Análise de ataques cibernéticos de *jamming* e *spoofing* em drones

Analysis of jamming and spoofing cyber-attacks on drones

Jeferson Nascimento Aquilar Pey; Georges Daniel Amvame Nze; Robson de Oliveira Albuquerque
Pós-graduação Profissional em Engenharia Elétrica – PPEE – Departamento de Engenharia Elétrica,
Faculdade de Tecnologia, Universidade de Brasília (UnB), Brasília, Brasil, Zip Code 70910-900
jeferson.pey@aluno.unb.br; georges@unb.br; robson@redes.unb.br

Resumo — **O uso de Aeronaves Remotamente Pilotadas (RPA), *Unmanned Aerial Vehicle (UAV), Unmanned Aircraft Systems* (UAS) ou mais conhecidos como "drones" tem aumentado nos últimos anos e isso se deve à sua versatilidade de uso (militar, construção civil, mineração, topografia, agropecuária, meio ambiente, entre outras). Esses veículos aéreos possuem uma variedade de tecnologias embarcadas que fazem com que sejam atrativas e de fácil uso. Entretanto, existem vulnerabilidades cibernéticas que podem ser exploradas para fins maliciosos (terrorismo, invasão de privacidade, tráfico de drogas e danos ao patrimônio). Este trabalho realiza uma breve análise sobre os ataques cibernéticos de *jamming* e *spoofing* em um sistema UAV e aponta alguns direcionamentos futuros de estudos sobre a segurança cibernética de drones.**

Palavras Chave – Drones; jamming, spoofing, ataques cibernéticos.

Abstract — **The use of Remotely Piloted Aircraft (RPA), Unmanned Aerial Vehicle (UAV), Unmanned Aircraft Systems (UAS) or better known as "drones" has increased in the last years and this is due to its versatility of use, be it for military purpose, civil construction, mining, topography, agriculture, environment, among others. These air vehicles have a range of embedded technologies, which make them attractive and easy to use. However, there are cyber vulnerabilities that can be exploited for malicious purposes (terrorism, invasion of privacy, drug trafficking and property damage). This work presents a brief analysis of jamming and spoofing cyber-attacks on UAV system and points out some directions for studies on drone cybersecurity.**

Keywords – Drones; jamming; spoofing; cyber attacks.

I. INTRODUÇÃO

O uso de aeronaves remotamente pilotadas (RPA), mais conhecidas como drones, tem se tornado cada vez mais frequente devido à sua facilidade de uso, além do grande número de possibilidades de emprego. Até o início do século XXI, apenas pilotos habilitados podiam sobrevoar o espaço aéreo, hoje em dia, qualquer pessoa pode utilizar drones num espaço aéreo desregulado [1].

O mercado mundial de drones crescerá a uma média anual de 13% entre 2020 e 2025, quando atingirá aproximadamente U$ 43 bilhões em valores de comercialização [2]. A estimativa para 2025 é que haja cerca de 17,89 milhões de drones na Ásia; 11,82 milhões na América do Norte; 9,86 milhões na Europa; 1,11 milhões na América do Sul; 1,09 milhões na Oceania e 1,08 milhões na África [3]. Atualmente, os maiores mercados consumidores são: Estados Unidos, China, Japão, Alemanha, Reino Unido, França, Austrália, Canadá, Itália e Índia [2].

O uso dessa tecnologia tem se expandido para áreas cada vez mais amplas: militar, turismo, agricultura, busca e salvamento, georeferenciamento, mineração, construção civil, segurança pública, *hobby*, imagens e fotos para entretenimento, dentre outros. À medida que a utilização de drones provê maiores facilidades para o dia a dia das pessoas, os problemas de segurança cibernética são gradualmente expostos.

O objetivo deste estudo é realizar breve análise de alguns tipos de ataques cibernéticos - *jamming* e *spoofing* - na utilização de drones comerciais de asa rotativa. O assunto é relevante porque a proliferação de UAV traz uma série de preocupações relativas à segurança da sociedade e do Estado, seja por causa dos riscos à aviação, seja por causa do uso malicioso: terrorismo, invasão de privacidade ou tráfico de drogas e armas. É necessário discutir os ataques cibernéticos de drones a fim de aprimorar a gestão de riscos.

