SOFTWARE DE ALARME DE *SPOOFING* DE GNSS: UMA ABORDAGEM EFICIENTE DE BAIXO CUSTO

GNSS spoofing alarm software: an efficient low-cost approach

Antônio Pedro Santos Dias de Carvalho[1], **Luis Gustavo Ronsani Vito**[2]

Resumo: Este artigo apresenta um sistema de alarme para detecção de *spoofing* (falsificação) em sinais do Sistema Global de Navegação por Satélite (GNSS), baseado na verificação da consistência entre a distância percorrida por um veículo entre amostras consecutivas e sua velocidade máxima operacional declarada. O sistema utiliza um *script* (rotina) em Python para coletar dados de localização a cada segundo e calcular a velocidade instantânea. Se a velocidade calculada ultrapassar o limite operacional do veículo, um alarme é acionado com a mensagem "ALERTA DE *SPOOFING*!". Para aumentar a confiabilidade, o algoritmo incorpora suavização por média móvel exponencial, validação da precisão horizontal e uma lógica que detecta discrepâncias em amostras consecutivas, reduzindo falsos positivos. Testes realizados com dados de GNSS de um smartphone Motorola, um módulo GPS u-blox NEO-6M e um GPS marítimo Furuno GP-90 demonstraram a eficácia do sistema na detecção de anomalias. O *software* apresenta baixo custo e facilidade de implementação, mostrando potencial para aplicação em diversos tipos de veículos em ambientes com baixa interferência multipercurso.

Palavras-chave: *Spoofing*. Alarme. Navegação. GNSS. Velocidade.

Abstract: This article presents an alarm system for detecting Global Navigation Satellite System (GNSS) spoofing signals, based on verifying the consistency between the distance traveled by a vehicle between consecutive samples and its declared maximum operational speed. The system uses a Python script to collect location data every second and calculate the instantaneous speed. If the calculated speed exceeds the vehicle's operational limit, an alarm is triggered displaying the message "SPOOFING ALERT!". To increase reliability, the algorithm incorporates exponential moving average smoothing, horizontal accuracy validation, and a logic that detects discrepancies in consecutive samples, reducing false positives. Tests conducted with GNSS data from a Motorola smartphone, a u-blox NEO-6M GPS module, and a Furuno GP-90 marine GPS demonstrated the system's effectiveness in anomaly detection. The software is low-cost and easy to implement, showing potential for application in various types of vehicles in environments with low multipath interference.

Keywords: Spoofing. Alarm. Navigation. GNSS. Speed.

1. Capitão de Corveta. Mestre em Guerra Eletrônica pelo Instituto Tecnológico de Aeronáutica. Encarregado da Seção de Inteligência Eletrônica no Centro de Guerra Acústica e Eletrônica da Marinha, Rio de Janeiro, RJ – Brasil. E-mail: pedro.antonio@marinha.mil.br

2. Capitão de Corveta. Mestre em Guerra Eletrônica e Sensoriamento Remoto pelo Instituto Tecnológico de Aeronáutica. Adido da Marinha do Brasil no Programa de Pós-Graduação em Aplicações Operacionais do Instituto Tecnológico de Aeronáutica, São José dos Campos, SP – Brasil. E-mail: luis.vito@marinha.mil.br

1. INTRODUÇÃO

Em um mundo cada vez mais dependente da tecnologia, o Sistema Global de Navegação por Satélite (GNSS, Global Navigation Satellite System) tornou-se fundamental para diversas operações civis e militares. Além de orientar a navegação, o GNSS sustenta sistemas essenciais em transporte terrestre, aéreo e marítimo, guiagem de munições, sincronização de redes elétricas, infraestrutura financeira e monitoramento de equipamentos (DIAS DE CARVALHO, 2023). Essa ampla utilização torna o GNSS um recurso crítico e insubstituível para a sociedade moderna. Entretanto, essa dependência também expõe vulnerabilidades significativas, especialmente diante dos ataques de *spoofing*. Esses ataques consistem na emissão de sinais falsificados que imitam os sinais legítimos do GNSS, levando receptores a calcular posições ou horários incorretos. Como resultado, veículos, *drones* e sistemas de armas podem ser desorientados, causando falhas operacionais e comprometendo missões estratégicas (C4ADS, 2019; DIAS DE CARVALHO, 2023). O conflito atual entre Rússia e Ucrânia exemplifica o uso estratégico dessa ameaça. Ambas as partes têm empregado ataques de *spoofing* para desviar *drones*, proteger bases militares e confundir sistemas inimigos, evidenciando o impacto tangível e crescente dessa técnica em cenários atuais de guerra (GPS WORLD, 2022; KYIV INDEPENDENT, 2024; LO *et al.*, 2025). A Figura 1 ilustra os destroços de um *drone* abatido em decorrência de um ataque de *spoofing* (NEW SCIENTIST, 2021).

