Avaliação Experimental de Ataque Jamming em Receptores GPS/GLONASS Utilizando SDRs de Baixo Custo

Lisandra Bozz Gonçalves[1], **Anthony Gabriel Kuhnen**[1], **Vinicius Amilgar Brenner**[1]

[1]Segurança Cibernética Diretoria de Tecnologias (SC.DT) - Itaipu Parquetec
Av. Tancredo Neves, 6731 - Jardim Itaipu, Foz do Iguaçu - PR, 85867-900

{anthony.kr,lisandra.bg}@bolsista.pti.org.br

vinicius.brenner@itaipuparquetec.org.br

Abstract. *Global Navigation Satellite Systems (GNSS), such as GPS and GLONASS, are widely used for location and time synchronization. However, they are vulnerable to jamming (interference) and spoofing (signal falsification), compromising their reliability. This work experimentally investigates the susceptibility of GPS and GLONASS receivers to jamming signals generated by low-cost software-defined radios (SDRs), using HackRF with Mayhem firmware. By emitting interference signals, the signal degradation was evaluated through the GPS Test application and the SEL-2488 dashboard. The results show that, even at multiple distances, significant loss or complete disruption occurs. Thus, it is concluded that accessible SDRs represent real risks, reinforcing the need for protection and monitoring.*

Resumo. *Os sistemas GNSS, como GPS e GLONASS, são amplamente usados para localização e sincronização de tempo. No entanto, são vulneráveis a jamming (interferência) e spoofing (falsificação de sinal), comprometendo sua confiabilidade. Este trabalho investiga experimentalmente a suscetibilidade de receptores GPS e GLONASS a sinais de jamming gerados por rádios definidos por software (SDRs) de baixo custo, utilizando o HackRF com firmware Mayhem. Emitindo sinais de interferência, avaliou-se a degradação do sinal por meio do GPS Test e do dashboard do SEL-2488. Os resultados mostram que, mesmo a múltiplas distâncias, ocorre perda significativa ou interrupção total. Dessa forma, conclui-se que SDRs acessíveis representam riscos reais, reforçando a necessidade de proteção e monitoramento.*

1. Introdução

O primeiro Sistema Global de Navegação por Satélite (GNSS) de cobertura global foi o Global Positioning System (GPS), projetado na década de 1970 pelos militares dos Estados Unidos para fins estratégicos e mais tarde foi liberado para uso civil na década de 1980 [of Defense 2008]. Desde então, houve o surgimento de outros sistemas de navegação global, como o Globalnaya Navigatsionnaya Sputnikovaya Sistema (GLONASS), desenvolvido pela Rússia, que também passou a ser amplamente utilizado em diversas aplicações[Montenbruck and Teunissen 2017]. Anos se passaram e a realidade dos dias atuais é que um imenso número de aplicações cabeadas dependem de sinais GNSS (GPS, GLONASS, entre outros) para prover serviços de navegação, localização e sincronização de tempo em setores críticos, como telecomunicações, transporte e energia. Um exemplo da relevância e da vulnerabilidade desses sistemas ocorreu em 2019, quando o petroleiro britânico Stena Impero foi apreendido por forças iranianas no Estreito de Ormuz. Após o incidente, análises sugerem que o navio pode ter sido vítima de um ataque de spoofing de GPS, que o fez desviar para águas iranianas, onde foi capturado [Lloyd's List 2020]. Casos assim evidenciam como o GPS civil está suscetível a ataques de interferência (jamming) ou de falsificação de sinal (spoofing) [Tippenhauer et al. 2008].

Com a popularização de rádios definidos por software (SDRs) no mercado, se torna ainda mais preocupante a possibilidade de ataques, já que esses dispositivos se tornaram relativamente acessíveis no mercado, além de portáteis. Modelos como o HackRF One, combinados com firmwares específicos (ex.: Mayhem) ou acoplados a módulos como PortaPack, podem operar de forma autônoma, tornando-se uma ferramenta de baixo custo e fácil transporte para gerar sinais de jamming. Isso representa um risco não apenas para infraestruturas consideradas críticas, mas também para várias aplicações cotidianas que dependem de GPS e GLONASS, desde sistemas de transporte até redes de telecomunicações que utilizam referências de tempo e posição fornecidas por esses satélites [Tippenhauer et al. 2008]. Nesse contexto, se mostra fundamental avaliar experimentalmente a suscetibilidade de receptores GNSS, em especial aqueles voltados ao uso de GPS e GLONASS, aos sinais de jamming gerados por SDRs de baixo custo. Este trabalho tem como objetivo apresentar uma análise do impacto desses ataques em receptores GNSS, apresentando aspectos como a perda de sinal e a degradação de desempenho, por meio da transmissão de sinais de jamming de implementação relativamente simples.