O artigo está organizado da seguinte forma: a Seção II apresenta alguns trabalhos relacionados. A Seção III apresenta e faz uma breve análise de ataques cibernéticos de *jamming* e *spoofing*. Finalmente, na Seção IV, o futuro da segurança cibernética em UAV é discutido.

II. TRABALHOS RELACIONADOS

Um sistema de aeronave não tripulada (*Unmanned Aircraft Systems* - UAS) é composto por três elementos principais: aeronave não tripulada, estação de controle de solo (*Ground Control Station* - GCS) e a interface de link de dados [4]. Uma vez estabelecida a arquitetura do sistema de drones, conforme descrito na Figura 1, é possível a realização de ataques cibernéticos contra os UAV.

Os *Surveys* de Altawy e Youssef [1] e Yaacoub *et al.* [5] tratam com amplitude e profundidade assuntos relacionados aos

2022 17th Iberian Conference on Information Systems and Technologies (CISTI)
22 – 25 June 2022, Madrid, Spain
ISBN: 978-989-33-3436-2

drones, abordando vários aspectos importantes, tais como: marcos regulatórios de cada país, diferentes possibilidades de comunicações entre drones, classificação dos drones, domínios de uso de UAV, tipos de ataques contra drones, tipos de sistemas anti drones e técnicas de detecção de UAV.

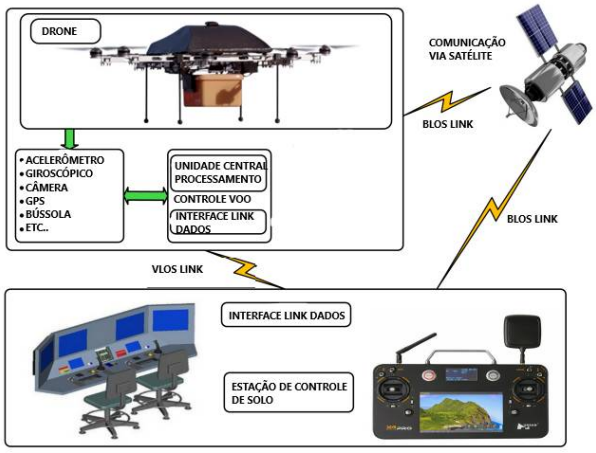

Figura 1. Arquitetura de sistema de drones – adaptado de [1]

O artigo de Likou *et al.* [6], sobre o emprego de sistemas anti-drones próximos à aeroportos, concluiu que existe a tendência de aumento de ataques a essas infraestruturas com a utilização de drones e que planos de gestão de riscos e de contingência devem ser elaborados pelas autoridades para enfrentar essas ameaças.

Os Estudos de Wesson e Humphreys [7] e Kerns *et al*. [8] relatam que uma das principais vulnerabilidades cibernéticas no emprego de drones civis encontra-se no enlace de dados porque a comunicação, tanto do sistema de navegação via satélite, quanto por meio de rádio frequência, *Wi-Fi* ou *bluetooth* ocorre geralmente de forma não protegida por criptografia, uma vez que o uso de recursos criptográficos diminui a performance na transmissão de dados, dentre outras considerações de segurança.

Quanto as ameaças cibernéticas em relação aos sensores, a maioria dos trabalhos enfoca na segurança de transmissão de dados, mas geralmente ignora a análise de segurança dos sensores em si, que dependem de um contato físico com o dispositivo. Além disso, devido a restrições técnicas ou de custos, sensores comerciais em UAV normalmente não conseguem distinguir entre dados normais e anormais [9]. Essa vulnerabilidade facilita o uso de *spoofing* contra os sensores, especialmente os de sistema de navegação.

O motivo do amplo emprego do Sistema Global de Navegação por Satélite (GNSS), seja o GPS ou GLONASS, nos drones é devido à simplicidade de uso e baixo custo da tecnologia, assim como a boa acurácia na transmissão das coordenadas [10]. A errônea coleta de dados por esses sensores compromete a segurança do voo, podendo causar grave acidente ou queda, porém, antes de ser realizado o ataque de *spoofing* contra o sinal de GNSS é necessário que o drone seja detectado.

