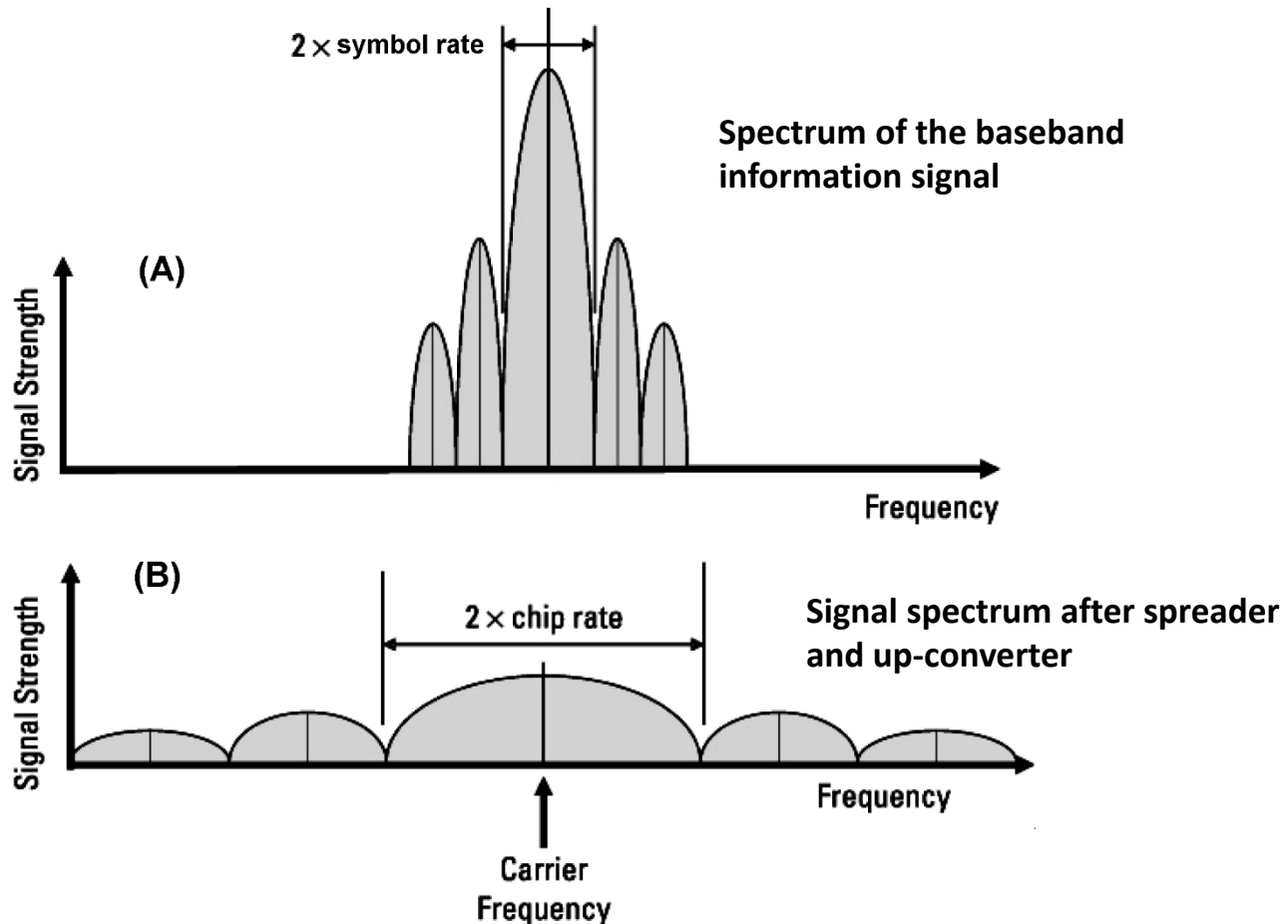
A faixa de frequência do sinal *chirp* pode ser determinada por um analisador de espectro, mas para efetuar o *follower jamming* (ver slide anterior), a declividade e o tempo de início da varredura precisam ser conhecidos. Como a curva de varredura pode ser não linear, surge ainda esta complicação adicional. No entanto, se o TX do enlace *chirp* usa um padrão de varredura previsível (linear e de declividade constante, por exemplo), a declividade da curva de varredura pode ser determinada por análise espectral através da FFT (*Fast Fourier Transform*) do sinal *chirp* recebido no *search receiver* do *jammer* (com base na propriedade 3 no slide 15 de [http://www.fccdecastro.com.br/pdf/SS\\_Aula13&14\\_04052020.pdf](http://www.fccdecastro.com.br/pdf/SS_Aula13&14_04052020.pdf)) e, uma vez determinado o padrão de varredura, o TX do *jammer* pode ser sincronizado com a varredura do sinal *chirp* que trafega no enlace, estabelecendo-se então um cenário de *follower jamming* do RX do enlace.