2. Fundamentação teórica

Nesta seção, apresenta-se de forma breve conceitos necessários para o desenvolvimento do artigo.

2.1. Sistema Global de Navegação por Satélite

Os sistemas GNSS fornecem informações precisas, contínuas e globais de posição tridimensional e de velocidade para os usuários que possuem algum equipamento receptor adequado, além disso disseminam o tempo de acordo com a escala de tempo do Tempo Universal Coordenado (UTC). As constelações globais do GNSS, às vezes chamadas de constelações principais, normalmente consistem em 24 ou mais satélites em órbita média da Terra (MEO), organizados em 3 ou 6 planos orbitais, com quatro ou mais satélites por plano [Kaplan and Hegarty 2017]. Entre os sistemas de navegação de maior destaque, estão presentes o GPS e o GLONASS. Adiante, são descritas suas principais características, respectivamente.

2.1.1. Global Positioning System

Os satélites GPS transmitem dados de navegação e códigos de medição por meio de modulação BPSK, além de usar Acesso Múltiplo por Divisão de Código (CDMA) para separar canais entre diferentes satélites[Kaplan and Hegarty 2017, Misra and Enge 2006]. São utilizadas duas portadoras principais, L1 e L2.

L1 — Calculada como $10,23\,\text{MHz} \times 154 = 1575,42\,\text{MHz}$, com comprimento de onda de aproximadamente 19 cm. Nessa portadora são transmitidos o código civil C/A (Coarse/Acquisition), de acesso aberto e o código de precisão P(Y), normalmente criptografado, além da mensagem de navegação.

L2 — Calculada como $10,23\,\text{MHz} \times 120 = 1227,60\,\text{MHz}$, com comprimento de onda de aproximadamente 24 cm. Essa portadora transmite apenas o código P(Y), utilizado em aplicações militares e restritas.

Além dos códigos de medição, os satélites enviam o almanaque, as efemérides e os dados de temporização. E devido à dispersão da energia (free space loss), os sinais chegam com níveis muito baixos, cerca de $-158,5$ dBW para o código C/A em L1 e -160 dBW para o código P(Y) em L2.

2.1.2. Globalnaya Navigatsionnaya Sputnikovaya Sistema

Os satélites GLONASS transmitem informações de navegação e códigos de medição utilizando modulação BPSK, mas diferem do GPS ao empregarem Acesso Múltiplo por Divisão de Frequência (FDMA) para separar os canais[Hofmann-Wellenhof et al. 2001, Misra and Enge 2006]. Portadoras e frequências:

L1 — A frequência L1 é definida pela fórmula

$$f_{L1} = 1602\,\text{MHz} + k \times 0.5625\,\text{MHz},$$

onde k é o número do canal, variando tipicamente de -7 a +6.

L2 — A frequência L2 é determinada de forma similar:

$$f_{L2} = 1246\,\text{MHz} + k \times 0.4375\,\text{MHz}.$$

Assim como o GPS, os satélites GLONASS transmitem dados como almanaque, efemérides e informações de temporização, possibilitando o posicionamento via trilateração.

2.2. Jammer

Um Jammer é um dispositivo capaz de bloquear ou interferir na recepção de sinais GNSS e o sinal de interferência em si é geralmente um ruído aleatório ou um sinal puro. Os bloqueadores funcionam emitindo um sinal de RF na mesma frequência esperada pelo dispositivo que está sendo bloqueado, mas com uma potência maior em comparação com o sinal normal. Então o dispositivo que está sendo bloqueado, receberá o sinal de maior potência que é do jammer e dessa forma os dispositivos podem deixar de funcionar corretamente [Pardhasaradhi and Kumar 2013].

2.3. Rádio Definido por Software

Um SDR é um sistema de comunicação de rádio flexível que permite o fácil processamento de sinais, no qual componentes normalmente implementados em hardware são executados por software em um computador ou sistema embarcado. Isso permite controlar diversas frequências de RF sem alterar o hardware[Zheng and Sun 2020]. A seguir, está uma breve descrição do hardware e do projeto de código aberto utilizados.

2.3.1. HackRF One

O HackRF One é um transceptor SDR de código aberto, com operação na faixa de 1 MHz a 6 GHz, permitindo tanto transmissão como recepção de sinais (half-duplex). Devido a uma ampla cobertura de frequências, ele consegue atuar nas bandas de navegação por satélite, como GPS L1 (1575,42 MHz) e GLONASS L1 (1.602 MHz). Além disso, apresenta taxa de amostragem de até 20 MS/s e se conecta ao computador via USB para alimentação e transferência de dados[Great Scott Gadgets].