Trabalho realizado por Ezuma *et al.* [11] identificou e classificou 15 tipos de UAV por meio de características de rádio frequência (RF *fingerprints*) emitidas pelos controles dos drones, mesmo com a interferência de sinal de *bluetooth e Wi-Fi*, usando sistema de vigilância passiva de RF.

Segundo Park *et al*. [12], os métodos de detecção de drones ainda estão em estágio inicial. Isso explica por que a maioria dos sistemas anti-drones realiza neutralização e/ou interdição. De acordo com Michel [13], cerca de 80,96 % dos sistemas anti-drones (*Counter Unmanned Aircraft Systems C-UAS*) utilizam as técnicas de *spoofing* e/ou *jamming* para realizar a neutralização e/ou interdição de um sistema de drones (de 352 produtos C-UAS relatados, 285 utilizam as referidas técnicas).

Dado que existe predominância na utilização das técnicas de *jamming/spoofing* para realizar ataques sobre drones, a proposta desta pesquisa é analizá-las a fim de contribuir com o debate sobre a viabilidade do uso dessas técnicas. Além disso, sugere-se novos direcionamentos de pesquisas a partir da utilização dos sinais da quinta geração de rede de comunicação móvel (5G).

III. ANÁLISE DOS ATAQUES CIBERNÉTICOS EM DRONES

Os ataques cibernéticos afetam um ou mais dos princípios de segurança da informação: disponibilidade, integridade, confidencialidade e, em alguns casos, inclui-se a autenticidade. Todos esses princípios são vulneráveis a determinados tipos de ataques e a gestão de riscos atua com a intenção de diminuir a probabilidade de ocorrência de danos ou prejuízos decorrentes destes ataques.

A. Drone Jamming

Qualquer tipo de decodificação de comunicação digital está fortemente relacionado à relação sinal-ruído (*Signal-Noise Ratio*-SNR) no receptor. A SNR define o quão intenso é o sinal em relação ao ruído, sempre presente nos dispositivos de telecomunicações. Em uma comunicação digital, conforme aumenta a distância entre o transmissor e o receptor, a potência do sinal recebida diminui, devido a atenuações do meio de propagação [14].

O *jamming* é uma maneira de bloquear a comunicação sem fio entre o transmissor e receptor por meio da adição de um sinal interferente até o momento em que a sensibilidade do receptor não seja suficiente para identificar os sinais, perdendo assim o enlace de comunicação [14].

Este tipo de ataque afeta diretamente o princípio da disponibilidade, uma vez que não permite a utilização do sistema por usuários autorizados. Como exemplo, um ataque de GPS *Jamming* foi executado no drone *S-100 Camcopter*, resultando em uma colisão com o controle terrestre que feriu dois pilotos remotos e matou um engenheiro durante os testes [15].

Diferentes técnicas de *jamming* podem ser usadas para interromper a comunicação entre o controlador e o drone, sendo que as mais comuns são utilizando antenas omnidirecionais ou direcionais [16]. As primeiras emitem sinal interferidor em todas as direções (360º graus) e não necessitam de localizar o drone, mas tem a desvantagem de possuir menor poder interferidor.

Em um exemplo de uso de antenas direcionais foi empregado o radar de ondas contínuas modulada por frequência 3D - *Frequency Modulated Continuous Wave* (FMCW) com múltiplas entradas e mútiplas saídas - *Multiple Input Multiple*

Output (MIMO) e a utilização de antena direcional de *jammer* na faixa de 2.4 GHz [17]. O radar escaneia constantemente determinada área até que o alvo entre no seu raio de atuação. O algoritmo de detecção avalia o movimento do alvo e, se ele for identificado como ameaça, a antena direcional emite o sinal interferidor sobre o alvo, tornando impossível o controle do drone.

Segundo Park *et al.* [12], *jamming* apresenta como vantagens a simplicidade e o emprego imediato, além de poder ser usado contra protocolos de comunicação desconhecidos, desde que estejam utilizando a faixa de frequência atacada. Por outro lado, apresenta como desvantagens: interferência em outros dispositivos e não é efetivo contra voos autônomos.

Em termos legais, o uso de *jamming* é controverso. Por exemplo, no Brasil, o uso de *jammers* é permitido somente em unidades prisionais. Já nos EUA, os bloqueadores de sinal são proibidos em todo o território estadunidense. O motivo da proibição do *jamming* é que tal técnica inutiliza toda a faixa do espectro com a adição do sinal interferente, impossibilitando que outros sistemas de comunicação permaneçam operantes na frequência considerada.

