

Detecção de Drones Utilizando Rede Sensores de RF baseados em RDS

Cristiano Torres do Amaral¹, Edilson Vasconcelos Dantas Júnior², Olympio Coutinho³

¹Sistema de Proteção da Amazônia (Censipam), Porto Velho/RO – Brasil

² Departamento de Ciência e Tecnologia Aeroespacial (DCTA), São José dos Campos/SP - Brasil

³Instituto Tecnológico de Aeronáutica (ITA), São José dos Campos/SP – Brasil

Resumo – Este artigo apresenta uma proposta de sistema para detecção emissões de radiofrequência (RF) de *drones* baseada na utilização de Rádio Definido por Software (RDS) distribuído. Um experimento de demonstração de conceito é apresentado, onde o sinal de dois *drones* diferentes pode ser detectado e analisado. Também foi utilizada simulação computacional para predição de cobertura eletromagnética. Os resultados obtidos subsidiam estudos para estabelecer diretrizes e protocolos para desenvolvimento de uma plataforma de detecção da assinatura espectral de utilizando RDS. O texto apresenta a revisão da literatura sobre o tema, bem como requisitos técnicos para utilização de sensores baseados em rádio definido por software para varredura e detecção da assinatura espectral de RPA.

I. INTRODUÇÃO

O desenvolvimento tecnológico e a popularização dos dispositivos robóticos está promovendo uma revolução no mundo contemporâneo, estimulando maior competitividade e produtividade na sociedade. A robótica está presente em diferentes segmentos sociais e possui distintas aplicações civis e militares [1]. Atualmente, o seguimento de Aeronaves Remotamente Tripuladas (RPA - *Remotely Piloted Aircraft*), ou *drones*, é um dos mais promissores e que também tem fomentado grande preocupação para departamentos de inteligência e defesa de todo o mundo. O equipamento eletrônico que é utilizado como recreação por algumas pessoas, também pode ser utilizado por grupos terroristas ou criminosos [2].

Apesar da legislação e exigência de registros para operação dos RPAs no Brasil, ainda ocorrem incidentes que colocam em risco a segurança de instituições e pessoas. Em 2019, um RPA interrompeu as operações do aeroporto de Congonhas, em São Paulo/SP, por 20 minutos. Essa interrupção provocou o atraso de, pelo menos, 16 voos [3]. Em 2020, a concessionária Ecoponte, que opera a ponte Rio-Niterói, acionou a Polícia Rodoviária Federal e DECEA para impedir a ação de um homem que realizava filmagens em uma área de segurança da ponte [4].