2.3.2. Portapack H2+

O PortaPack H2+ permitiu ampliar as funcionalidades do HackRF One ao adicionar uma tela LCD, controles físicos como botões e joystick, entrada para cartão SD e um circuito de áudio[ShareBrained Technology]. O HackRF acoplado ao PortaPack pode operar de forma autônoma sem o uso constante do computador, é possível configurar e executar funções de transmissão ou recepção diretamente da interface gráfica, o que tornou viável a realização de experimentos em campo ou em laboratório de maneira mais prática.

2.3.3. Mayhem

O Mayhem é um firmware alternativo que expande as capacidades do PortaPack, adicionando diversas funcionalidades de análise de espectro, captura e transmissão[PortaPack Mayhem Project]. Entre elas, a função Jammer foi a principal utilizada por possibilitar gerar sinais de teste para GPS e GLONASS, por meio de configurações como a escolha de faixas de frequência e o tipo de sinal. Esses detalhes são descritos mais adiante na Seção 3.2, onde há a explicação de como essa função foi ajustada para os testes.

3. Metodologia

3.1. Descrição do Cenário

O experimento ocorreu em um ambiente controlado de dimensões com aproximadamente 20 m x 30 m em área aberta, optou-se por um local sem cobertura para garantir a melhor visibilidade dos satélites GNSS, permitindo a fixação do sinal com maior facilidade. Em relação às condições climáticas, nos dois dias de teste o clima estava ensolarado e com altas temperaturas, e o horário dos experimentos manteve-se em torno das 15h (horário de Brasília, UTC-3). A Figura 1 ilustra a disposição espacial: o HackRF (jammer) permaneceu a 1,70 m de altura em relação ao solo, enquanto as medições foram realizadas a cada 2 m, em incrementos até 28 m.

3.2. Ferramentas e Configurações

3.2.1. Fonte de sinal jamming

A utilização de SDRs para a geração de jamming GNSS já foi validada em experimentos práticos [Ferreira et al. 2020], confirmando que dispositivos como o HackRF apresentam capacidade suficiente para comprometer a integridade dos sinais de navegação. Desse modo, o dispositivo foi acoplado ao PortaPack H2+, utilizando a antena de uso geral ANT500, cuja faixa nominal de operação varia entre 75 MHz e 1 GHz [Great Scott Gadgets 2024].

Embora essa faixa esteja fora das frequências centrais dos sinais L1 de GPS e GLONASS, optou-se por sua utilização devido à praticidade, portabilidade e ao fato de ser fornecida junto ao HackRF como antena padrão. Ainda assim, os resultados obtidos demonstraram que a interferência

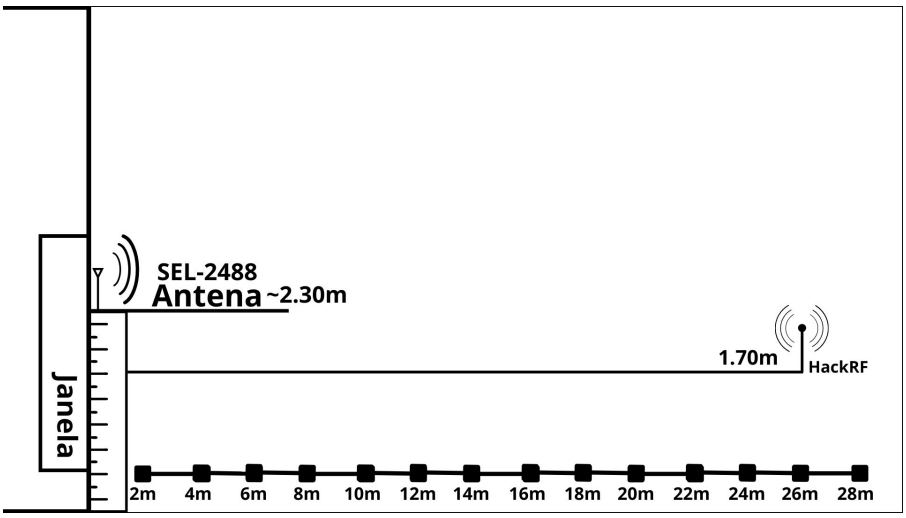

Figura 1. Disposição do ambiente físico do experimento

gerada foi suficiente para comprometer a recepção dos sinais GNSS em ambos os receptores testados, reforçando o risco associado ao uso de SDRs de baixo custo mesmo sem configurações otimizadas. Adicionalmente, embora a potência de transmissão não tenha sido medida diretamente, a documentação oficial do HackRF One indica que a potência de saída típica pode atingir até +10 dBm (10 mW), dependendo da frequência [Great Scott Gadgets]. Considerando o ganho configurado no jammer (30 dB), essa estimativa fornece uma dimensão prática da energia utilizada nos testes. Ressalta-se que, com o uso de uma antena sintonizada especificamente para a faixa L1 (como uma antena patch GPS), o alcance efetivo do ataque poderia ser potencialmente ampliado ou demandar ainda menos potência para causar interferência significativa.