Em termos técnicos, o uso de *jamming* é simples de ser executado, sobretudo se forem utilizadas antenas omnidirecionais, que não dependem de algoritmo para localização e identificação do drone. Neste estudo, considera-se apenas o uso de *jamming* em drones comerciais com faixas de frequência de 2.4 GHz ou 5 GHz, entretanto podem ser desenvolvidas aeronaves que operem em outras bandas de frequência ou em outros protocolos de comunicação e que escapam ao objetivo deste trabalho.

Atualmente, a maioria dos países tem restrições legais rígidas quanto ao uso de *jammers* por usuários civis [12], portanto os novos sistemas anti drones não militares devem ser desenvolvidos considerando a limitação/proibição de bloqueadores. No Brasil, por exemplo, está em debate a possibilidade de ampliar o uso de *jamming* para proteção de outras instalações estratégicas, além das unidades prisionais.

B. *Drone Spoofing*

Para a realização do *GCS-Drone spoofing* é necessário que seja empregado um *sniffer* de RF capaz de identificar e descobrir os parâmetros de configuração do tipo de drone objeto do ataque, conforme demonstrado por Ezuma *et al.* [11]. O termo já é empregado na área de redes de computadores, quando um elemento externo tenta se infiltrar na rede copiando as credenciais de um computador já pertencente à estrutura. A aplicação de *spoofing* para sinais de RF depende do uso de um dispositivo que se passa pelo controle do drone, possibilitando assim, tomar o seu controle de voo.

A técnica de *spoofing* em drones tem como vantagens*:* largo espectro de emprego e possibilidade de uso em voos autônomos, uma vez que pode confundir o sistema de navegação GPS da aeronave [12].

No experimento, conduzido por Donatti [14] e ilustrado na Figura 2, foi utilizado um sistema de intervenção de voo que contorna as barreiras técnicas inerentes ao projeto e permite tomar o controle de drones guiados por rádio frequência, mesmo na presença do controle real, de forma eficiente porque emite sinais de *clock* quase 5 vezes mais rápido do que o sinal do controlador original (tempo de chaveamento original 3.857ms, ao passo que o chaveamento com o sistema *spoofing* era de apenas 0.8024ms).

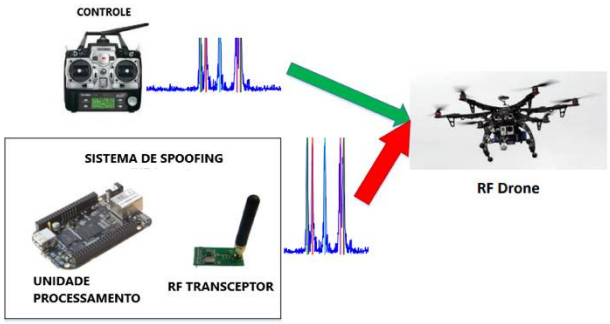

Figura 2 – Sistema de *GCS-Drone* Spoofing – adaptado de [14]

Para ocorrer um ataque de GPS *spoofing,* um transmissor é utilizado para enviar sinais falsos de GPS para o controlador de voo do drone, forçando o UAV a sincronizar com os sinais do atacante [18]. Em recente estudo sobre identificação de ataque cibernético de GPS *spoofing* [10] foi proposta metodologia para detecção de ataque por meio da análise de mudança de parâmetros internos da UAV.

Segundo Park *et al*. [12], o uso de *spoofing* apresenta as seguintes vantagens: ampla disponibilidade de uso e possibilidade de emprego também em voos autônomos por meio do *spoofing* de GNSS. Em outra mão, existe a dificuldade de controle e execução da técnica, além da possibilidade de anulação da ação de *spoofing* com o controle manual da UAV.

Em termos regulatórios esta técnica não se enquadra na especificação de bloqueador de sinal, o que facilita o seu emprego sob o ponto de vista legal. Além disso, o *spoofing* tem duas vantagens técnicas principais sobre o *jamming* [14]: primeiro porque permite que a faixa de frequência seja operada por outros aparelhos e usuários, e segundo porque possibilita o controle da aeronave e, consequentemente, a captura dos objetos e das mensagens transportadas.