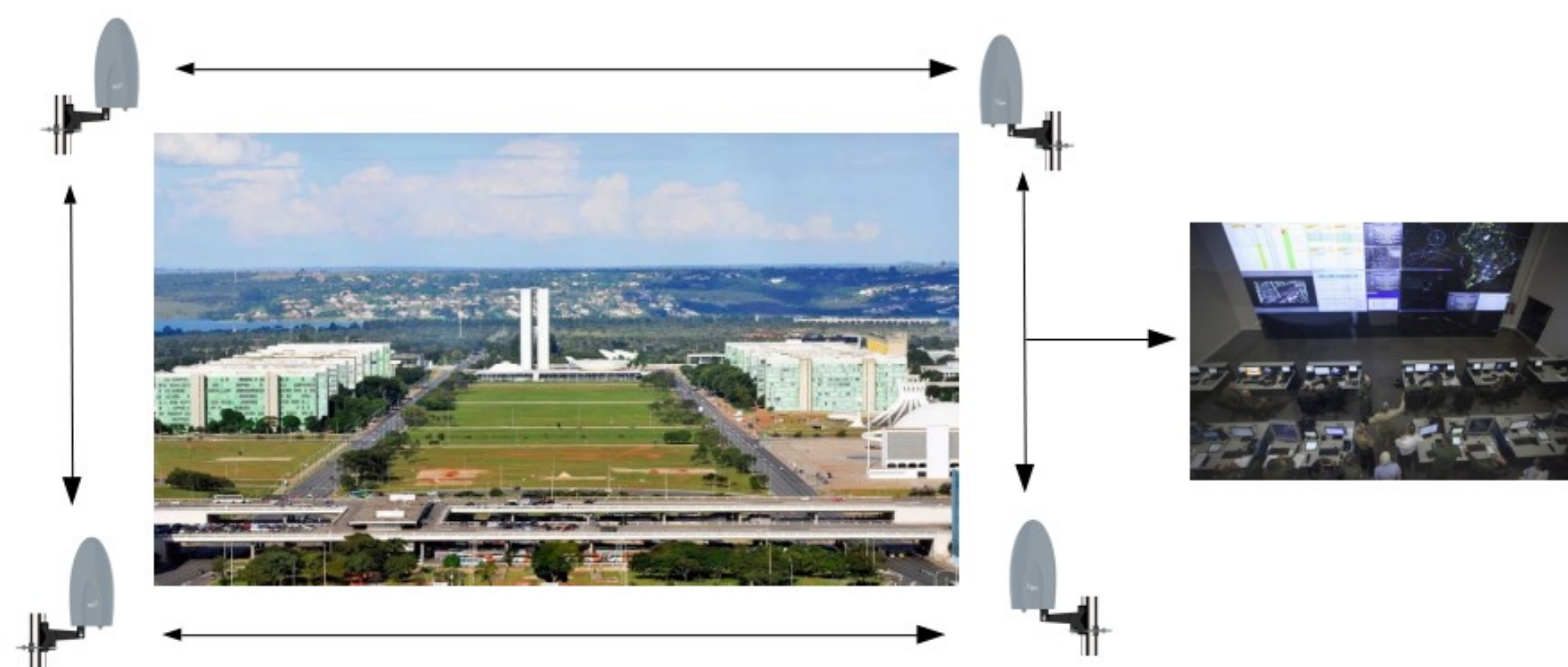


Fig. 1 - Proposta de monitoramento de perímetro

A utilização de RPA de recreação para fins ilegais não é uma exclusividade no Brasil. No mundo inteiro, agências de defesa e de inteligência estão se mobilizando para encontrar soluções para contrapor as ameaças de uso ilegal desses sistemas [5]. Entre as alternativas tecnológicas existentes, destaca-se o monitoramento do canal de comunicação entre o piloto remoto e a aeronave, identificando a ameaça pela análise da assinatura espectral da emissão eletromagnética. Nessa estratégia, são adotados recursos guerra eletrônica e defesa cibernética para localizar, identificar e eliminar o alvo. A implantação de estações de monitoramento e contramedida exigem investimentos elevados, pois são necessários equipamentos fixos e móveis dispostos em áreas de cobertura que possibilitem a triangulação para localização do RPA. Uma opção que se torna atrativa é o uso de Rádio Definido por Software (RDS) para aquisição e análise de sinais. Os RDS tiveram a sua origem na indústria de defesa, em um projeto norte-americano denominado *SpeakEasy*, em meados da década de 70. Atualmente, esses dispositivos versáteis e de baixo custo são utilizados para monitoramento de sinais radioelétricos com diferentes propósitos [6]. Este pôster apresenta a viabilidade de implantação de um sistema de monitoramento de RPA, utilizando estações de Rádio Definido por Software (RDS) [7] para varredura do espectro electromagnético. Essa rede de monitoramento com RDS pode ser utilizada para segurança em um perímetro sensível (Fig. 1).

II. PROPOSTA E DEMONSTRAÇÃO DE CONCEITO

O diagrama esquemático mostrado na Fig. 2 apresenta o experimento realizado em laboratório para demonstração de uma estação de monitoramento remoto. Para tanto, foi utilizado um analisador de espectro de baixo custo baseado em RDS (Aaronia) para varredura de RF e detecção de *drones*. Também foram realizadas simulações de predição da aeronave para delimitar o perímetro de cobertura da rede para detecção.