Para viabilizar a portabilidade do dispositivo nos testes, a função jammer do firmware Mayhem foi configurada para gerar sinais de interferência contínua (portadora e/ou ruído) nas faixas de frequência L1 do GPS (1.575,42 MHz) e GLONASS (1.602 MHz). Nos experimentos, foram considerados três cenários principais de interferência: apenas GPS, apenas GLONASS e GPS/GLONASS simultaneamente. A seguir, as Tabelas 1 e 2 apresentam as configurações das variáveis utilizadas pela função Jammer em cada cenário:

Tabela 1. Configuração das variáveis da função Jammer (Banda Estreita)

Modo	Início	Centro	Fim	Largura	Tipo	Velocidade	Salto	TX	Repouso	Jitter	Ganho
GPS banda estreita	1575.42	1575.42	1575.42	0.00	Rand CW	10 kHz	50 ms	5 s	1 s	40/60	30 A:1
Glonass banda estreita	1602.50	1602.50	1602.50	0.00	Rand CW	10 kHz	50 ms	5 s	1 s	40/60	30 A:1

Tabela 2. Configuração das variáveis da função Jammer (Banda Larga)

Modo	Início	Centro	Fim	Largura	Tipo	Velocidade	Salto	TX	Repouso	Jitter	Ganho
Glonass banda larga	1595.00	1602.50	1610.00	15.00	Rand CW	100 kHz	50 ms	5 s	1 s	40/60	30 A:1
GPS banda larga	1570.42	1575.42	1580.42	10.00	Rand CW	100 kHz	100 ms	5 s	1 s	30/60	30 A:1

3.2.2. Receptores

A fim de representar de maneira complementar os efeitos da degradação do sinal por conta de interferências, são utilizados dois receptores GNSS, a aplicação móvel GPS Test e o relógio SEL-2488 de uso industrial. O aplicativo GPS Test permite a visualização de diferentes satélites de sistemas GNSS, além de monitorar em tempo real a quantidade de satélites visíveis e a precisão do posicionamento (CEP). Já o relógio industrial SEL-2488 é destinado a aplicações críticas, este dispositivo é responsável pela sincronização temporal via PPS, IRIG-B, NTP, PTP e registra alarmes operacionais

por meio de um dashboard web [Schweitzer Engineering Laboratories 2024]. A robustez deste dispositivo permite identificar a perda de sincronismo causada pela interferência e a rápida recuperação do lock após o término do jamming. Essa abordagem complementar possibilita comparar a vulnerabilidade de um receptor comercial com a resiliência de um sistema industrial, proporcionando uma análise abrangente dos impactos do jamming.

3.3. Procedimento Experimental

Nos testes, inicialmente foram configurados e ligados os receptores GNSS (aplicativo GPS Test e relógio industrial SEL-2488), além de se ajustar o HackRF One com PortaPack de acordo com as Tabelas 1 e 2 da seção 3.2 para gerar a interferência na faixa de frequência desejada. Após a primeira configuração, não foi necessário reiniciar os receptores nos próximos cenários, apenas houve o monitoramento do sinal quando retornava ao normal (quando havia perda de sincronismo) antes de passar para o próximo tipo de interferência. Dessa forma, o tempo de cada teste variava conforme a estabilização ou queda do sinal. Em cada posição de medição com distâncias crescentes a cada 2 m, até 28 m, ajustava-se apenas o HackRF para alternar entre os três cenários de jamming: GPS, GLONASS e ambos simultaneamente. Após observar o efeito da interferência por um período de em média 10 min em cada cenário, aumentava-se a distância até completar os incrementos planejados. A limitação de 28 m ocorreu por razões físicas do local, porque não seria possível manter as mesmas condições e posicionamento para distâncias maiores. A Figura 2 ilustra o procedimento do experimento.