C. *Observações considerando tecnologia 5G*

A velocidade de conexão 5G é cerca de 16 vezes mais rápida do que a Rádio Frequência (de 600 Mbit/s no padrão Rádio Frequência de 2.4GHz para 10.000 Mbit/s no padrão 5G) [19]. Isso permite o desenvolvimento da *Internet of Drones* (IoD) [20], estrutura concebida para possibilitar avanços como o controle do tráfego aéreo de baixa altitude (*UAS Traffic Management*-UTM) ou *Urban Space* (U-Space). Esse espaço compreende altitude de voo abaixo de 400 pés (ft) ou 121.92 metros, normalmente utilizado como parâmetro para limitação de drones comerciais civis [21].

Outro avanço do 5G foi a possibilidade de coordenação de voos de frotas de drones ou Veículos Conectados e Autônomos (CAVs), onde altas taxas de transmissão de dados, baixa latência e cobertura onipresente permitem que os veículos troquem dados vitais com o centro de controle e com veículos vizinhos [22].

A conectividade do uso do 5G entre as aeronaves, as entidades de transporte e as de infraestrutura permite Sistemas de Transporte Inteligentes (ITS) que, por sua vez, fornecem uma gama de aplicações, incluindo o gerenciamento de tráfego do U-Space [22].

IV. CONCLUSÕES E TRABALHOS FUTUROS

Com o aumento acentuado na utilização dos drones e com a expansão de dispositivos de comunicação sem fio através dos conceitos de *Internet of Drones* (IoD), a segurança e a robustez dos protocolos, modulações e técnicas de comunicação devem ser estudadas e aprimoradas.

Estudos futuros devem considerar que os ganhos de conectividade da tecnologia 5G trouxeram novas perspectivas para o uso coletivo (enxame ou frota) de drones e para o controle do espaço aéreo de baixa altitude. Com o aumento do uso intensivo de dados e dos aplicativos em tempo real, a privacidade dos dados e os requisitos de segurança também devem ser reforçados a fim de proporcionar um confiável grau de proteção contra ataques de *jamming* e *spoofing*.

Resultados preliminares desta pesquisa apontam que o desenvolvimento de sistemas anti-drones deve considerar que o uso da técnica de *jamming* tende a ser cada vez mais restrito, portanto, devem ser aprimoradas as técnicas de detecção para que os drones sejam neutralizados de forma pontual. O uso de técnicas combinadas de detecção de UAV é um ramo a ser desenvolvido a fim de aumentar a possibilidade de sucesso dos sistemas anti-drones.

Quanto ao *spoofing*, seja de Rádio Frequência ou de GNSS, conclui-se parcialmente que as vulnerabilidades cibernéticas dos drones comerciais civis ainda estão longe de serem sanadas e esta técnica tende a ser cada vez mais utilizada. Finalmente, trabalhos futuros de segurança cibernética em UAV devem aprofundar novas formas de detecção de ataques de *spoofing* em drones.

V. AGRADECIMENTOS

Os autores agradecem o suporte da ABIN TED 08/2019. R.d.O.A. gratefully acknowledges the General Attorney of the Union - AGU grant 697.935/2019; the General Attorney's Office for the National Treasure - PGFN grant 23106.148934/2019-67; the support from EC Horizon 2020 HEROES project grant 101021801.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] Altawy, R.; Youssef, A. M. "Security, privacy, and safety aspects of civilian drones: A survey". ACM Transactions on Cyber-Physical Systems, v. 1, n. 2, 2017.

[2] Schroth, L.; Bodecker, H.; Radovic, M. "Drone Market Report 2020-2025". Drone Industry Insight, 2020. Disponível em https://droneii.com/wp-content/uploads/2020/06/Drone-Market-Report-2020-2025-Sample.pdf. Acesso em 04 de fevereiro de 2022.

[3] Schroth, L. "Drone Market Size and Forecast 2020-2025". Drone Industry Insight, 2020. Disponível em https://droneii.com/project/drone-market-size-2020-2025. Acesso em 08 de fevereiro de 2022.

[4] Marshall D. M., Barnhart R.K., Shappee E., and Most M.T. "Introduction to Unmanned Aircraft Systems". CRC Press, 2015.