Fonte: New Scientist (2021).

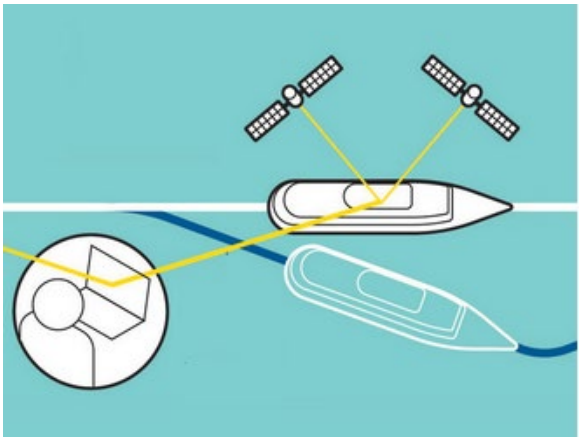
Figura 1. Destroços de um *drone* abatido em virtude de ataque *spoofing*.

Diferentemente do *jamming*, que bloqueia completamente os sinais GNSS, o *spoofing* é mais perigoso e difícil de detectar, pois engana o receptor com sinais aparentemente válidos, fazendo-o funcionar de forma incorreta e muitas vezes sem suspeitas (PSIAKI; HUMPHREYS, 2016). Essa sutileza torna o *spoofing* uma ameaça crítica para setores que dependem da precisão do GNSS, como transporte e defesa.

A Figura 2 apresenta, de forma simplificada, os efeitos de um ataque de *spoofing* contra uma embarcação, mostrando como o deslocamento aparente pode ser manipulado por agentes mal-intencionados (PSIAKI; HUMPHREYS, 2016). Diante desse cenário, o desenvolvimento de métodos eficazes para a detecção e mitigação do *spoofing* em sinais de GNSS torna-se essencial para garantir a segurança operacional e a integridade das missões militares.

2. OBJETIVO

Este estudo teve como objetivo desenvolver e validar um sistema de alarme para detecção de *spoofing* em sinais de GNSS, baseado na análise de consistência do deslocamento calculado entre amostras consecutivas e a velocidade máxima operacional declarada do veículo. Para isso, um *script* em Python coleta dados de localização a uma taxa de 1 Hz, calculando a distância percorrida entre pontos consecutivos. A velocidade instantânea é comparada ao limite máximo informado pelo usuário e, caso ultrapassado, o sistema dispara



Fonte: Psiaki e Humphreys (2016).

Figura 2. Efeitos do ataque *spoofing*.

um alerta indicando possível *spoofing*. A validação do sistema foi realizada com dados coletados de três tipos distintos de receptores GNSS: um smartphone Motorola, um módulo GPS u-blox NEO-6M acoplado a uma placa Arduino e um GPS marítimo Furuno GP-90, todos testados em ambientes operacionais representativos. Os resultados indicam que a solução é eficaz na detecção de anomalias relacionadas ao *spoofing*, possui baixo custo e é facilmente implementável, exigindo apenas um dispositivo computacional para a execução do *software*. Ao receber o alerta, recomenda-se a utilização imediata de métodos alternativos de navegação, como técnicas visuais ou inerciais, para garantir a segurança e a confiabilidade das operações.

3. METODOLOGIA

A arquitetura aberta do GNSS o torna intrinsecamente vulnerável a ataques de *spoofing*, uma ameaça que é frequentemente subestimada em diversos contextos (WU *et al.*, 2020). Essa negligência é particularmente prevalente em sistemas embarcados de baixo custo, nos quais a implementação de soluções robustas de mitigação pode ser economicamente inviável. As contramedidas de *spoofing* atualmente empregadas operam predominantemente em dois níveis: no nível do sinal ou no nível dos dados (WU *et al.*, 2020). Inserido nesse cenário, o presente trabalho propõe uma abordagem de detecção de *spoofing* no nível de dados que se destaca por sua simplicidade, acessibilidade e eficácia. A metodologia baseia-se em um princípio lógico e físico fundamental: todo meio de transporte possui uma velocidade máxima operacional que, se excedida, implicaria uma violação das leis da física ou dos limites estruturais do próprio veículo. Com base na premissa supracitada, foi desenvolvido um sistema em Python para analisar a coerência entre pontos sucessivos de navegação por GNSS. O processo de coleta de dados envolveu a aquisição de coordenadas de GNSS em intervalos de um segundo. O instrumento a ser utilizado para essa coleta pode ser qualquer dispositivo GNSS capaz de fornecer dados de posicionamento em série temporal.