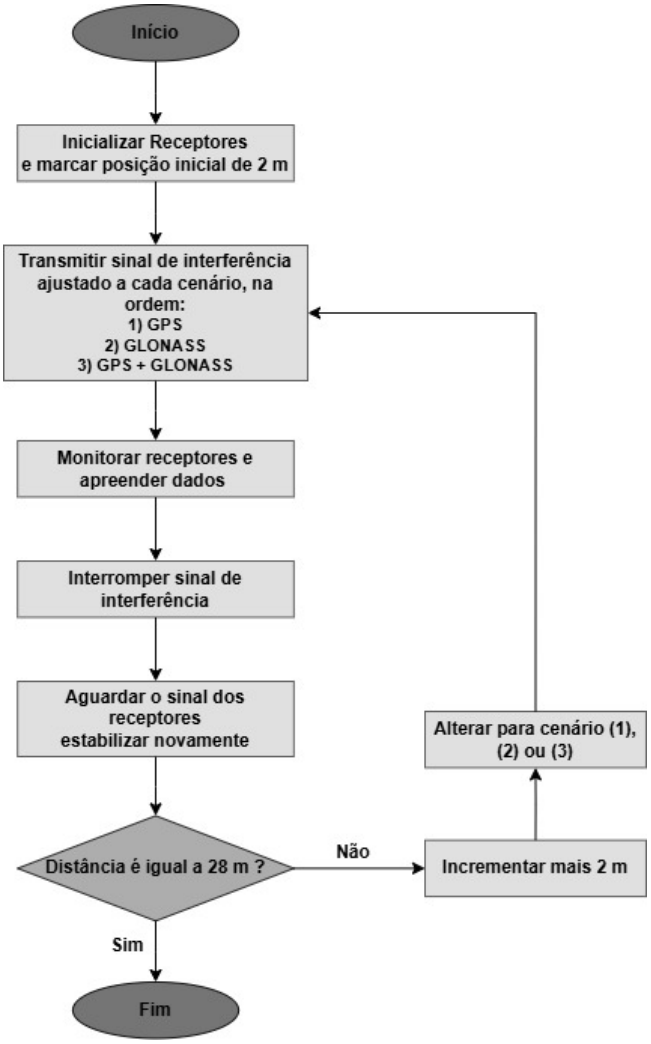

Figura 2. Fluxograma do experimento

3.4. Resultados

Para avaliar o impacto da interferência (jamming) nos receptores, foram considerados três cenários principais: (1) apenas GPS, (2) apenas GLONASS e (3) GPS/GLONASS simultaneamente, cobrindo distâncias de 2 m a 28 m como já mencionados na Seção 3.3. A Figura 3 ilustra o SEL-2488 antes da interferência e durante o jamming, enquanto a Figura 4 apresenta o GPS Test nessas mesmas condições. Ambas as figuras exibem a quantidade de satélites visíveis (View) e utilizados (Used), respectivamente, em cada distância e cenário.

