XIII Seminário de Extensão e Inovação
XXVIII Seminário de Iniciação Científica e Tecnológica da UTFPR
Ciência e Tecnologia na era da Inteligência Artificial: Desdobramentos no Ensino Pesquisa e Extensão
20 a 23 de novembro de 2023 - *Campus Ponta Grossa, PR*
SEI-SICITE 2023

Análise de ataques práticos para a comunicação de Veículos Aéreos Não Tripulados

Analysis of practical attacks for unmanned aerial vehicle communication

Giovanni Henrique Munhoz de Lion Siervo[1], Natássya Barlate Floro da Silva[2]

RESUMO

Atualmente é comum o uso de Veículos Aéreos Não Tripulados, também conhecidos como drones, em diversas áreas, principalmente na agricultura para o monitoramento de lavouras e plantações devido à sua versatilidade e capacidade de reconhecimento. Tais dispositivos são conectados a uma rede para serem controlados remotamente, com isso são suscetíveis a ataques cibernéticos. Logo, o objetivo deste trabalho é analisar ataques à comunicação entre drone e estação de controle em uma rede sem mecanismos de segurança. Será realizada uma tentativa de alterar o trajeto do veículo durante a execução de uma missão por meio do envio de mensagens com o protocolo Mavlink utilizado nessa comunicação. Para o ataque, foi implementado um código que se conecta ao piloto automático e interfere na sua conexão com o controlador. Por meio de uma simulação, foram comparados os dados de latitude, longitude e altitude em relação ao solo da aeronave em uma missão sem interferência e depois com a execução do ataque. Foi possível observar uma diferença na trajetória percorrida já que a rede de comunicação não possui certificação de segurança contra ataques.
PALAVRAS-CHAVE: Ataques; Comunicação; Veículos Aéreos Não Tripulados.

ABSTRACT

Currently, unmanned aerial vehicles, also known as drones, is common in various fields, particularly in agriculture, for monitoring crops and plantations due to their versatility and reconnaissance capabilities. These devices are connected to a network for remote control, making them susceptible to cyberattacks. Therefore, this work aims to analyze attacks on the communication between the drone and the control station in a network without security mechanisms. An attempt will be made to alter the vehicle's trajectory during the execution of a mission by sending messages with the Mavlink protocol used in this communication. A code was implemented for the attack that connects to the autopilot and interferes with its connection to the controller. Through a simulation, the aircraft data of latitude, longitude, and altitude relative to the ground were compared in a mission without interference and then with the execution of the attack. It was possible to observe a difference in the trajectory traveled, as the communication network lacks security certification against attacks.
KEYWORDS: Attack; Communication; unmanned aerial vehicles.

INTRODUÇÃO

Com o avanço da tecnologia, vem se tornando gradativo o uso de drones ou VANTs (Veículos Aéreos Não Tripulados). Trata-se de aeronaves controladas remotamente que são utilizadas em uma variedade de setores, principalmente na agricultura para monitoramento de lavouras e plantações,

[1] Voluntário. Universidade Tecnológica Federal do Paraná, Cornélio Procópio, Paraná, Brasil. E-mail: gsiervo@alunos.utfpr.edu.br. ID Lattes: http://lattes.cnpq.br/1672473573952010.
[2] Docente do Departamento Acadêmico de Computação. Universidade Tecnológica Federal do Paraná, Cornélio Procópio, Paraná, Brasil. E-mail: natassyasilva@utfpr.edu.br. ID Lattes: http://lattes.cnpq.br/3393376801047734.

pois são caracterizadas pela capacidade de reconhecimento e de voo em locais de difícil acesso (SHAKHATREH et al., 2019).

Dentre as especificidades dessas aplicações, destaca-se a segurança desses veículos. Seus componentes físicos incluem sensores e atuadores que se comunicam com o sistema de controle em solo por meio de uma conexão sem fio. Além disso, uma vez que os VANTs não possuem pilotos a bordo, são controlados por meio de uma GCS (*Ground Control Station*, estação de controle terrestre em português), podendo ser um computador ou celular que são conectados via rede. Esse tipo de interface apresenta vulnerabilidades, tornando o sistema suscetível a ataques que afetam os elementos cibernéticos ou físicos, a interface de controle, a conexão sem fio ou uma combinação desses componentes (CONSTANTINIDES; PARKINSON, 2008).

Um exemplo de ataque ocorreu em 2011 quando um drone militar estadunidense foi capturado por unidades iranianas. Primeiramente, todos os *links* de comunicação da aeronave com a base de operação foram bloqueados, com isso o piloto automático foi ativado. Com o veículo neste estado, o atacante falsificou o sistema de GPS (*Global Positioning System*, sistema de posicionamento global em português) enviando coordenadas falsas, o que fez o drone pousar em uma base iraniana supondo que estava pousando em uma base norte-americana. Esse tipo de ataque foi também replicado por pesquisadores em um ambiente controlado, demonstrando a fragilidade desse tipo de veículo (SHEPARD; BHATTI; HUMPHREYS, 2012).