Caso o padrão de varredura do *chirp* não for previsível, então a abordagem usualmente adotada é o *search receiver* do *jammer* utilizar o sinal de RF *raw* (= bruto), i.e., sem efetuar qualquer demodulação ou filtragem, e digitalizar e gravar este sinal de RF *raw* em uma DRFM (*Digital Radio Frequency Memory* – ver <https://www.mdpi.com/2076-3417/10/12/4123/htm>, [https://en.wikipedia.org/wiki/Digital\\_radio\\_frequency\\_memory](https://en.wikipedia.org/wiki/Digital_radio_frequency_memory) e <https://web.archive.org/web/20110722014927/http://ftp.rta.nato.int/public//PubFullText/RTO/MP/RTO-MP-SET-080///MP-SET-080-P07.pdf>). Em seguida, uma análise estatística detalhada é efetuada no domínio tempo e no domínio frequência do sinal gravado na DRFM e os parâmetros do sinal *chirp* são identificados. Os parâmetros do padrão de varredura do *chirp* são informados ao TX do *jammer* que replica o sinal do *chirp* recebido, estabelecendo o cenário de *follower jamming* do RX do enlace.

O *partial band jamming*, que discutimos no Exemplo 14 do slide 122 para sinais *frequency hopping*, também pode ser aplicado a sinais *chirp*. Os critérios são os mesmos: o *jammer* deve ser capaz de obter  $J/S = 0$  [dB] com *duty cycle* 33.3%. Por exemplo, se o *sweep range* (ver slides 61 e 62) do *chirp* for  $SwR = 5$  [MHz] e a largura de banda da informação for  $BW = 25$  kHz, um *partial band*  $PB = 1.65$  [MHz] resulta em um *duty cycle*  $\delta = PB/SwR = 33\%$ . Para atingir  $J/S = 0$  [dB] em cada largura de banda  $BW$  de informação em toda a banda  $PB$  é necessário multiplicar a potência do TX do *jammer* por  $\rho = PB/BW = 66$ , ou equivalentemente adicionar  $10 \log \rho = 18.2$  [dB] à potência do TX em [dBm].

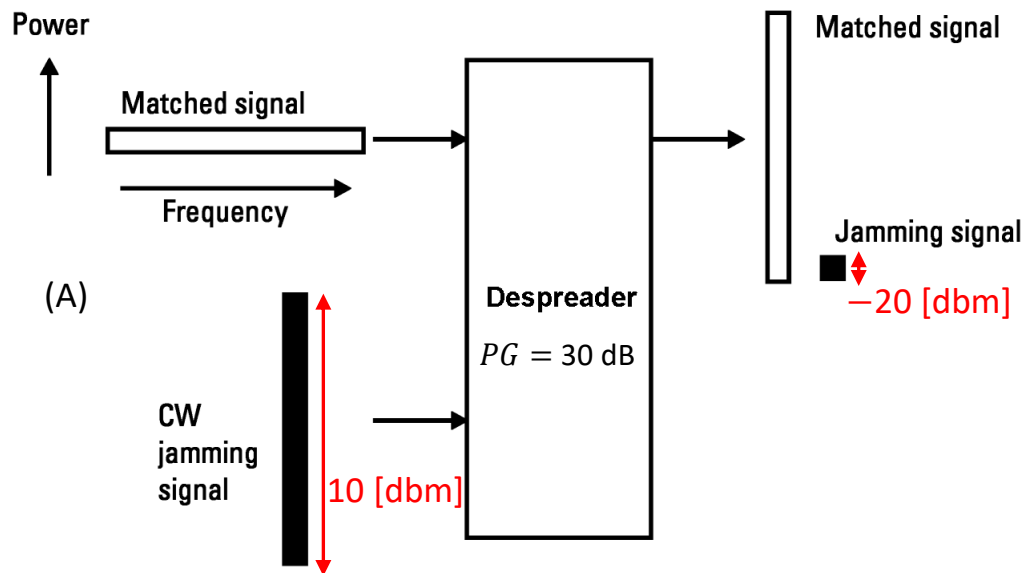
## Jamming de sinais *Direct Sequence Spread Spectrum (DS-SS)*

