

Funcionalidade dos Software e Hardware livres na Localização De Sinais: estudo de caso, analisando o uso do SDR-RTL pelo método TDOA.

(CT) Pedro Tebaldi Medeiros da Silva*

RESUMO

O Sistema SDR-RTL tem sido cada vez mais explorado no campo da localização de sinais. O sistema apresentou como desvantagem a necessidade de posicionamento do sinal pretendido. Em situações onde o emissor encontrava-se situado fora do triângulo formado pelos receptores, não foi possível obter sua localização precisa; na melhor hipótese, obteve-se a direção do sinal, porém sem um ponto específico para sua posição. Apesar disso, apresentou relevantes vantagens que levaram à conclusão pela sua viabilidade de emprego. Além do baixo custo e fácil acesso, o processamento do sistema se dá no meio digital, não dependendo, assim, da precisão de componentes analógicos do rádio convencional. Foi verificado que o sistema pode ser instalado em ambientes internos sem perder sua eficácia, não sendo necessário locais como campo aberto ou terraços de prédios para seu bom funcionamento. Outra vantagem é a interface do sistema, que facilita tanto sua operação como manutenção, além do amplo número de entusiastas que compartilham informações e algorítimos em diversos sites pela internet. Neste trabalho, verificou-se que os testes realizados se mostraram eficientes e capazes de serem aplicados não apenas no meio civil, mas também pelas Forças Armadas, com a vantagem de custo reduzido e menor emprego de pessoal.

Palavras-chave: Localização de sinais. TDOA. Software livre.

**Functionality of Free Software and
Hardware in Signal Location: a case study,
analyzing the use of SDR-RTL by the TDOA
method.**

ABSTRACT

The SDR-RTL System has been increasingly explored in the field of signal localization. The disadvantage of the system was the need to position the desired signal. In situations where

the emitter was located outside the triangle formed by the receivers, it was not possible to obtain its precise location; in the best case, the direction of the signal was obtained, but without a specific point for its position. Despite this, it presented significant advantages that led to the conclusion of its viability of employment. In addition to low cost and easy access, the processing of the system occurs in the digital medium, thus not depending on the accuracy of analogical components of the conventional radio. It was verified that the system can be installed indoors without losing its effectiveness, and it is not necessary to have places such as open fields or terraces of buildings for their proper functioning. Another advantage is the system interface, which facilitates both its operation and maintenance, as well as the large number of enthusiasts who share information and algorithms on various websites over the internet. In this work, it was verified that the tests performed were efficient and capable of being applied not only in the civilian medium, but also by the Armed Forces, with the advantage of reduced cost and lower personnel employment.

Keywords: Signal localization. TDOA. Free software.

1 INTRODUÇÃO

De acordo com Exército Brasileiro (2019), a Guerra Eletrônica compreende o conjunto de ações que tem por finalidade desenvolver e assegurar a capacidade de emprego eficiente das emissões eletromagnéticas próprias, ao mesmo tempo em que buscam impedir, dificultar ou tirar proveito das emissões inimigas.

Poucos podem ter real acesso às atividades de GE, pois os conhecimentos dos seus domínios envolvem tecnologias, técnicas e táticas que têm sido circunscritas a duas categorias limitadas de pessoas: os engenheiros e técnicos peritos no assunto; e os especialistas das forças que planejam o emprego das atividades de GE, operam e executam a manutenção dos seus complexos meios.

Conforme Exército Brasileiro (2019), a GE se divide em dois campos de atuação: Comunicações e Não Comunicações, sendo aquela o foco do presente trabalho.

2 GUERRA ELETRÔNICA

Segundo Adamy (2001), "Guerra eletrônica é definida como a arte e ciência de preservar o uso do espectro eletromagnético para uso amigável, enquanto negando o seu uso para o inimigo.". (ADAMY, 2001, p. 3).

Outra definição pode ser obtida de acordo os ensinamentos de Oliveira (2002): A GE é o componente do emprego militar da eletrônica que abrange ações realizadas com a finalidade de evitar ou reduzir o uso eficaz da energia eletromagnética, radiada pelas forças inimigas, bem como as atividades efetuadas com o propósito de garantir o seu emprego pelas forças inimigas. (OLIVEIRA, 2002, p. 47).