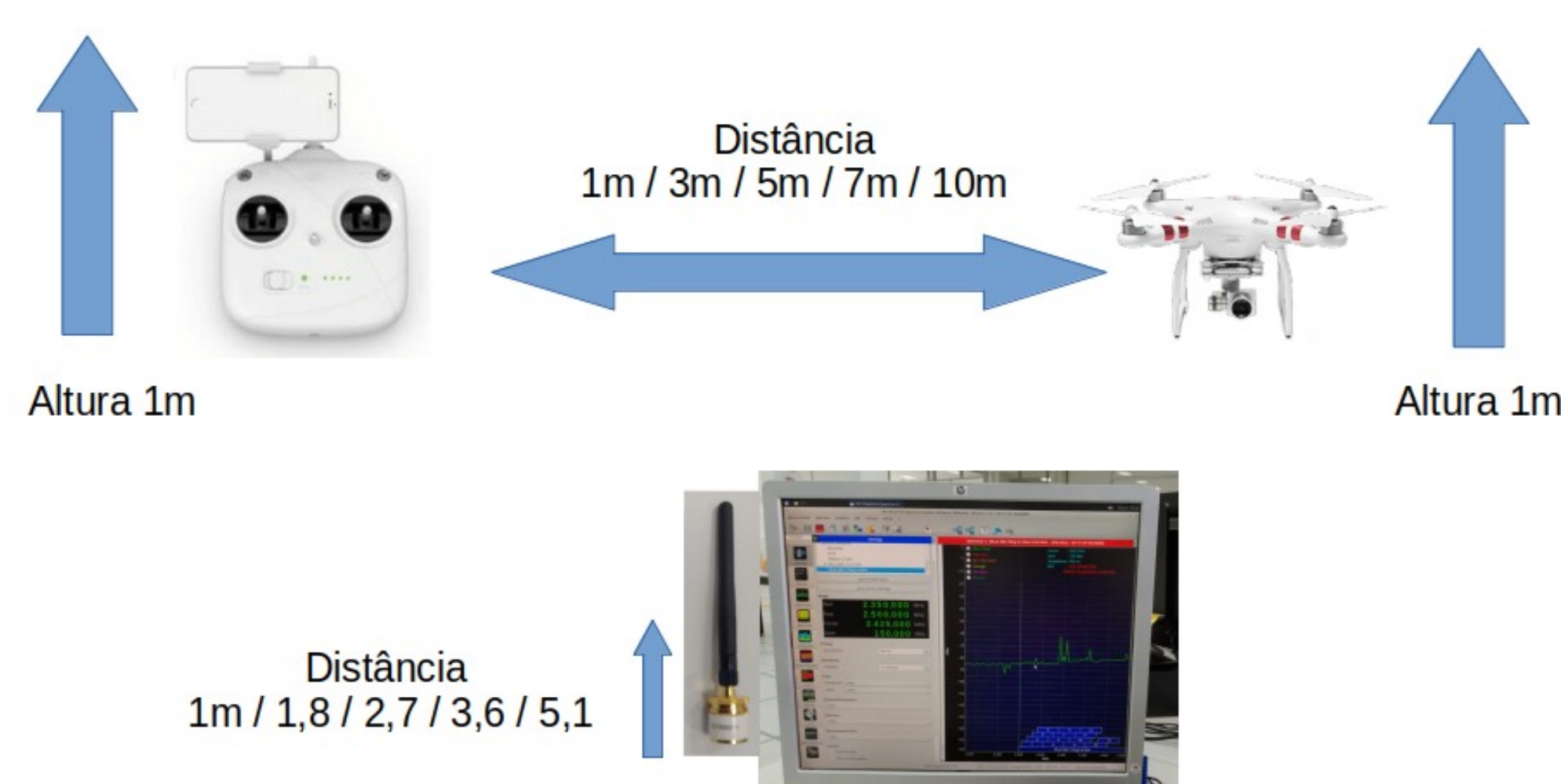


Fig. 2 - Experimento de demonstração de conceito

III. RESULTADOS E DISCUSSÃO

Distância RPA – Piloto (m)	Distância da Analisador (m)	Transmissão de Vídeo (dBm)	Sem Transmissão de Vídeo (dBm)
1,0	1	-47,72	-44,89
3,0	1,8	-47,64	-63,84
5	2,7	-56,83	-76,83
7	3,6	-58,84	-67,03
10	5,1	-56,81	-60,27