Este trabalho tem como objetivo avaliar ataques à comunicação entre o piloto automático ArduCopter e sua GCS MavProxy, ambos do projeto de código aberto ArduPilot . Nesse ataque, será realizada a tentativa de alterar o trajeto da aeronave por meio do envio de mensagens com o protocolo Mavlink usado na comunicação desses sistemas. Para possibilitar o ataque, foi implementado um *script* que se conecta ao piloto automático para interferir em sua comunicação com o controlador.

MATERIAIS E MÉTODOS

As ferramentas utilizadas neste trabalho são apresentadas no Quadro 1. As ferramentas ArduCopter, MavProxy e Pymavlink são parte do projeto do ArduPilot, que é um sistema de código aberto criado para o desenvolvimento de pilotos automáticos para diversos veículos (ARDUPILOT DEV TEAM, 2023).

Quadro 1 – Ferramentas utilizadas para a reprodução do ataque em ambiente de simulação.

Nome	Descrição
ArduCopter 4.5.0	Software do piloto automático para multirrotores utilizado no veículo
MavProxy 1.8.66	Software da GCS usado em computadores
MAVLink 2	Protocolo de comunicação entre GCS e veículo
Python 3	Linguagem de programação utilizada nos *scripts*
Pymavlink 2.4.40	Biblioteca de integração da linguagem com o protocolo
Wireshark 4.0.8	Programa *sniffer* de captura de pacotes enviados na rede

Fonte: Elaborado pelos autores (2023).

Para analisar um ataque prático na comunicação entre VANT e GCS, foi desenvolvido um *script* com a linguagem Python, utilizando a biblioteca *Pymavlink*. O código irá estabelecer uma conexão UDP com o veículo, depois enviará um comando para a aeronave sobrevoar até determinada

coordenada, totalmente diferente do *waypoint* fixado pela estação de controle. Em seguida, o *script* irá receber e exibir a mensagem de confirmação se o comando foi aceito ou não. Espera-se algum tipo de interferência na comunicação destes dispositivos e alteração na rota do veículo.

Para a execução do ataque, foi utilizada a técnica de *Software-in-the-Loop* (SITL), que consiste em gerar um ambiente de simulação virtual para a execução do piloto automático e da movimentação da aeronave. Esse ambiente foi disponibilizado pelo ArduPilot, que permitiu a simulação de um *quadrotor* sem o uso de hardware específico para o piloto automático, utilizando o mesmo computador em que estava instalado o ambiente do ArduPilot com o software MavProxy como GCS.

O experimento consistiu em rodar a simulação, com a configuração tradicional de uma missão com a definição dos *waypoints*, pontos a serem seguidos para a trajetória da aeronave, e com o envio de comandos de navegação ao veículo normalmente através da estação de controle. Primeiramente foi realizada a simulação sem o ataque. Posteriormente, a simulação era reiniciada e os mesmos comandos eram dados, mas desta vez o *script* responsável pelo ataque era também executado paralelamente durante a missão para observar se ocorria alguma interferência na trajetória do veículo, simulando um ataque na comunicação.

As variáveis utilizados para a comparação dos resultados obtidos foram a latitude, longitude e altitude relativa ao solo do *quadrotor* em relação ao tempo de inicialização dos sistemas. Para a captura dos dados de localização da aeronave, um código foi rodado em segundo plano durante as duas situações. Ele estabelece uma conexão UDP com o veículo, em seguida recebe e imprime mensagens enviadas referentes ao seu GPS. Para fins práticos, as saídas de dados foram salvas em um arquivo de texto e depois tratadas para elaboração dos gráficos. Também foi utilizado o programa Wireshark para capturar as mensagens trocadas na rede entre VANT e GCS.

RESULTADOS E DISCUSSÃO

A simulação define o ponto de partida do VANT nas coordenadas de latitude -35,3632621 e longitude 149,1652374, como a captura dos dados se iniciou antes da decolagem, a altitude inicial foi de 0 m em relação ao solo.

Partindo da GCS, o primeiro comando dado ao veículo foi para armar os motores. Com os motores funcionando, foi ordenada uma decolagem para 40 m de altitude. Em seguida, foi comandado para o *quadrotor* voar até as coordenadas de latitude -35,3621259, longitude 149,1664594 e altitude 100 m. A Figura 1 mostra no mapa a trajetória a ser seguida pela aeronave após o comando.