2.1 LOCALIZAÇÃO DE SINAIS

A localização de sinais (ou Localização Eletrônica) pode ser vista como uma das diversas finalidades da GE. De acordo com Exército (2019), "Consiste na determinação, por intermédio de sistemas eletrônicos especializados, da posição geográfica provável de um emissor de energia eletromagnética." (EXÉRCITO, 2019, p. 3-3).

Ainda de acordo com Exército Brasileiro (2019), a precisão da localização de um sinal eletrônico depende, dentre outros fatores, da técnica empregada. Neste trabalho, focaremos o estudo na técnica TDoA – *Time difference of arrival*, a ser abordada em tópico posterior.

3 EQUIPAMENTOS UTILIZADOS NA LOCALIZAÇÃO DE SINAIS

Neste tópico, serão apresentados os equipamentos que serão objeto de estudo do trabalho.

3.1 RÁDIO DEFINIDO POR SOFTWARE (SDR)

De acordo com CHEN e HO (2017), O SDR teve seu início no início da década de 90, quando o Departamento de Defesa dos EUA, visando a atender às demandas por comunicações seguras, iniciou o programa SPEAKEasy com a finalidade de facilitar a integração entre os sistemas de comunicação de rádio. (REED, 2002 apud CHEN, Wen Tzu e HO, Chen-Hsun, 2017).

A fim de definir o que vem a ser o SDR, *Wireless Innovation Forum (2018)* traz a seguinte consideração:

O SDR define uma coleção de tecnologias de hardware e software em que algumas ou todas as funções operacionais do rádio (também conhecidas como processamento da camada física) são implementadas por meio de software ou firmware modificável que operam em tecnologias de processamento programáveis. (WIRELESS, 2018.).

De acordo com Martins (2015), "O conceito de rádio definido por software (SDR) permite substituir a tradicional implementação dos dispositivos de comunicação analógicos por uma implementação mais flexível.". Em sua obra, Martins (2015) afirma que o sistema possui maior flexibilidade de reconfiguração, se comparado aos rádios convencionais, podendo, assim, melhor atender às necessidades de cada operação.

Na mesma obra, SRUTHI (2013) afirma que a tecnologia SDR visa a substituir os *hardwares* de rádio convencionais com a implementação daquele sistema, através de softwares abertos, reconfiguráveis e reprogramáveis.

3.2 RTL-SDR

De acordo com STEWART (2015), o RTL-SDR é um pequeno dispositivo USB compacto e fácil de usar, capaz de receber sinais de rádio RF. Em seu artigo, afirma que o dispositivo possuía outra finalidade quando da sua criação: Originalmente, esses dispositivos foram projetados para uso como DVB-T (*digital vídeo broadcast – terrestrial*) [...], permitindo que os consumidores recebessem transmissão UHF e assistissem TV em seus computadores. (STEWART et al., 2015, p. 65).

Conforme RTL-SDR.COM, O RTL-SDR é um dispositivo USB de baixo custo (aproximadamente US\$ 25), que pode ser usado como um *scanner* de rádio baseado em computador para receber sinais de rádio ao vivo. (ABOUT RTL-SDR, 2018).

3.3 O SOFTWARE

A fim de integrar a plataforma do RTL-SDR com o computador, será necessário um *software* para tal. Nesse estudo, foi utilizado o MATLAB. Segundo Stewart (2017): O MATLAB e o Simulink fornecem um ambiente onde você pode codificar e construir os receptores de forma conveniente, e essas caixas de ferramentas fornecerão os meios necessários para

implementar qualquer algoritmo de receptor SDR desejado. Eles não apenas fornecem as facilidades para projetar coisas como os filtros digitais, decimadores e sincronizadores que seu sistema requer, mas também fornecem ferramentas que permitem visualizar sinais nos domínios de tempo e frequência à medida que passam pelo processo de demodulação. (STEWART et al., 2017, p. 6).