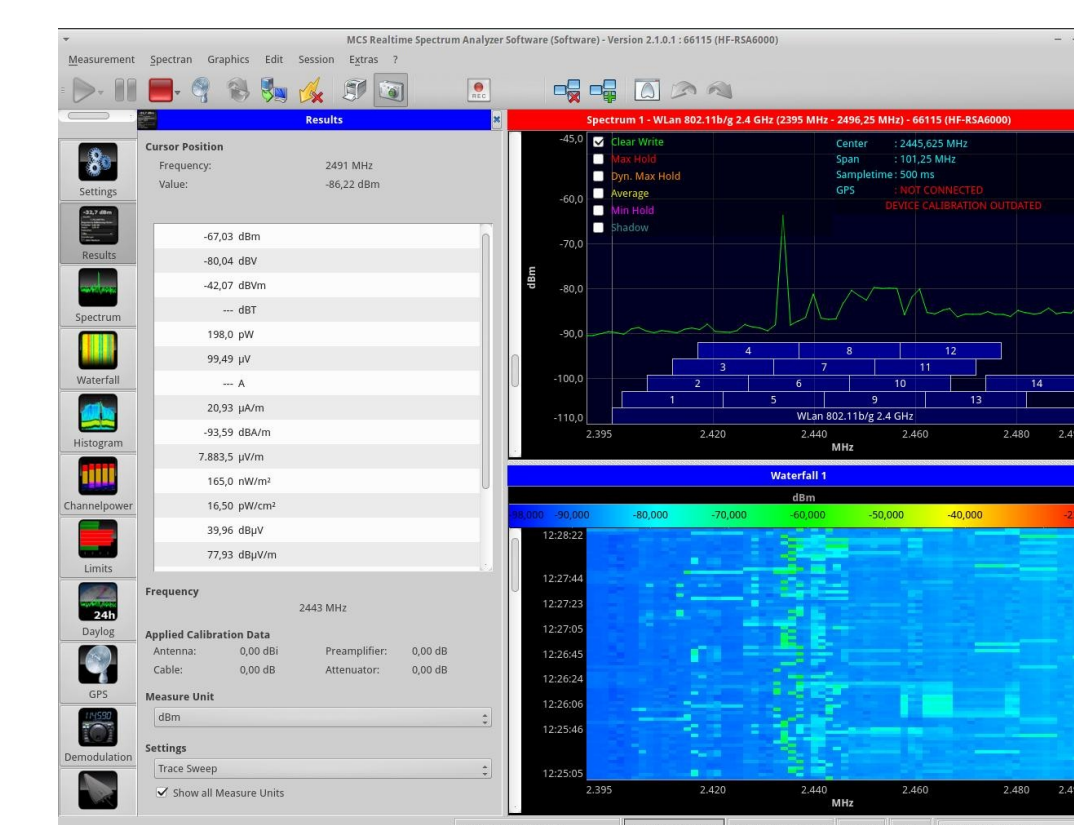


Fig. 3 - Intensidade de campo do RPA avaliado no experimento

O dispositivo RPA foi detectado na frequência de 2,474 GHz com níveis demonstrados no analisador de espectro (Fig. 3). Esta frequência faz parte do canal 6 do padrão IEEE 802.11g e apresentou maior intensidade de energia. Também foram realizadas simulações com a posição da console de pilotagem disposta na cobertura de um prédio de 10 metros e a aeronave em posição estática nas altitudes 50 e 100 metros (Fig. 4). Os resultados deste ensaio sugerem a área de cobertura do RPA e o perímetro de cobertura para instalação das antenas de monitoramento na cidade de Porto Velho/RO.