O *script* em Python, desenvolvido especificamente para este estudo, verifica se a distância percorrida entre dois pontos consecutivos, calculada com base nas coordenadas GNSS, é consistente com uma velocidade máxima previamente definida pelo usuário. Essa velocidade máxima atua como um limite de coerência. Caso a velocidade calculada exceda o limite máximo definido, o sistema sinaliza a ocorrência de um potencial ataque de *spoofing*. A Figura 3 apresenta um fluxograma simplificado do funcionamento do *script* de detecção de *spoofing*.

3.1. PRINCÍPIO DE FUNCIONAMENTO

A solução proposta foi desenvolvida em Python e opera com base na análise da coerência entre pontos de navegação sucessivos. O usuário deve informar previamente a velocidade máxima que seu veículo pode atingir (em km/h, m/s ou nós). A cada segundo, o sistema coleta a latitude e a longitude da posição atual e, com uma taxa de amostragem de 1 Hz, calcula a distância em relação ao ponto anterior. Esse cálculo é feito por meio da fórmula de Haversine, que considera a curvatura da Terra e fornece resultados precisos para deslocamentos curtos ou longos (Equação 1):

$$d = 2R \cdot \arcsin\left(\sqrt{\sin^2\left(\frac{\Delta\varphi}{2}\right) + \cos(\varphi_1) \cdot \cos(\varphi_2) \cdot \sin^2\left(\frac{\Delta\lambda}{2}\right)}\right) \quad (1)$$

Onde:
d: distância entre dois pontos (em metros);
R: raio da Terra ≈ 6.371.000 metros;
φ_1, φ_2: latitudes dos pontos 1 e 2 (em radianos);
λ_1, λ_2: longitudes dos pontos 1 e 2 (em radianos);
$\Delta\varphi$: $\varphi_2 - \varphi_1$;
$\Delta\lambda$: $\lambda_2 - \lambda_1$.

3.2. VALIDAÇÃO E TESTES

Para validar o sistema, foram utilizados três tipos distintos de receptores GNSS: um smartphone Motorola; um módulo GPS u-blox NEO-6M acoplado a uma placa Arduino; e o Furuno GP-90, navegador GPS marítimo de uso profissional.

Para validar a eficácia do sistema proposto, foram realizados testes que englobaram duas abordagens principais: cenários reais e simulações controladas. A coleta de dados nos cenários reais envolveu o monitoramento de deslocamentos abruptos. Utilizaram-se, para isso, dispositivos de rastreamento veicular padrão, que registram continuamente a velocidade e a posição dos veículos. Em paralelo, foram desenvolvidas simulações com dados manipulados artificialmente. Essa abordagem permitiu criar condições controladas e reproduzir um espectro mais amplo de anomalias de velocidade, garantindo a robustez do sistema. A técnica de análise