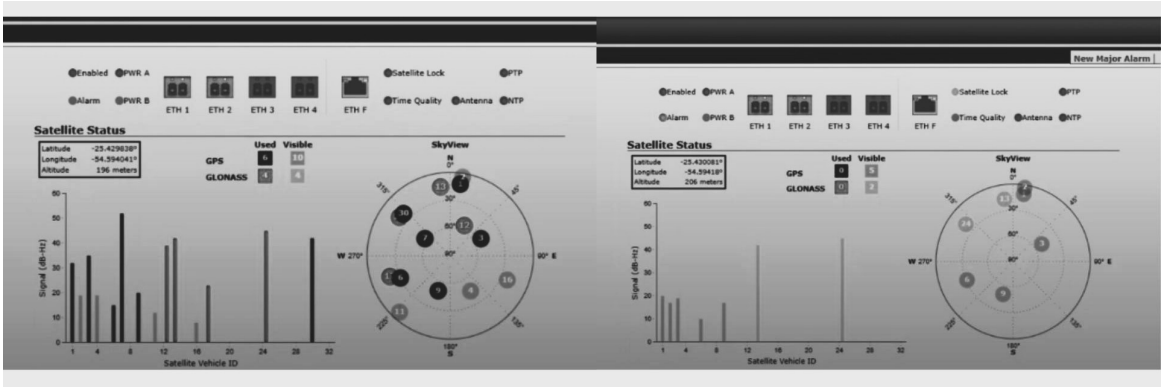

Figura 3. Dashboard SEL-2488

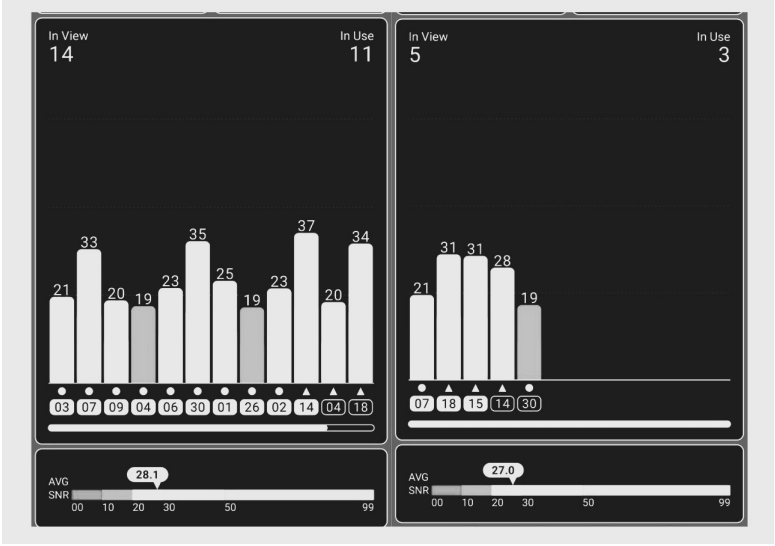

Figura 4. Interface do aplicativo GPS Test

Na Figura 3, observa-se o dashboard do SEL-2488 em condições normais, com 6 satélites GPS em uso e 4 GLONASS. Quando o jammer é ativado, o número de satélites em uso cai totalmente, causando perda de lock indicada no painel superior. De maneira similar, a Figura 4 mostra o aplicativo GPS Test detectando 14 satélites antes do jamming, já com o sinal de interferência, restam apenas 3 satélites em uso, a maioria com nível insuficiente para manter uma solução de posicionamento confiável. Essas imagens evidenciam a resposta imediata de cada receptor diante do jamming.

3.4.1. Análise do SEL-2488

Para cada uma das distâncias testadas, foram registrados o número de satélites visíveis (View) e utilizados (Used). As Figuras 5 e 6 mostram o comportamento do SEL-2488 antes e durante o ataque.

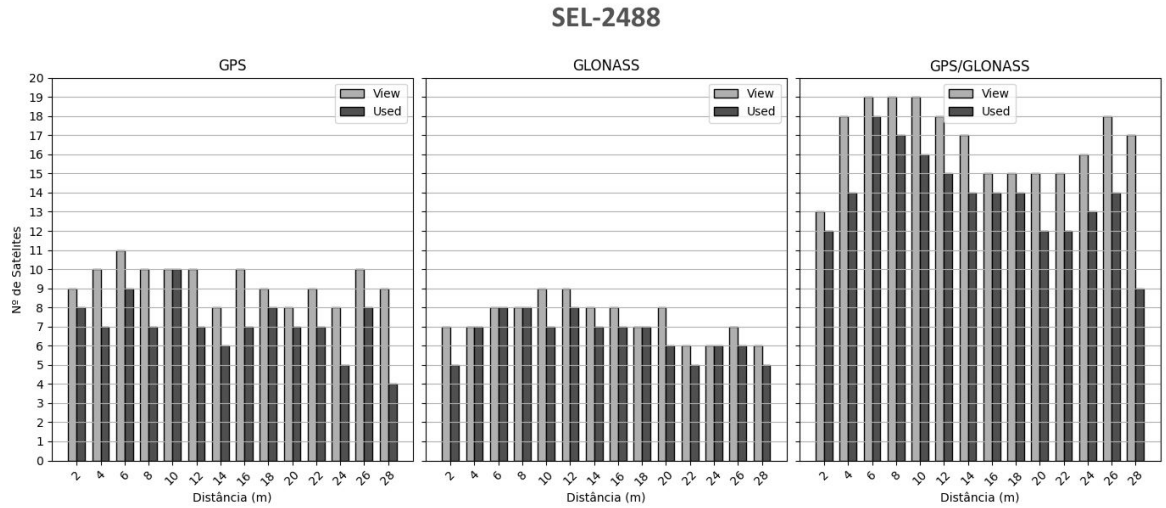

Figura 5. Número de satélites visíveis pelo SEL-2488 antes da transmissão do sinal de jamming