Conforme vimos no Cap 1.3, o ganho de processamento  $PG$  de um sistema DS-SS é obtido através da operação de *spreading* efetuada pelo *spreader* (ver slide 78). O *spreader* efetua o *spreading* da sequência de símbolos IQ de duração  $T_s$  em banda-base, utilizando códigos PN.  $1/T_s$  é denominado **symbol rate**. Um código PN (PN – *pseudo noise*) implementa um sinal aleatório com espectro similar ao espectro do ruído branco. No âmbito da geração de sinais DS-SS, os códigos PN devem idealmente apresentar função de autocorrelação impulsiva. Um código PN gera uma sequência de símbolos BPSK, cada símbolo BPSK (denominado de *chip*) tendo uma duração  $T_c = T_s/PG$ , conforme mostrado no slide 78, sendo  $1/T_c$  denominado **chip rate**. Em (A) abaixo é mostrado o espectro do sinal em banda-base antes do *spreader* e em (B) é mostrado o espectro do sinal após o *spreader* e *up-converter*.



## Jamming de sinais Direct Sequence Spread Spectrum (DS-SS)

Assim como para os sinais *chirp* e *frequency hopping*, o *jamming* de um sinal DS-SS é considerado eficaz na situação  $J/S = 0$  [dB] com *duty cycle* 33.3%, referida para após o bloco *despreader* (ver slide 80). No entanto, o *despreader* apresenta um ganho de processamento  $PG$  significativo ao recuperar o sinal de informação desejado em banda-base (*matched-signal* em (A) abaixo – ver slide 79). Como o sinal do *jammer* não é correlacionado com o código PN do enlace DS-SS o  $J/S$  será subtraído de  $PG$ , reduzindo drasticamente a eficácia do *jammer*. Por exemplo, se um *jammer* interfere um RX DS-SS com um sinal CW (*continuous wave*) de frequência constante e de potência  $J = 10$  [dbm] na entrada do *despreader* do RX DS-SS, cujo ganho de processamento é  $PG = 30$  [dB], então o sinal do *jammer* será “visto” após o *despreader* com uma potência de  $J - PG = -20$  [dBm], conforme mostrado em (A) abaixo.



No entanto, um *jammer* CW é um simples oscilador de RF de alta potência, e é um dispositivo relativamente simples e de médio custo. Então pode ser viável um *jammer* CW com potência extra de modo a superar o ganho de processamento  $PG$  do *despreader* e , com isto, manter  $J/S = 0$  [dB].

Ainda, é possível adotar um sinal de *jamming* CW, mas pulsado com um *duty cycle* de 33.3% ou menor no domínio tempo, de modo que possamos aumentar a potência de pico do *jammer* de um fator inversamente proporcional ao *duty cycle*. Em <http://www.fccdecastro.com.br/pdf/CWPJDSSS.pdf> é analisado o desempenho do *jamming* pulsado versus o desempenho do *jamming* CW, e os resultados para *jamming* pulsado são significativos mesmo para um *duty cycle* menor que 33.3%.

## Homework 1

Refazer o Exemplo 1 no slide 20 para  $PRF = 15\text{KHz}$ .

## Homework 2

Refazer o Exemplo 2 no slide 24 para  $f_s = 8$  [Gsa/s].

## Homework 3

Refazer o Exemplo 3 no slide 30 para  $f_s = 8$  [Gsa/s].



## Homework 4

Refazer o Exemplo 4 no slide 38 para  $f_0 = 4$  [GHz].

## Homework 5

Refazer o Exemplo 5 no slide 39 para  $f_s = 12$  [Gsa/s].

## Homework 6

Refazer o Exemplo 6 no slide 54 para  $d = 12$  [Km]  $\alpha = 28^\circ$  e  $\beta = 45^\circ$ .

## Homework 7

Refazer o Exemplo 7 no slide 70 para  $f_1 = 3.0$  [GHz] e  $f_2 = 17$  [GHz].

## Homework 8

Refazer o Exemplo 8 no slide 71 para  $PRF = 15\text{KHz}$ .

## Homework 9

Refazer o Exemplo 9 no slide 73 para  $f_1 = 400$  [MHz] e  $f_2 = 1.6$  [GHz].

## Homework 10

Refazer o Exemplo 11 no slide 99 para para  $f_1 = 70$  [MHz] e  $f_2 = 90$  [MHz].