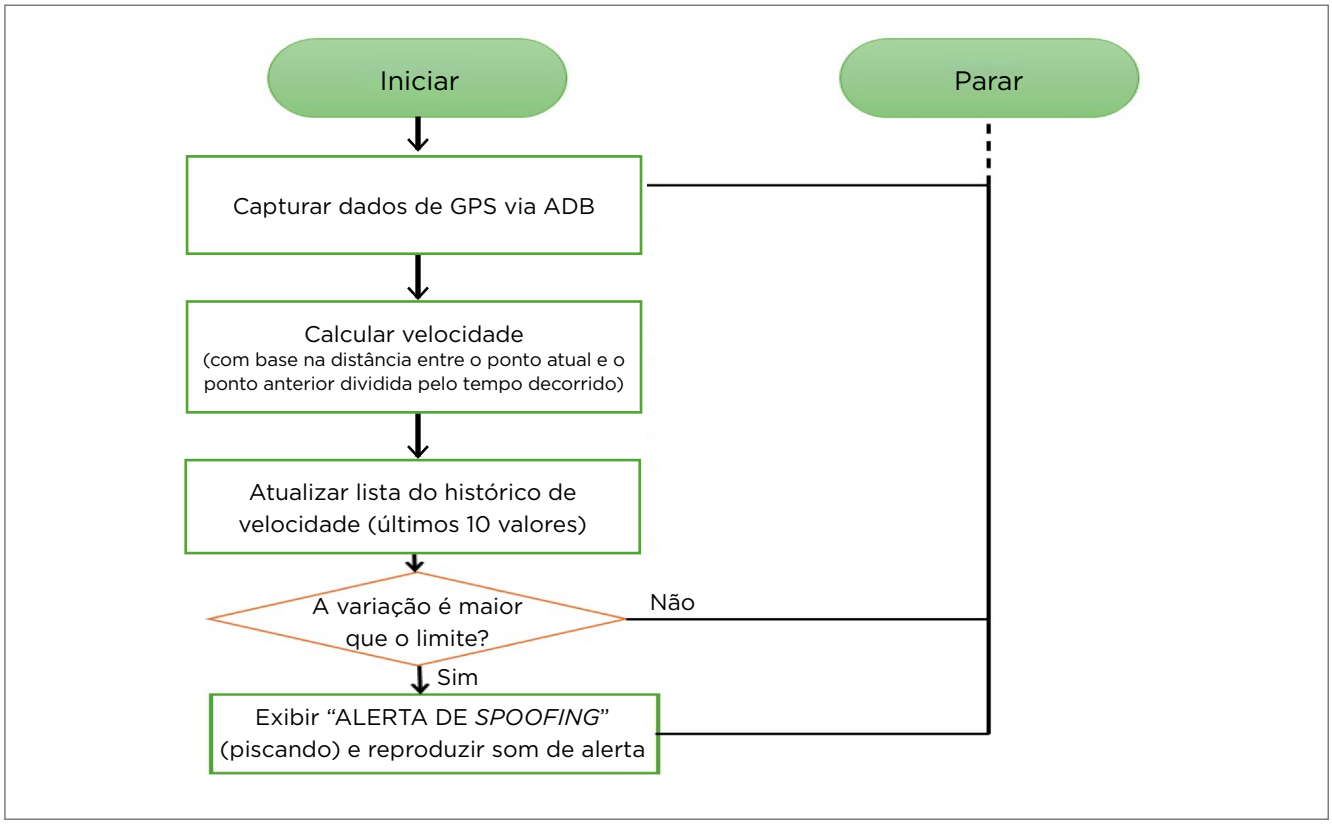


Figura 3. Fluxograma do *script* da detecção de *spoofing* do *software*.

de dados empregada é baseada em lógica física elementar. Desvios significativos em relação a esse critério seriam prontamente identificados como anomalias. Essa metodologia dispensa a necessidade de equipamentos complexos, como múltiplas antenas ou redes neurais avançadas, e não requer bancos de dados extensos de padrões de sinal. Um dos principais diferenciais desta solução reside em seu baixo custo. Ao contrário de outras abordagens que frequentemente exigem infraestruturas complexas ou algoritmos computacionalmente onerosos, a dependência exclusiva de lógica física básica torna-a universalmente aplicável a qualquer tipo de veículo. Essa característica contribui significativamente para sua acessibilidade e escalabilidade. Além do bom desempenho na detecção de anomalias, a solução também se concentrou na flexibilidade de integração. O *script* subjacente pode ser facilmente incorporado a diversas plataformas já existentes, tais como sistemas de monitoramento em tempo real, painéis de navegação veicular ou aplicativos de rastreamento. Essa capacidade de integração otimiza a implementação e o uso do sistema em diferentes contextos operacionais.

3.3. APLICAÇÕES DIDÁTICAS E EDUCACIONAIS

Além do uso operacional, o sistema também se mostra valioso como ferramenta didática. Alunos de cursos técnicos ou superiores podem aplicar conceitos de física, geolocalização, segurança cibernética (ataque e proteção) e programação embarcada em um contexto prático, com *feedback* instantâneo. A visualização do comportamento do sistema em diferentes cenários permite compreender os limites operacionais do GNSS e reforça a importância da navegação segura, bem como da operação coordenada de sistemas integrados de geração, transmissão e distribuição de energia, de sistemas de vigilância com *drones* e outros equipamentos, sistemas financeiros, etc.