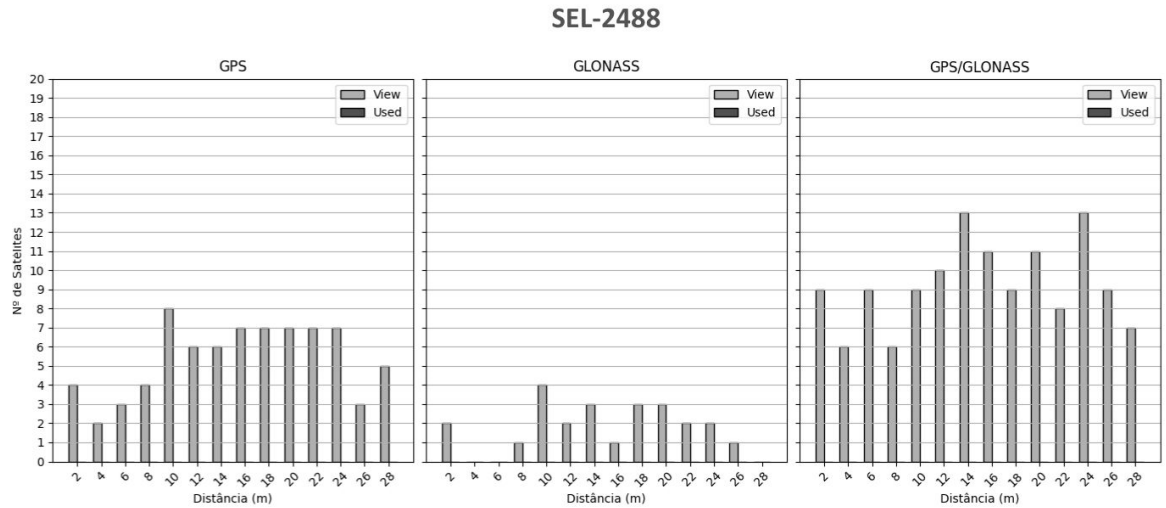

Figura 6. Número de satélites visíveis pelo SEL-2488 durante a transmissão do sinal de jamming

Ainda analisando o SEL-2488, observa-se que antes da transmissão do jamming o número de satélites visíveis e utilizados mantinha-se estável ao longo das diferentes distâncias, com pequenas variações naturais. Em condições normais, a média de satélites utilizados pelo dispositivo era superior a 14, com eficiência de uso acima de 85% dos satélites visíveis. Entretanto, durante a transmissão do sinal de interferência, houve uma queda na quantidade de satélites utilizados. As figuras mostram que, mesmo com alguns satélites ainda visíveis no céu, o SEL-2488 foi incapaz de manter a utilização efetiva desses sinais. O número de satélites usados reduziu a zero em todas as distâncias, resultando na perda total de sincronismo, como também indicado pelos alarmes de Holdover no dashboard. Essa degradação é evidenciada de maneira quantitativa ao calcular a eficiência de uso dos satélites. Antes da interferência, o dispositivo utilizava aproximadamente 85% dos satélites visíveis. Após o início do jamming, essa eficiência caiu para 0%, demonstrando o impacto crítico da interferência mesmo em equipamentos de nível industrial.

3.4.2. Análise do GPS Test

As Figuras 7 e 6 apresentam o comportamento do aplicativo GPS Test antes e durante a transmissão do sinal de jamming. Antes da interferência, a média de satélites utilizados era de 9,15, com uma

eficiência de uso em torno de 79%. Durante o jamming, essa média caiu para 3,31 satélites utilizados, com eficiência reduzida para aproximadamente 47%. Embora o GPS Test tenha conseguido manter a utilização de alguns satélites mesmo sob interferência, a qualidade da solução de posicionamento foi comprometida.

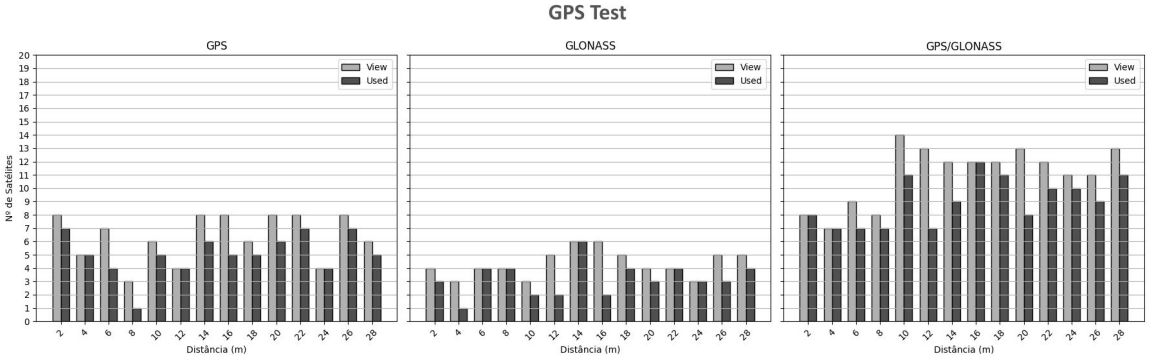

Figura 7. Número de satélites visíveis pelo GPS Test antes da transmissão do sinal de jamming

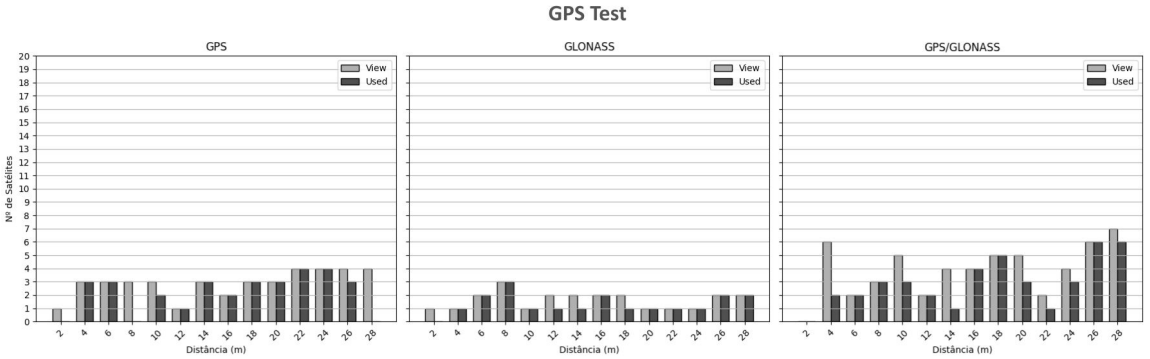

Figura 8. Número de satélites visíveis pelo GPS Test durante a transmissão do sinal de jamming

