



SIMPÓSIO BRASILEIRO DE HIDROGRAFIA 2025



"Desafios da Hidrografia na Transformação Digital"

RESILIÊNCIA GNSS COM FOCO NO BRASIL

Krueger, C.P.¹; Souza, A.V.^{2}*

¹ Universidade Federal do Paraná; ² Universidade Federal do Paraná

*cpkrueger64@gmail.com; *avs76@icloud.com

A resiliência dos Sistemas Globais de Navegação por Satélite (GNSS), com foco nos desafios enfrentados no Brasil, pretende discorrer sobre os impactos da interferência do sinal do sistema GNSS no dia-a-dia dos diversos usuários. O sistema GNSS é essencial para aplicações em defesa nacional, segurança pública e setores civis, como levantamentos hidrográficos, monitoramento de massas de água e terrestres, agricultura de precisão e mapeamentos, mas sua fragilidade intrínseca, devido à baixa potência dos sinais, o torna vulnerável à interferências como *jamming* (bloqueio) e *spoofing* (falsificação). No Brasil, com 8,5 milhões de km² e 16.000 km de fronteiras, essas ameaças são amplificadas devido a sua vasta extensão territorial, pela dependência de constelações de satélites administrados por outros países e por atividades ilícitas, como narcotráfico e garimpo ilegal, especialmente na Amazônia, que representa 60% do território nacional.

A baixa potência dos sinais GNSS recebidos pelos receptores facilita interferências. O *jamming*, comum em áreas fronteiriças, utiliza dispositivos de baixo custo (US\$ 50) para bloquear sinais, criando zonas cegas de até 5 km, como observado em operações policiais em Tabatinga (AM). O *spoofing*, mais sofisticado, pode induzir erros de posicionamento, comprometendo drones do Sistema Integrado de Monitoramento de Fronteiras (SISFRON) ou mapeamentos agrícolas. Essas interferências são agravadas pela dependência do GPS americano, estando ainda os satélites do Bloco II sujeito a disponibilidade seletiva, e pela ausência de um sistema GNSS nacional, expondo o Brasil a riscos geopolíticos, como tensões com a Venezuela, que geraram 260.000 migrantes em Roraima até 2023.

As ameaças criminais, como o uso de *jammers* por facções como o PCC e o Comando Vermelho, impactam a segurança pública, bloqueando rastreamentos e facilitando o tráfico de drogas, que movimenta R\$ 10 bilhões anuais. Na defesa, a interrupção do GNSS compromete o SISFRON, essencial para monitorar 27% do território, e operações militares, como o uso de caças Gripen. Em aplicações civis, o *jamming* gera lacunas em levantamentos hidrográficos no rio Amazonas, aumentando custos.

Para mitigar essas vulnerabilidades, existem soluções tecnológicas, operacionais e estratégicas. Tecnicamente, antenas CRPA (*Controlled Reception Pattern Antennas*) reduzem o impacto de *jammers* em 20-30 dB, e a autenticação OS-NMA do Galileo detecta *spoofing*. Sistemas complementares, como o *eLoran*, com precisão de 8-20 m, e navegação inercial (INS), com erros de 1-2 m/min, oferecem redundância, sendo viáveis para a Amazônia e o litoral. Operacionalmente, o treinamento em navegação manual e a fiscalização de *jammers* fortalecem a resposta imediata. Estrategicamente, uma Política Nacional de PNT (Posicionamento, Navegação e Tempo), e parcerias com outros países são cruciais. A implementação de estações eLoran, protegeria 2.000 km de fronteira, enquanto receptores multi-GNSS reduziriam falhas em operações civis e militares.

Apesar do potencial, a implementação enfrenta desafios, como o orçamento de defesa limitado, burocracia e competição com saúde e educação. Comparado à Coreia do Sul, com *eLoran* operacional, e aos EUA, com autenticação civil avançada, o Brasil está atrasado, mas pode adaptar essas soluções priorizando áreas críticas como a Amazônia e o Pantanal. Superar essas barreiras exige coordenação interministerial, incentivos fiscais e parcerias público-privadas, garantindo que a resiliência GNSS proteja a soberania, a segurança e a economia brasileira.

Palavras-chave: GNSS; Resiliência; Jamming; Spoofing; Soberania Nacional