## Homework 11

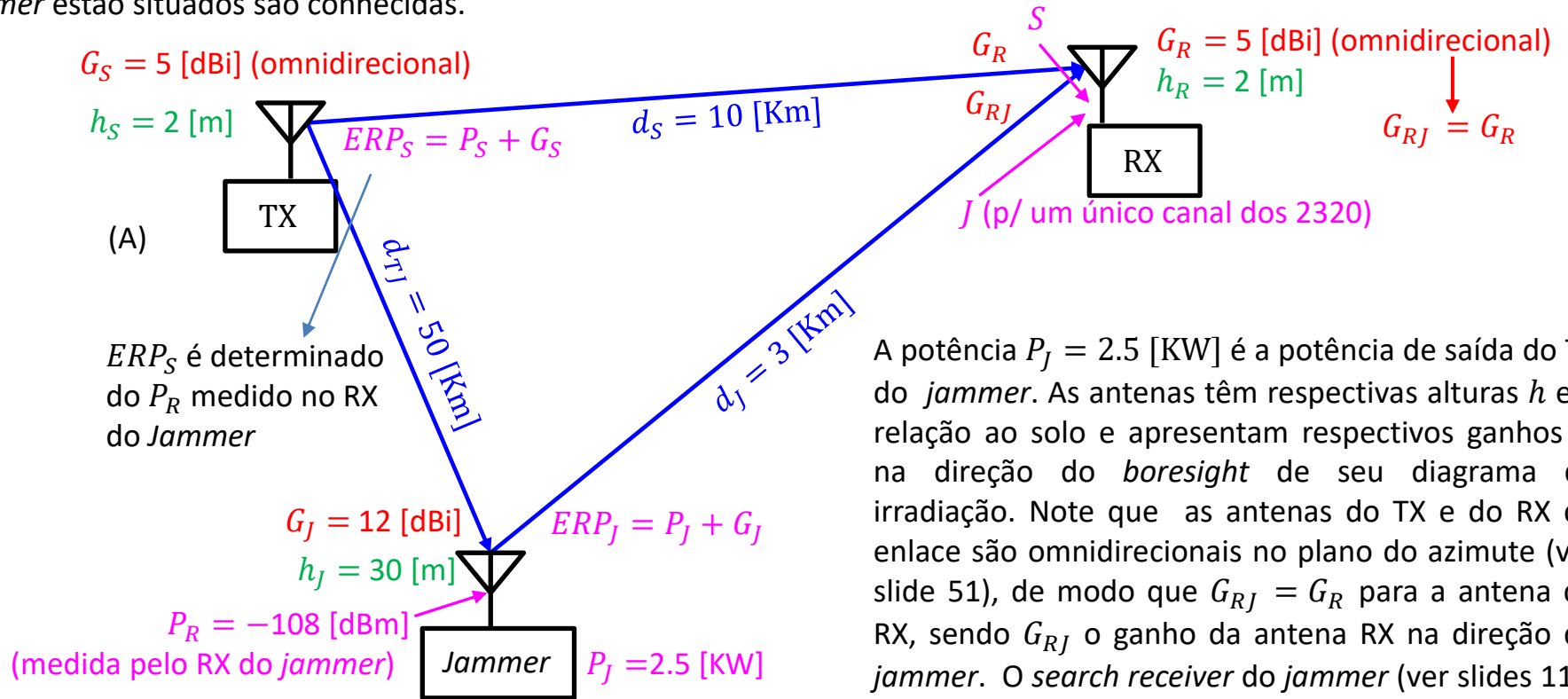
Refazer o Exemplo 12 no slide 105 para  $t_{21} = 12.623$  [ $\mu\text{s}$ ],  $t_{31} = -6.204$  [ $\mu\text{s}$ ],  $X_2 = 20.36$  [Km] e  $(X_3, Y_3) = (17.15, 5.59)$  [Km].

## Homework 12

Refazer o Exemplo 13 no slide 119 para as modulações **(a)** 16-PSK e **(b)** BPSK.

## Homework 13

Um sistema FH inimigo opera sob um *hopping range* de 58MHz (de 30MHz a 88 MHz), com  $N_{ch} = 2320$  canais de  $BW = 25$  kHz nesta faixa. Em (A) é mostrado a geometria do cenário de *jamming* para este sistema. As coordenadas onde TX, RX e *Jammer* estão situados são conhecidas.



A potência  $P_J = 2.5$  [KW] é a potência de saída do TX do *jammer*. As antenas têm respectivas alturas  $h$  em relação ao solo e apresentam respectivos ganhos  $G$  na direção do *boresight* de seu diagrama de irradiação. Note que as antenas do TX e do RX do enlace são omnidirecionais no plano do azimute (ver slide 51), de modo que  $G_{RJ} = G_R$  para a antena do RX, sendo  $G_{RJ}$  o ganho da antena RX na direção do *jammer*. O *search receiver* do *jammer* (ver slides 11 e 25) mediu uma potência  $P_R = -108$  [dBm] para o sinal recebido do TX do enlace.