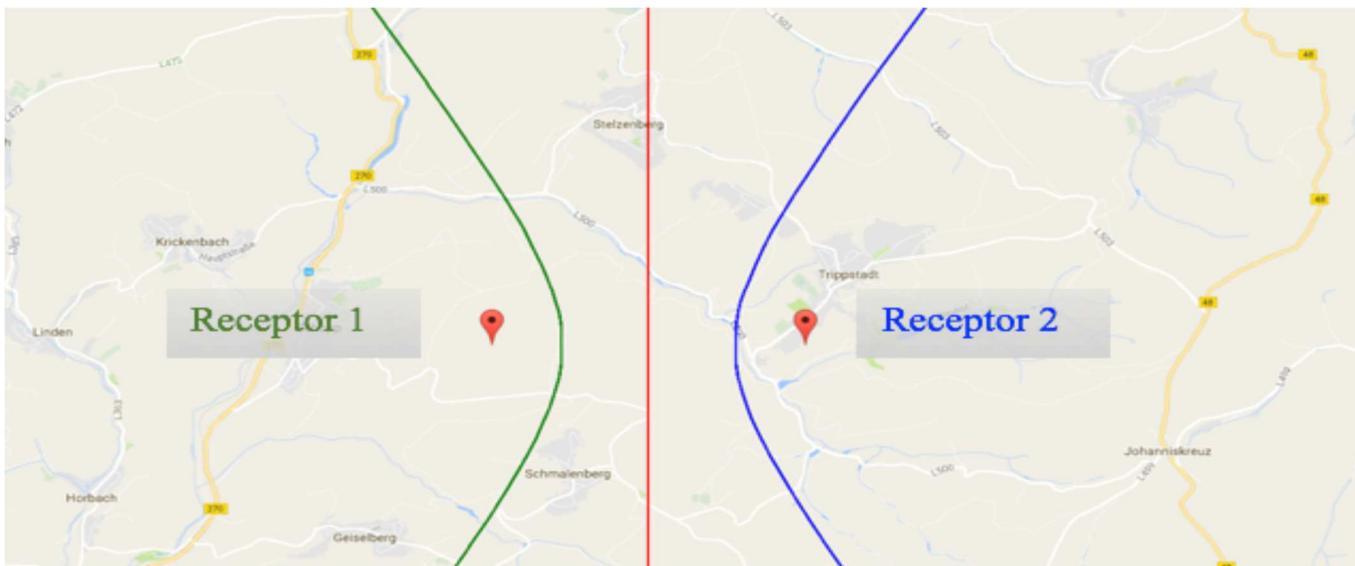
4 ESTUDO DE CASO ANALISANDO O USO DO RTL-SDR

Para o referido estudo, será exposto o experimento realizado por Stefan Scholl em 2017 na cidade de Kaiserslautern, Alemanha.

Inicialmente, Scholl utilizou o que chamou de “situação simplificada”, com apenas 2 receptores a fim de localizar a emissão do sinal pretendido. Para tal, utilizou a técnica *Time Difference of Arrival* (TDoA), que Adamy (2001) explica: Um sinal que sai do transmissor em algum momento definido chegará ao receptor no tempo d/c mais tarde, onde d é a distância do transmissor ao receptor e c a velocidade da luz. Assim, o tempo de chegada define a distância. Os receptores GPS emitem referências de tempo muito precisas, tornando a medição TOA de precisão muito mais fácil (logisticamente) do que há alguns anos atrás. (ADAMY, 2001, p. 172).

Inicialmente, ilustrou o possível resultado de um teste utilizando apenas dois receptores.

Figura 1 – Situação simplificada com 2 receptores



Fonte: Scholl (2017).

Acima, tem-se 3 hipérboles. A hipérbole central (de cor vermelha) foi obtida após verificar um TDOA de 0ns, ou seja, não houve diferença entre o tempo de chegada do sinal em relação aos receptores. Com isso, observou-se que o emissor poderia assumir qualquer posição ao longo dessa linha, estando, assim, posicionado de forma equidistante dos dois receptores.