3.4. MINIMIZAÇÃO DE FALSOS POSITIVOS

Os GNSS mais comumente utilizados são GPS, Galileo, BeiDou e GLONASS. Considerando que o erro mais grosseiro entre tais sistemas de navegação é de aproximadamente 15 metros, para o GPS, foram implementadas medidas para

mitigar alarmes falsos (RUSSIAN FEDERAL SPACE AGENCY, 2019; CHINA SATELLITE NAVIGATION OFFICE, 2020; EUROPEAN UNION, 2021; U.S. GOVERNMENT, 2025). Os dados coletados foram analisados sequencialmente para calcular médias móveis de velocidade, variando-se o número de amostras de acordo com a velocidade do meio de transporte. Se um ponto se desviar significativamente, tanto dos dados anteriores quanto dos posteriores, é descartado como *spike* (erro GNSS). Como esses erros são raros em ambientes marítimos ou aéreos, onde os efeitos de multipercurso são mínimos, não foi necessário considerar erros sucessivos de 15 metros. As Figuras 4 e 5 demonstram, respectivamente, a tela de operação normal do *software* e a interface do *software* com o alerta de ataque de *spoofing*:

3.5. INTEGRAÇÃO NÃO INTRUSIVA

É importante destacar que o sistema foi concebido para operar de forma não intrusiva, sem necessidade de modificar a estrutura física ou lógica dos veículos. Toda a análise é realizada em dispositivos móveis, como celulares ou laptops do operador. No caso de *drones*, por exemplo, o *script* é executado diretamente no smartphone conectado ao controle remoto, que já recebe os dados de posição da aeronave. Isso permite a integração do sistema sem alterar o funcionamento do veículo, mantendo a arquitetura de controle totalmente intacta.

3.6. CONSIDERAÇÕES SOBRE ATAQUES AVANÇADOS

Embora em teoria seja possível que um ataque de *spoofing* seja iniciado com precisão, isto é, exatamente no tempo e local onde o receptor deveria estar, na prática, isso é altamente improvável. Esse tipo de ataque exigiria acesso antecipado e detalhado à trajetória do alvo, incluindo latitude, longitude e horários exatos, além de sincronização temporal em nível milimétrico. Mesmo em ambientes controlados, as dificuldades logísticas e os atrasos naturais na emissão de sinais falsificados tornam a execução quase inviável. Além disso, em cenários operacionais como portos, canais dragados ou regiões costeiras, os *drones* frequentemente utilizam referências visuais ou técnicas de mapeamento simultâneo (SLAM visual), o que reduz ainda mais a dependência exclusiva do GNSS e dificulta o sucesso de ataques sofisticados.

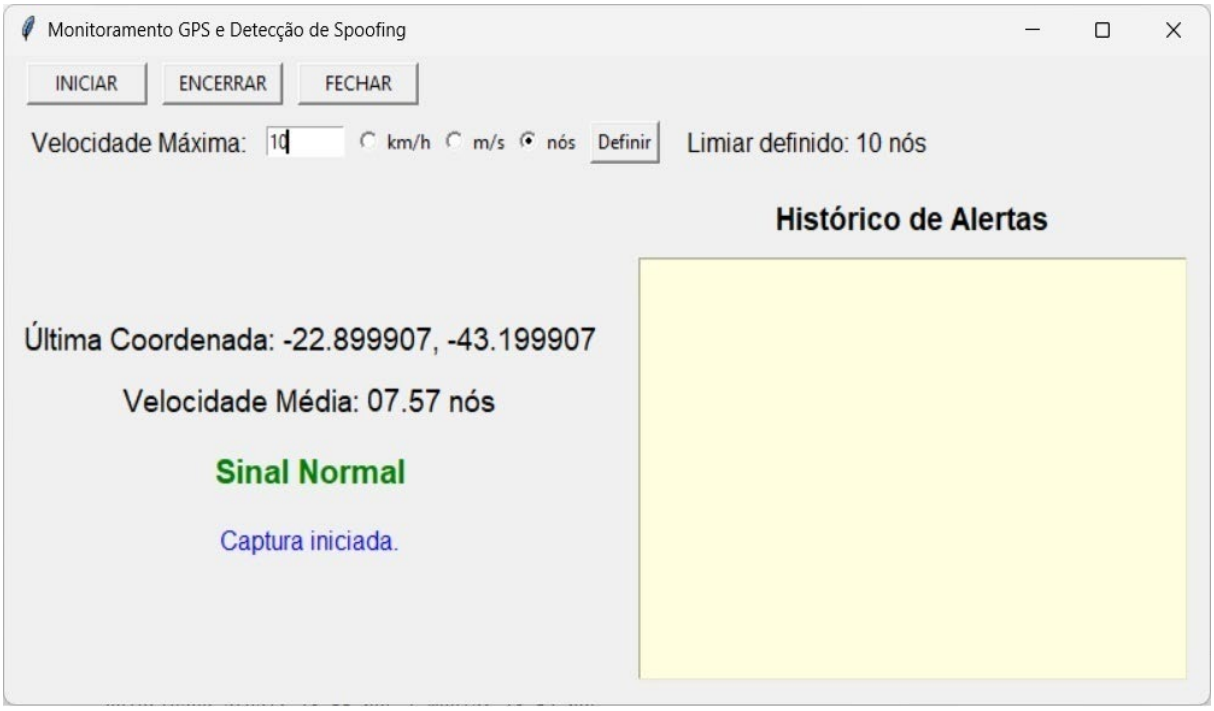


Figura 4. Tela de operação normal.