4. Conclusão

Este trabalho apresentou uma análise experimental da vulnerabilidade de receptores GNSS a sinais de jamming gerados por SDRs de baixo custo. Utilizando o aplicativo GPS Test e o relógio industrial SEL-2488, foram avaliados três cenários de interferência (GPS, GLONASS e ambos simultaneamente), dessa forma demonstrando que mesmo receptores projetados para aplicações críticas podem ser suscetíveis a degradação dos sinais. Os resultados mostraram perdas significativas de desempenho, com o SEL-2488 apresentando perda total de sincronismo e o GPS Test que possuiu redução acentuada no número de satélites utilizados, o que comprometeu sua precisão do posicionamento.

Esses resultados comprovam que dispositivos acessíveis como o HackRF One, representam uma ameaça real a confiabilidade de sistemas que dependem de navegação e temporização via GNSS, assim reforçando a necessidade de adotar mecanismos de mitigação e monitoramento, como filtros digitais, detecção de anomalias e redundância de fontes temporais. Recomenda-se expandir os experimentos para diferentes potências de transmissão, antenas dedicadas e múltiplas constelações, a fim de quantificar melhor o alcance e a severidade dos ataques. O estudo contribui para a compreensão prática dos impactos do jamming e destaca a importância de estratégias de resiliência e segurança para preservar a disponibilidade e integridade de sistemas baseados em sincronização com satélites.

Referências

Ferreira, R., Gaspar, J., Sebastião, P., and Souto, N. (2020). Effective gps jamming techniques for uavs using low-cost sdr platforms. *Wireless Personal Communications*. Published online: 6 March 2020.

Great Scott Gadgets. Hackrf one documentation. https://hackrf.readthedocs.io/en/latest/hackrf_one.html. Accessed: 2025-03-11.

Great Scott Gadgets (2024). Ant500: Telescopic antenna for sdr. https://www.greatscottgadgets.com/ant500/. Accessed: 2025-03-01.

Hofmann-Wellenhof, B., Lichtenegger, H., and Wasle, E. (2001). *GNSS – Global Navigation Satellite Systems: GPS, GLONASS, Galileo and more*. Springer.

Kaplan, E. D. and Hegarty, C. J. (2017). *Understanding GPS/GNSS: Principles and Applications*. Artech House, 3rd edition.

Lloyd's List (2020). Seized uk tanker likely spoofed by iran. https://www.lloydslist.com/LL1128820/Seized-UK-tanker-likely-spoofed-by-Iran. Accessed: 2025-04-01.

Misra, P. and Enge, P. (2006). *Global Positioning System: Signals, Measurements, and Performance*. Ganga-Jamuna Press.

Montenbruck, O. and Teunissen, P. J., editors (2017). *Springer Handbook of Global Navigation Satellite Systems*. Springer.

of Defense, D. (2008). Global positioning system standard positioning service performance standard. Technical report, U.S. Government. Available at: https://www.gps.gov/technical/ps/2008-SPS-performance-standard.pdf.

Pardhasaradhi, A. and Kumar, R. (2013). Signal jamming and its modern applications. *International Journal of Science and Research (IJSR)*, 2(4):429–431.

PortaPack Mayhem Project. Mayhem firmware for portapack. https://github.com/portapack-mayhem/mayhem-firmware. Accessed: 2025-03-11.

Schweitzer Engineering Laboratories (2024). Sel-2488 satellite-synchronized network clock - data sheet. Technical report, Schweitzer Engineering Laboratories, Inc., Pullman, WA, USA. Available at: https://selinc.com, Accessed: 2025-04-01.

ShareBrained Technology. Portapack for hackrf one. https://github.com/sharebrained/portapack-hackrf. Accessed: 2025-03-11.

Tippenhauer, N. O., Pöpper, C., Rasmussen, K. B., and Čapkun, S. (2008). On the requirements for successful gps spoofing attacks. In *Proceedings of the 15th USENIX Security Symposium*, pages 1–16.

Zheng, X.-C. and Sun, H.-M. (2020). Hijacking unmanned aerial vehicle by exploiting civil gps vulnerabilities using software-defined radio. *Sensors and Materials*, 32(8):2729–2743.