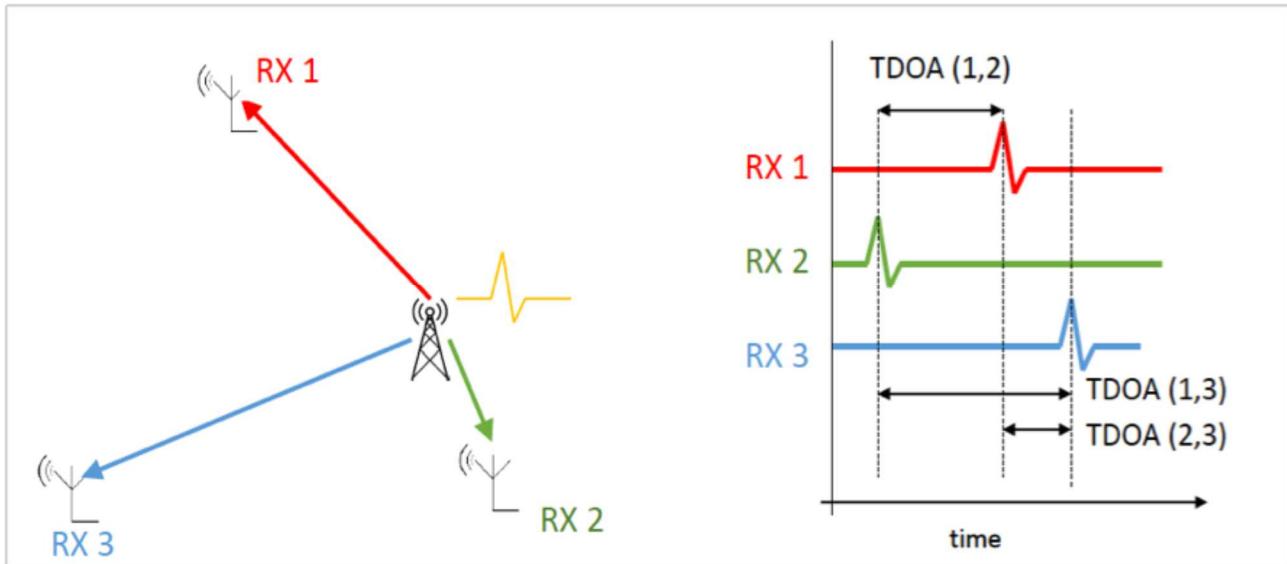
A hipérbole verde foi obtida após verificar um TDOA de 6,7ns entre os receptores. Com isso, concluiu-se que o transmissor estava posicionado 2000m mais próximo do receptor 1 em relação ao receptor 2. Analogamente ao ocorrido com a hipérbole central, o emissor poderia assumir qualquer posição ao longo da hipérbole verde.

Quanto à hipérbole azul, foi obtida após verificar também um TDOA de 6,7ns entre os receptores, porém, agora o emissor estaria localizado mais próximo ao receptor 2, mantendo a mesma relação de distância anterior (2000m).

Assim, concluiu-se que, utilizando apenas 2 receptores, não seria possível precisar a localização da fonte de sinal. Para eliminar as ambiguidades quanto ao posicionamento do emissor, seria necessário acrescentar mais um receptor.

Scholl (2017) ilustrou o que viria a ser a localização pela técnica TDOA utilizando 3 receptores conforme abaixo:

Figura 2 – Técnica TDOA

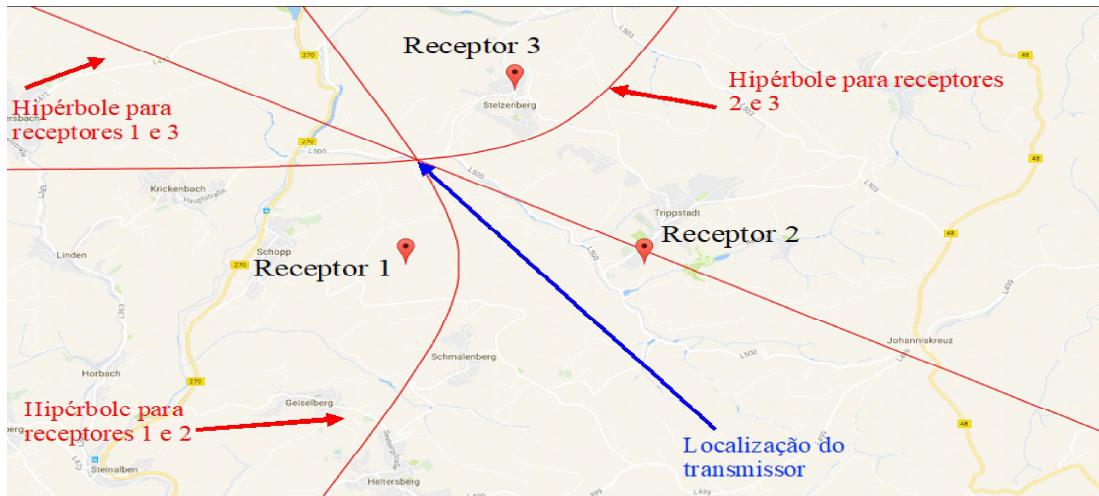


Fonte: Scholl (2017).

Em seguida, explicou o resultado que seria obtido utilizando 3 receptores dispostos em geometria triangular. Desta forma, a ambiguidade quanto à localização do emissor

seria mitigada pelo cruzamento das 3 hipérboles, obtendo, assim, sua localização neste ponto.

Figura 3 – Sistema completo com 3 receptores



Fonte: Scholl (2017).

4.1 CORRELAÇÃO ENTRE OS SINAIS RECEBIDOS

Para calcular o atraso do recebimento dos sinais entre os receptores, Scholl utilizou a seguinte função de correlação:

$$Corr(\tau) = \sum_{t=0}^{N-1} s_1(t)s_2(t + \tau)$$

A correlação é máxima quando os dois sinais casam melhor. Se os dois sinais forem idênticos, esse máximo se dará quando as duas cópias estiverem sincronizadas (sem atraso). (ABU-RGHEFF, 2018, p. 40).

Onde $s_1(t)$ e $s_2(t)$ são os sinais recebidos pelos receptores 1 e 2.

De acordo com Abu-Rgheff (2007), a correlação é amplamente utilizada para estimar o tempo de atraso e sincronização entre sinais. Segundo o autor: Correlação é a medida de similaridade entre dois sinais quando um está defasado em relação ao outro. A correlação é máxima quando os dois sinais casam melhor. Se os dois sinais forem idênticos, esse máximo se dará quando as duas cópias estiverem sincronizadas (sem atraso). (ABU-RGHEFF, 2018, p. 40).

4.2 POSICIONAMENTO DOS RECEPTORES

Scholl(2017) verificou que, para uma melhor acurácia, o emissor do sinal deveria estar entre os 3 receptores. Em uma situação ideal, os receptores formariam os vértices de um triângulo, e o emissor estaria localizado no interior deste. Na situação em estudo, não foi possível realizar tal disposição por questões geográficas, visto que seria necessário dispor os receptores em regiões de floresta, com difícil acesso e sinal de internet desfavorável. A figura abaixo ilustra a situação descrita.

Figura 4 - Posicionamento dos receptores



Fonte: Scholl (2017).

4.3 INFRAESTRUTURA DO SISTEMA

A estrutura utilizada por Scholl consiste em 3 receptores RTL-SDR, cada qual ligado a um computador, conectados via internet a um computador mestre.

Assim, o computador mestre é capaz de iniciar a recepção pelos receptores como um “gatilho”. Com isso, os receptores recebem o sinal e o transmitem de volta para o computador mestre.