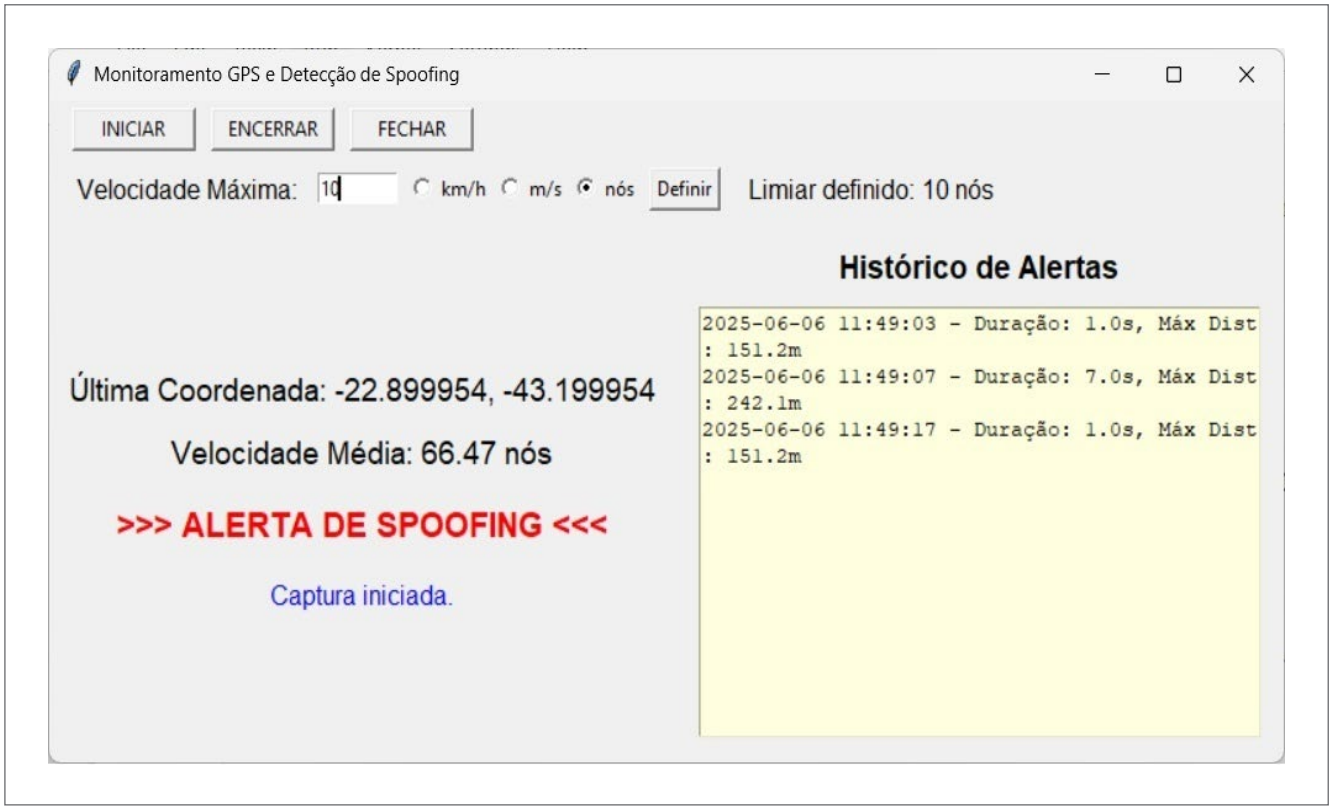


Figura 5. Tela de alerta de ataque de *spoofing* e histórico de alertas.

Dessa forma, mesmo diante de um hipotético ataque de nível 2, no qual o atacante possui conhecimento prévio da posição e velocidade do receptor, a probabilidade de êxito sem a ativação do alerta é extremamente baixa, devido às limitações tecnológicas e ambientais que são naturalmente envolvidas.