[5] Yaacoub, J.-P., Noura H., Salman O. and Chehab A. "Security analysis of drones systems: Attacks, limitations, and recommendations". Internet of Things, v. 11, 2020.

[6] Lykou, G.; Moustakas, D.; Gritzalis, D. "Defending airports from UAS: A survey on cyber- attacks and counter-drone sensing technologies". Sensors, v. 20, n. 12, p. 1–35, 2020.

[7] Wesson k. and Humphreys T. "Hacking drones". Scientific American 309, 5, 54–59, 2013.

[8] Kerns A. J., Shepard D. P., Bhatti J. A., and Humphreys T. E. "Unmanned aircraft capture and control via GPS spoofing". Journal of Field Robotics 31, 617–636, 2014.

[9] He, D. J., Du, X., Qiao, Y. R., Zhu, Y. K., Fan, Q., & Luo, W. "A Survey on Cyber Security of Unmanned Aerial Vehicles". Jisuanji Xuebao/Chinese Journal of Computers. Science Press. 2019. https://doi.org/10.11897/SP.J.1016.2019.01076

[10] Basan, E., Basan, A., Nekrasov, A., Fidge, C., Gamec, J., Gamcová, M. . "A self-diagnosis method for detecting uav cyber attacks based on analysis of parameter changes". Sensors, v. 21, n. 2, p. 1–17, 2021.

[11] Ezuma, M., Erden, F., Anjinappa C. K., Ozdemir O., and Guvenc I. "Detection and Classification of UAVs Using RF Fingerprints in the Presence of Wi-Fi and Bluetooth Interference". IEEE Open Journal of the Communications Society, v. 1, p. 60–76, 2019.

[12] S. Park, H. T. Kim, S. Lee, H. Joo and H. Kim, "Survey on Anti-Drone Systems: Components, Designs, and Challenges". *IEEE Access*, vol. 9, pp. 42635-42659, 2021, doi: 10.1109/ACCESS.2021.3065926.

[13] Michel, A. H. "Counter-Drone Systems". 2nd Edition. Bard College. v. 19, 2019.

[14] Donatti, M. M. "Sistema de spoofing para intervenção de voo em aeronaves não tripuladas guiadas por radiofrequência através de modulação multicanal". Dissertação de mestrado. UNICAMP. 2017.

[15] Krishna, C. G. L. and Murphy, R. R. "A review on cybersecurity vulnerabilities for Unmanned Aerial Vehicles". IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR), pages 194–199, 2017.

[16] Tedeschi, P., Oligeri, G., and Di Pietro, R. "Leveraging jamming to help drones complete their mission". IEEE Access, 8, 5049-5064, 2019.

[17] T. Multerer et al., "Low-cost jamming system against small drones using a 3D MIMO radar based tracking," European Radar Conference (EURAD), pp. 299-302, 2017. doi: 10.23919/EURAD.2017.8249206.

[18] Vattapparamban, E., Guvenc, I., Yurekli, A.I., Akkaya, K., and Uluagaç, S. "Drones for smart cities: Issues in cybersecurity, privacy, and public safety". International Wireless Communications and Mobile Computing Conference (IWCMC), pages 216–221, 2016. doi: 10.1109/IWCMC.2016.7577060

[19] Schroth, L. "Evolution of drone control connectivity and the role of 5G". Drone Industry Insight. Disponível em https://droneii.com/project/evolution-of-drone-control-connectivity. Acesso em 26 de dezembro de 2021.

[20] Abdelmaboud A. "The Internet of Drones: Requirements, Taxonomy, Recent Advances, and Challenges of Research Trends". *Sensors*. 21(17):5718., 2021. doi.org/10.3390/s21175718

[21] Shrestha R., Oh I., and Kim S. "A Survey on Operation Concept, Advancements, and Challenging Issues of Urban Air Traffic Management". *Front. Future Transp.* 2:626935. 2021. https://doi: 10.3389/ffutr.2021.626935

[22] Ansari, S., Taha, A., Dashtipour, K., Sambo, Y., Abbasi, Q. H., & Imran, M. A. "Urban Air Mobility—A 6G Use Case?" Frontiers in Communications and Networks, 2,2021. doi.org/10.3389/frcmn.2021.729767