Figura 5 - Infraestrutura do sistema



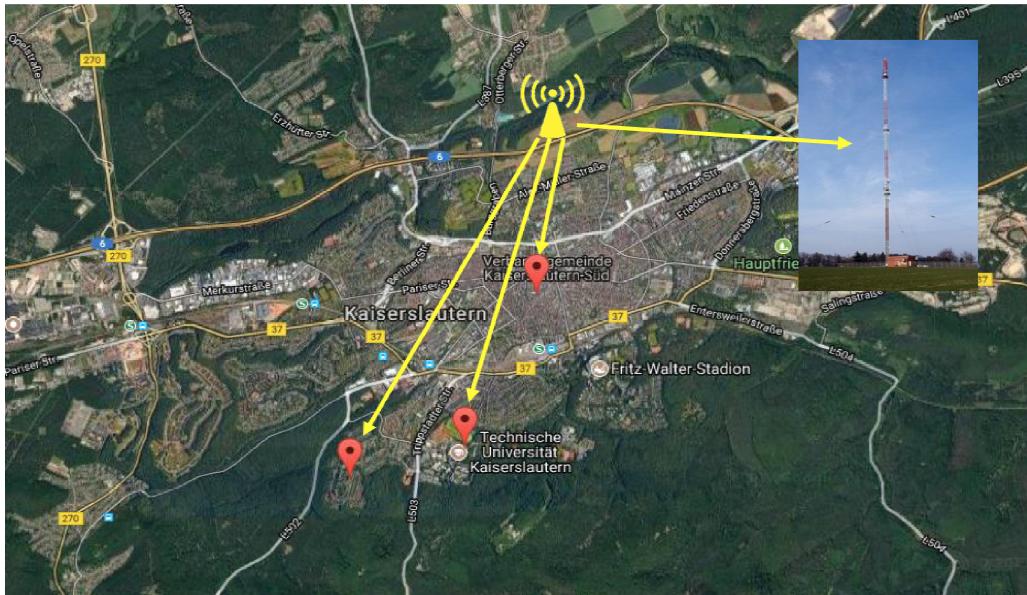
Fonte: Scholl (2017).

4.4 SÍNCRONIZAÇÃO

Segundo Scholl (2017), a sincronização é de vital importância para a eficiência do sistema e requer uma precisão na casa dos nano segundos. Para tal, utilizou como referência uma torre de transmissão de sinal áudio digital (de

posição conhecida), medindo 120m de altura e uma potência de 2Kw. Segundo Scholl, tais características foram fundamentais para a correlação de sinais.

Figura 6 - Receptores e antena para sincronização



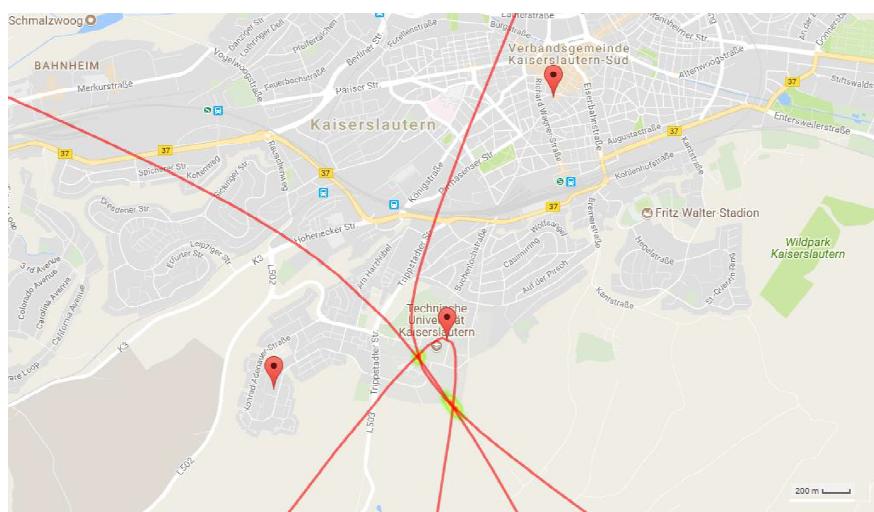
Fonte: Scholl (2017).

5 ANÁLISE DOS RESULTADOS

Nesse tópico, serão demonstrados os resultados obtidos por Scholl em seus testes a fim de se obter a localização dos transmissores de sinal, utilizando um sistema com 3 RTL-SDR conectados via internet a um computador mestre, conforme descrito anteriormente.

O primeiro teste foi realizado tendo como alvo uma antena repetidora de sinal DMR (Rádio Móvel Digital) de 70cm, localizada no topo do prédio da Universidade de Kaiserslautern, a qual operava na frequência de 439,4 MHz, com uma largura de banda de 12,5 KHz e modulação 4-FSK.