4. RESULTADOS

Os testes realizados com o *software* de detecção de *spoofing* em sinais GNSS permitiram avaliar seu desempenho com base em três indicadores principais: falsos positivos, falsos negativos e tempo médio de alerta (ATA, *average time to alert*). A seguir, são apresentados os resultados observados, com destaque para a confiabilidade e a agilidade da solução em cenários operacionais.

4.1. FALSO POSITIVO

Em todo o processo de validação, nenhum alerta indevido foi registrado. Falsos positivos ocorrem quando o sistema indica uma ameaça inexistente, o que pode levar à mobilização desnecessária de recursos e à sobrecarga das equipes. Para evitar esse tipo de erro, o algoritmo foi projetado com base em uma média móvel de pontos GNSS anteriores, em vez de simplesmente comparar pares consecutivos. Esse método, ajustado conforme a velocidade da plataforma, considera o erro típico dos sistemas GNSS — como o GPS, com margem de até 15 metros — para distinguir variações normais de movimentação de comportamentos suspeitos. A escolha dessa abordagem se mostrou acertada: em 30 testes realizados com plataformas móveis, não foi identificado nenhum falso positivo, demonstrando a eficácia da técnica mesmo em situações reais de deslocamento.

4.2. FALSO NEGATIVO

A detecção de ameaças também apresentou desempenho exemplar. Em todas as simulações de *spoofing*, o sistema foi capaz de identificar corretamente as inconsistências introduzidas no sinal. Diferentemente dos falsos positivos, que indicam ameaças inexistentes, os falsos negativos representam o não

reconhecimento de um ataque real — o que comprometeria seriamente a segurança operacional. O fato de o sistema não ter deixado passar nenhuma tentativa de *spoofing* evidencia sua robustez diante de diferentes padrões e níveis de complexidade das interferências simuladas.

4.3. TEMPO DE ALERTA

O tempo médio entre a identificação de uma ameaça e a emissão do alerta variou entre 5 e 20 segundos, dependendo da velocidade da plataforma monitorada. Na prática, esse intervalo representa uma defasagem de cerca de 75 metros para veículos a 55 km/h; aproximadamente 33 metros para deslocamentos a 6 km/h; e 0 (zero) metro para velocidades superiores a 55 km/h, graças à adaptação dinâmica do algoritmo.

Essa latência foi considerada aceitável para o uso operacional pretendido. O *script* ajusta automaticamente a quantidade de pontos analisados de acordo com a velocidade do deslocamento, equilibrando precisão e rapidez. Com isso, o sistema evita tanto atrasos que poderiam comprometer a resposta quanto decisões precipitadas baseadas em dados insuficientes.

5. CONCLUSÕES

A crescente dependência de sistemas de navegação baseados em GNSS em setores estratégicos como transporte, logística, energia, agricultura de precisão e defesa revela uma vulnerabilidade crítica: a suscetibilidade a ataques de *spoofing*. Esses ataques, que consistem na transmissão de sinais falsificados com o objetivo de enganar os receptores, podem comprometer a eficiência operacional e a segurança de usuários e equipamentos.

Como resposta a esse desafio, este trabalho apresentou uma abordagem prática e acessível para detectar inconsistências na trajetória registrada por dispositivos GNSS. A solução desenvolvida compara a distância percorrida com a velocidade máxima previamente definida pelo usuário, a fim de identificar deslocamentos incoerentes que possam indicar tentativa de *spoofing*. A implementação, realizada por meio de um *script* em Python, utiliza dados GNSS coletados a cada segundo, o que permite uma análise contínua e em tempo quase real.

Durante os testes, realizados com diferentes plataformas — incluindo um smartphone, um módulo u-blox NEO-6M com Arduino e um navegador marítimo Furuno GP-90 — o sistema demonstrou alta confiabilidade. Os alertas foram emitidos somente diante de desvios anômalos, sem ocorrência de falsos positivos, mesmo na ausência de tecnologias avançadas como aprendizado de máquina ou sensores múltiplos.

A principal contribuição deste trabalho está na proposta de um método alternativo, de baixo custo e fácil implementação, que pode complementar soluções GNSS mais robustas. Uma vez emitido o alerta, recomenda-se a adoção de medidas imediatas de mitigação, como a navegação inercial (KAPLAN; HEGARTY, 2016) ou, em último caso, navegação visual. A abordagem proposta estabelece também uma base sólida para aplicações futuras em áreas como guerra eletrônica, vigilância patrimonial, cibersegurança, navegação autônoma e sensoriamento remoto.