As antenas do TX e do RX do enlace operam sob linha de visada direta e sem multipercurso, no entanto os caminhos de propagação entre o *jammer* e o TX do enlace e entre o *jammer* e o RX do enlace localizam-se em região pantanosa e deve-se esperar desvanecimento em consequência da reflexão da onda EM no solo condutor. **Pede-se:** Para a geometria dada em (A) determine a largura da banda parcial  $PB$  para que a mesma seja interferida pelo sinal do *jammer* sob  $J/S = 0$  [dB] e verifique se a geometria atende um *duty cycle* de pelo menos 33.3%.

## Apêndice A – script Matlab para comparação de curvas de desempenho de modulações digitais

Fonte: <https://www.gaussianwaves.com/2010/04/performance-comparison-of-digital-modulation-techniques-2/>

```
clear all;
EbN0dB=-4:1:24;
EbN0lin=10.^(EbN0dB/10);
colors={'b-*','g-o','r-h','c-s','m-d','y-*','k-p','b-->','g:<','r-.d'};
index=1;

%BPSK
BPSK = 0.5*erfc(sqrt(EbN0lin));
plotHandle=plot(EbN0dB,log10(BPSK),char(colors(index)));
set(plotHandle,'LineWidth',1.5);
hold on;

index=index+1;

%M-PSK
m=2:1:5;
M=2.^m;
for i=M,
    k=log2(i);
    berErr = 1/k*erfc(sqrt(EbN0lin*k)*sin(pi/i));
    plotHandle=plot(EbN0dB,log10(berErr),char(colors(index)));
    set(plotHandle,'LineWidth',1.5);
    index=index+1;
end

%Binary DPSK
Pb = 0.5*exp(-EbN0lin);
plotHandle = plot(EbN0dB,log10(Pb),char(colors(index)));
set(plotHandle,'LineWidth',1.5);
index=index+1;
```

```
%Differential QPSK
a=sqrt(2*EbN0lin*(1-sqrt(1/2)));
b=sqrt(2*EbN0lin*(1+sqrt(1/2)));
Pb = marcumq(a,b,1)-1/2.*besseli(0,a.*b).*exp(-1/2*(a.^2+b.^2));
plotHandle = plot(EbN0dB,real(log10(Pb)),char(colors(index)));
set(plotHandle,'LineWidth',1.5);
index=index+1;

%M-QAM
m=2:2:6;
M=2.^m;

for i=M,
    k=log2(i);
    berErr = 2/k*(1-1/sqrt(i))*erfc(sqrt(3*EbN0lin*k/(2*(i-1))));
    plotHandle=plot(EbN0dB,log10(berErr),char(colors(index)));
    set(plotHandle,'LineWidth',1.5);
    index=index+1;
end

legend('BPSK','QPSK','8-PSK','16-PSK','32-PSK','D-BPSK','D-QPSK','4-QAM','16-QAM','64-QAM');
axis([-4 24 -8 0]);
set(gca,'XTick',-4:2:24); %re-name axis accordingly
ylabel('Probability of BER Error - log10(Pb)');
xlabel('Eb/N0 (dB)');
title('Probability of BER Error log10(Pb) Vs Eb/N0');
grid on;
```

## Apêndice B – Bibliografia

1. Air and Spaceborne Radar Systems An Introduction - Philippe Lacomme - SciTech - 2001
2. Electronic Warfare Receivers and Receiving Systems - Richard A. Poisel - Artech House - 2014
3. Electronic Warfare Techniques ATP 3-12.3 - USArmy - 2019
4. EW 103 - Tactical Battlefield Communications Electronic Warfare - Artech House - 2009
5. EW 104 - EW Against a New Generation of Threats - David L. Adamy - Artech House - 2015
6. FMCW Radar Design - M. Jankiraman - Artech House - 2018
7. Geolocation Techniques Principles and Applications - Gentile - Springer - 2013
8. Introduction to Airborne Radar 3rd - Stimson - SciTech
9. Introduction to Communication Electronic Warfare Systems - Richard Poisel - Artech House - 2002
10. Introduction to Modern EW Systems - Andrea De Martino - Artech House - 2018
11. INTRODUCTION TO RADAR SYSTEMS 2nd - Merrill I. Skolnik - McGraw-Hill
12. Manual de Ensino Trabalho de Comando EB60-ME-13.301 - Exército Brasileiro - 2019
13. Modern Communications Jamming Principles and Techniques 2nd - Richard Poisel - Artech House - 2011
14. Redefining information warfare boundaries for an Army in a wireless world - Rand - 2013
15. U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-7-6