Figura 7 - Resultado para antena DMR



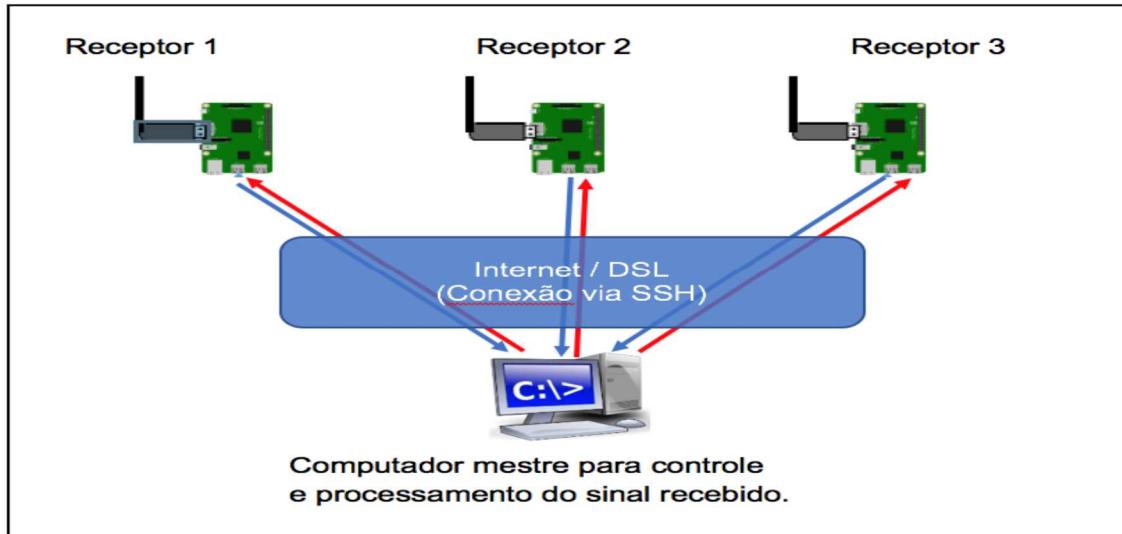
Fonte: Scholl (2017).

Nesse caso, pode-se observar que as hipérboles se cruzaram em dois pontos distintos, ocasionando uma ambiguidade quanto à real posição do emissor. Mesmo obtendo um resultado dúbio, o resultado obtido possui uma precisão relativamente boa, tendo em vista a escala de 1:200m verificada no mapa.

Outro teste realizado teve como alvo um sinal de transmissão FM na frequência 96,9 MHz. Nesse

caso, o resultado obtido não foi capaz de fornecer a localização precisa do emissor, tendo em vista estar localizado fora da área compreendida entre os 3 receptores [ver figura 4.5]. Entretanto, apesar do sistema não ter indicado um ponto exato da localização, Scholl verificou que pôde-se obter a direção do sinal (*Direction Finding*) com o resultado, concluindo que o alvo estaria localizado em algum lugar naquela direção.

Figura 8 - Resultado para antena de transmissão FM



Fonte: Scholl (2017).

6 CONCLUSÃO

Após analisar os testes realizados por Scholl (2017) e, considerando a real viabilidade de sua aplicação na localização de sinais, verificou-se a possibilidade da utilização de sistemas e equipamentos, livres de qualquer licença ou assinatura, de baixo custo e grande eficiência, em missões de Guerra Eletrônica.

Destaca-se o fato de o teste ter sido realizado por apenas uma pessoa. Nesse aspecto, vê-se uma considerável vantagem em utilizar esse sistema, visto que, empregando o mesmo esforço de pessoal (ou até mesmo menor), é possível ampliar a área monitorada, sem perder informações ou eficiência.

Somado a isso, levando em consideração que os equipamentos foram instalados em ambientes internos, sem a necessidade de dispô-los em terraços ou torres de antenas, o uso do RTL-SDR se mostrou grande facilitador em operações dos diversos tipos. Tendo como exemplo um ambiente hostil, o fato de instalar um sistema

em local aberto, como o terraço de um prédio ou até mesmo um campo aberto, poderia ser um fator preocupante para a equipe de GE em relação à segurança do equipamento e do pessoal envolvido.