6. PERSPECTIVAS PARA PESQUISAS FUTURAS

Para aumentar a eficácia da solução proposta, recomenda-se sua integração com sistemas de navegação inercial, especialmente em ambientes onde o sinal GNSS é instável, como áreas urbanas densas, túneis, regiões marítimas e condições climáticas adversas. A fusão com sensores inerciais pode melhorar a confiabilidade do posicionamento em cenários com interferência ou degradação do sinal.

Outra possibilidade é o desenvolvimento de um mecanismo de filtragem capaz de identificar e neutralizar sinais falsos de *spoofing*, preservando ao menos quatro sinais autênticos para manter a solução de posicionamento. Mesmo que alguns sinais legítimos sejam descartados, o foco seria garantir a integridade dos dados essenciais.

A adoção de processadores GNSS mais avançados, como os módulos u-blox M10 e Venus838FLPx, também pode fortalecer a robustez do sistema. Esses dispositivos oferecem maior sensibilidade, suporte multiconstelação e melhor desempenho em ambientes com ruído, além de compatibilidade com plataformas como Arduino e Raspberry Pi. Com maiores taxas de amostragem, esses módulos permitem reduzir a latência de detecção e ampliar a precisão.

Por fim, a utilização de processadores com mitigação de efeitos de multipercurso representa uma melhoria relevante, sobretudo em áreas urbanas, onde esse tipo de interferência compromete significativamente a precisão do GNSS.

REFERÊNCIAS

C4ADS. *Above us only start:* exposing GPS spoofing in Russia and Syria. 2019. Disponível em: https://c4ads.org/above-us-only-start. Acesso em: 19 abr. 2025.

CHINA SATELLITE NAVIGATION OFFICE. *BeiDou navigation satellite system signal in space interface control document*. Version 3.0. CNSA, 2020. Disponível em: http://en.beidou.gov.cn/SYSTEMS/ICD/. Acesso em: 21 maio 2025.

DIAS DE CARVALHO, A. P. S. *Mitigation of SPOOFING EFFECT in GNSS in pre-correlation*. 2023. Dissertação (Mestrado) – Instituto Tecnológico de Aeronáutica, São José dos Campos, 2023.

EUROPEAN UNION. *Galileo open service signal in space interface control document*. 2. ed. European GNSS Agency, 2021. Disponível em: https://www.gsc-europa.eu/system/files/galileo-os-sis-icd_v2.0.pdf. Acesso em: 21 maio 2025.

GPS WORLD. Ukraine attacks changed Russian GPS jamming. *GPS World*, 2022. Disponível em: https://gpsworld.com/article-link. Acesso em: 21 maio 2025.

KAPLAN, E. D.; HEGARTY, C. J. *Understanding GPS:* principles and applications. 2. ed. Boston: Artech House, 2006.

KYIV INDEPENDENT. Ukrainian GPS spoofing for repelling drone attacks could indirectly affect smartphone clock. *Kyiv Independent*, 2024. Disponível em: https://kyivindependent.com/article-link. Acesso em: 21 maio 2025.

LO, S.; LIU, Z.; IBRAHIM, L.; CHEN, Y. H.; WALTER, T. *Observations of GNSS Spoofing in Russia in 2023-2024*. Stanford University, 2025. Disponível em: https://www.researchgate.net/publication/388984397_Observations_of_GNSS_Spoofing_in_Russia_in_2023-2024. Acesso em: 21 maio 2025.

NEW SCIENTIST. Ukraine will spoof GPS across the country to stop Russian drones. *New Scientist*, 2023. Disponível em: https://www.newscientist.com/article/2415318-ukraine-will-spoof-gps-across-the-country-to-stop-russian-drones/. Acesso em: 16 jun. 2025.

PSIAKI, M. L.; HUMPHREYS, T. E. Protecting GPS from spoofers is critical to the future of navigation. *IEEE Spectrum*, 2016. Disponível em: https://spectrum.ieee.org/gps-spoofing. Acesso em: 21 mar. 2025.

RUSSIAN FEDERAL SPACE AGENCY. *GLONASS Interface Control Document*. Rev. 5.1. Russian Federal Space Agency, 2019. Disponível em: https://glonass-iac.ru/en/documents/. Acesso em: 21 maio 2025.

U.S. GOVERNMENT. *GPS Accuracy*. U.S. Government. Disponível em: https://www.gps.gov/systems/gps/performance/. Acesso em: 20 mar. 2025.

WU, Z.; ZHANG, Y.; YANG, Y.; LIANG, C.; LIU, R. Spoofing and anti-spoofing technologies of global navigation satellite system: a survey. *IEEE Access*, v. 8, p. 165444-165496, 2020. https://doi.org/10.1109/ACCESS.2020.3022294