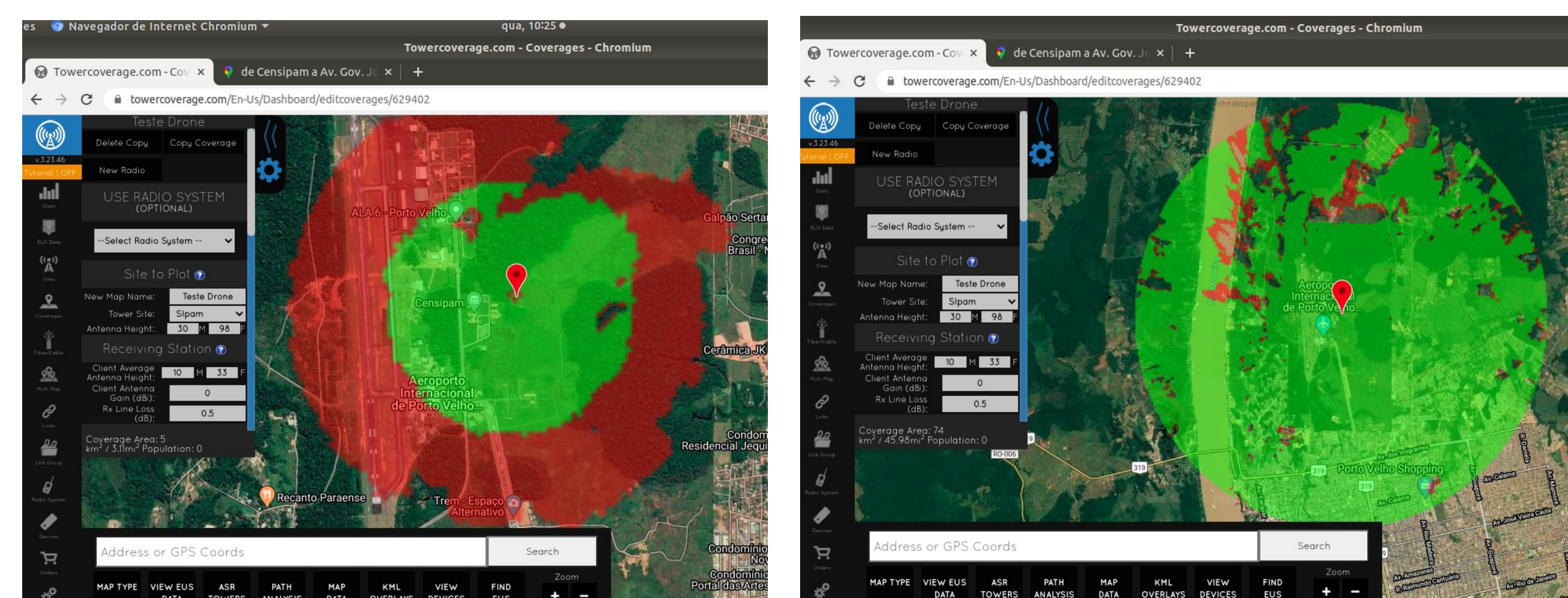


Fig. 4 - Cobertura do RPA 2.4GHz – Altitudes 50/100m

IV. CONCLUSÃO

Este pôster apresentou uma proposta de sistema de interceptação de emissões eletromagnéticas de sistemas *drones*, que é baseada no uso de RDS para detecção e análise dos sinais de rádio comunicação entre o RPA e a plataforma de rádio controle. Embora o equipamento de análise de sinais usado seja uma solução fechada, tecnologia de RDS atualmente disponível constitui uma solução aberta e baixo custo, que dá versatilidade ao desenvolvedor do sistema. Isso torna a proposta aqui apresentada viável e flexível. Por meio de uma revisão sobre legislação e classificações sobre sistemas RPAs, bem como uma sequência de ensaios em laboratório e em campo, foram apresentadas importantes considerações no sentido constituir um conjunto de diretrizes e protocolos a serem observados no momento se estabelecer a concepção de sistemas de interceptação e análise de sinais desta natureza.

REFERÊNCIAS

- [1] SHAKHATREH, H. et al "Unmanned Aerial Vehicles: A Survey on Civil Applications and Key Research Challenges". Disponível em: <https://arxiv.org/pdf/1805.00881.pdf> Acesso em: 01/06/2020.
- [2] CRS – Congressional Research Service "Department of defense counter-unmanned aircraft system" Disponível em: <https://news.usni.org/2020/02/14/report-on-pentagon-counter-drone-weapons> Acesso em: 01/06/2020.
- [3] GUEDES, P. "Um aparelho não tripulado perto de Congonhas fez aeroporto fechar por 20 minutos nesta terça". Disponível em: <https://bitly.com/RnJL8> Acesso em: 02/06/2020
- [4] DECEA Departamento de Controle do Espaço Aéreo - "Ação coordenada entre PRF e DECEA impede voo irregular na ponte Rio-Niterói" Disponível em: <https://www.decea.gov.br/?i=midia-e-informacao&p=pg_noticia&materia=acao-coordenada-entre-prf-e-decea-impede-voo-irregular-na-ponte-rio-niteroi> Acesso em: 02/06/2020.
- [5] DJI. "Manual do usuário Phantom 3 Advanced". Disponível em: <dl.djicdn.com/downloads/phantom_3/pt/Phantom_3_Advanced_User_Manual_pt.pdf> Acesso em: 02/06/2020.
- [6] AMARAL, C. T. et al "Guerra Eletrônica e Defesa Cibernética na Amazônia: Desenvolvimento de um Protótipo de Sistema de Interceptação de Comunicações para Indústria Nacional de Defesa" SIGE XXIII/ITA 2019. Disponível em: <https://bit.ly/2XQpXpB> Acesso em: 01/06/2020.
- [7] NGUYEN, Phuc et al. Matthan: Drone presence detection by identifying physical signatures in the drone's rf communication. In: Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services. 2017. p. 211-224.