Diante do exposto, pode-se concluir que os estudos sobre a GE não devem ser deixados em segundo plano. Pelo contrário, a necessidade de aprimorar o conhecimento sobre o assunto faz-se vital para que se mantenha o acompanhamento das evoluções tecnológicas e, assim, a constante atualização dos sistemas e doutrinas empregados. Nas palavras de Adamy (2001): A chave para entender os princípios da GE (particularmente a parte de radiofrequência) é ter uma compreensão realmente boa da teoria da propagação de rádio. Se você entender como os sinais de rádio se propagam, há uma progressão lógica para entender como eles são interceptados, bloqueados ou protegidos. Sem esse entendimento, parece que é quase impossível abraçar a Guerra Eletrônica. (ADAMY, 2001, p. 5).

Por fim, considerando a eficácia dos testes realizados por Scholl, após demonstrados os resultados obtidos, pôde-se concluir pela eficiência do sistema e entender que, ainda que de forma lenta e gradativa, sua utilização pelas Forças Armadas é viável e pode ser considerada como meio, mesmo que não substitutivo, mas ao menos complementar nas atividades de GE.

REFERÊNCIAS BIBLIOGRÁFICAS

ABU-RGHEFF, Mosa Ali. **Introduction to CDMA Wireless Communications.** Reino Unido. Ed. Elsevier, 2007. Disponível em: <<https://books.google.com.br/books?id=SI6XI8trarEC&printsec=frontcover&dq=inauthor:%22Mosa+Ali+Abu-Rgheff%22&hl=pt-BR&sa=X&ved=0ahUKEwmu9LI1ufbAhUDIZAKHcbxB4wQ6AEIKDAA#v=onepage&q=f=false>>. Acesso em 18 jun 2018.

ADAMY, David. **EW101: a first course in electronic warfare.** Norwood, MA: Artech House, 2001.

EXÉRCITO BRASILEIRO. **Manual de Campanha: A GUERRA ELETRÔNICA NA FORÇA TERRESTRE.** 2019.

MARTINS, Ramon Mayor. Rádio definido por software – SDR. **IFSC – Santa Catarina,** 2015. Disponível em: <https://wiki.sj.ifsc.edu.br/wiki/images/a/a7/Grupo_de_Estudos_em_R%C3%A1dio_Definido_por_Software.pdf> Acesso em: 2 jun 2018.

OLIVEIRA, Humberto José Corrêa de. **Coletânea história da guerra eletrônica.** V. 1. Brasília, DF: Ministério da Defesa – Centro Integrado da Guerra Eletrônica, 2002.

RTL-SDR.COM. **ABOUT RTL-SDR.** Disponível em: <<https://www rtl-sdr.com/about-rtl-sdr/>>. Acesso em: 2 jun 2018.

SCHOLL, Stefan. Introduction and Experiments on Transmitter Localization with TDOA. **Software Defined Radio Academy,** Friedrichshafen, Alemanha. Disponível em: <http://www.panoradio-sdr.de/wp-content/uploads/2017/07/sdr_tdoa_localization_online.pdf>. Acesso em 10 maio 2018.

SRUTHI, M. B. et al. Low cost digital transceiver design for software defined radio using RTL-SDR. **IEEE Communications Magazine,** [S. I.], 2013. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/6526525>>. Acesso em: 8 jun 2018.

STEWART et al. **Software Defined Radio Using MATLAB & Simulink and the RTL-SDR,** Glasgow, Scotland, UK. 2017.

STEWART, Robert W. et al. A Low-Cost Desktop Software Defined Radio Design Environment Using MATLAB, Simulink, and the RTL-SDR. **IEEE Communications Magazine,** [S. I.], 2015.

WIRELESS Innovation Forum. **Introduction to SDR,** [S.I.], [S.d.]. Disponível em <http://www.wirelessinnovation.org/Introduction_to_SDR>. Acesso em: 2 jun 2018.

*Artigo realizado a partir do trabalho de conclusão do Curso Básico de Guerra Eletrônica para Oficiais do Centro de Instrução de Guerra Eletrônica (CIGE) em 2018 pelo Capitão-Tenente Pedro Tebaldi Medeiros da Silva da Marinha do Brasil. Email: tebaldi@marinha.mil.br.