Após a execução da missão, a simulação foi reiniciada. Com o veículo na mesma posição inicial, foram enviados os mesmos comandos, porém, durante a execução do comando de navegação para o mesmo ponto determinado na simulação anterior, o *script* foi iniciado paralelamente e enviou um comando para o drone sobrevoar até a coordenada de latitude -35,36384566 e longitude 149,16480758. A Figura 2 mostra no mapa a trajetória a ser seguida pela aeronave após a execução do *script*.

A Figura 3 apresenta os valores da latitude em relação ao tempo de inicialização para o experimento em condições normais da missão, com a aeronave seguindo para a coordenada de latitude -35,3621259, e para o experimento em que o *script* responsável pelo ataque é executado

Figura 1 – Trajetória do *quadrotor* durante execução do comando.

Fonte: Elaborado por autores (2023).

Figura 2 – Trajetória do *quadrotor* após execução do *script*.

Fonte: Elaborado por autores (2023).

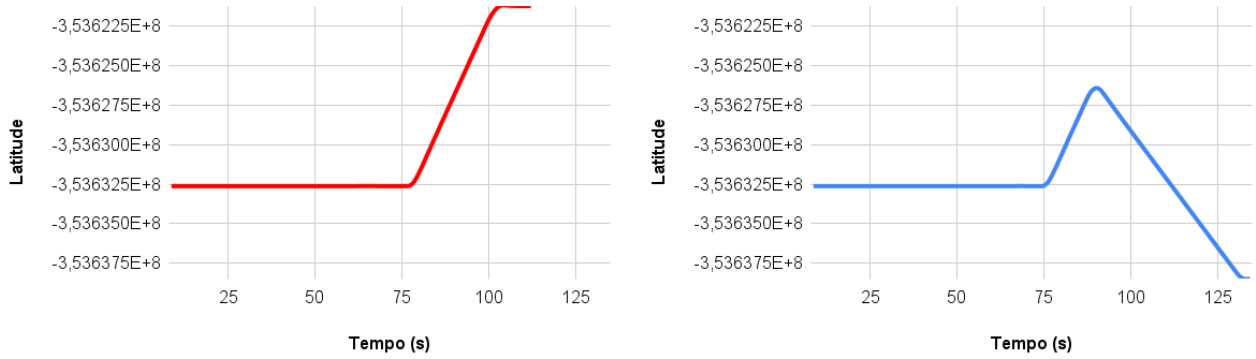
paralelamente durante a missão, em segundo plano.

A Figura 4 apresenta os valores da longitude em relação ao tempo de inicialização para o experimento em condições normais da missão, com a aeronave seguindo para a coordenada de longitude 149,1664594, e para o experimento com o ataque.

De forma similar, a Figura 5 apresenta os valores da altitude em relação ao tempo de inicialização para o experimento em condições normais da missão, com a aeronave seguindo para a coordenada de altitude 100 m, e para o experimento com o ataque.

Comparando os gráficos entre as simulações, observa-se uma alteração em todas as coordenadas de posição em determinado tempo. A curva do gráfico das duas simulações são semelhantes no início para todos as variáveis, porém há uma diferença brusca a partir do momento localizado entre os tempos 75 s e 100 s. Com isso, é possível concluir que houve interferência na comunicação entre VANT e GCS, comprovando a eficácia do ataque.

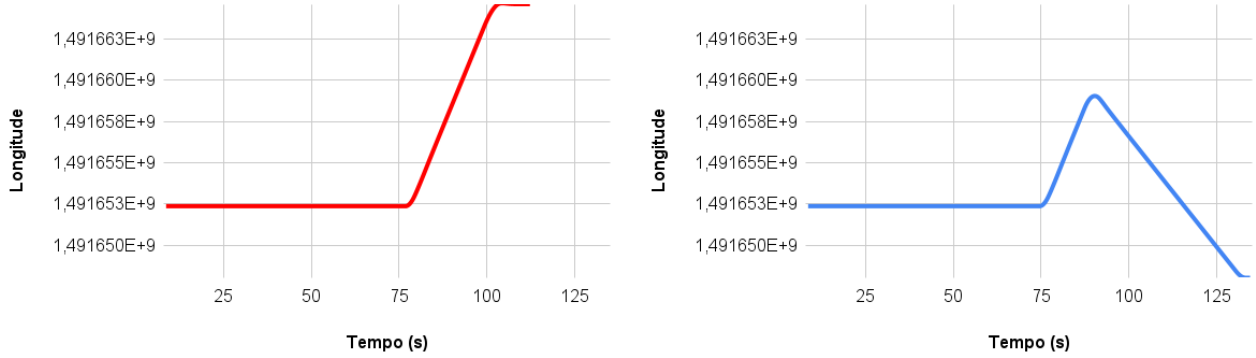
Figura 3 – Latitude capturada ao longo do tempo durante a execução dos experimentos: (a) em condições normais da missão, (b) com a execução do ataque iniciada durante a execução da missão.



(a) **(b)**

Fonte: Elaborado pelos autores (2023).

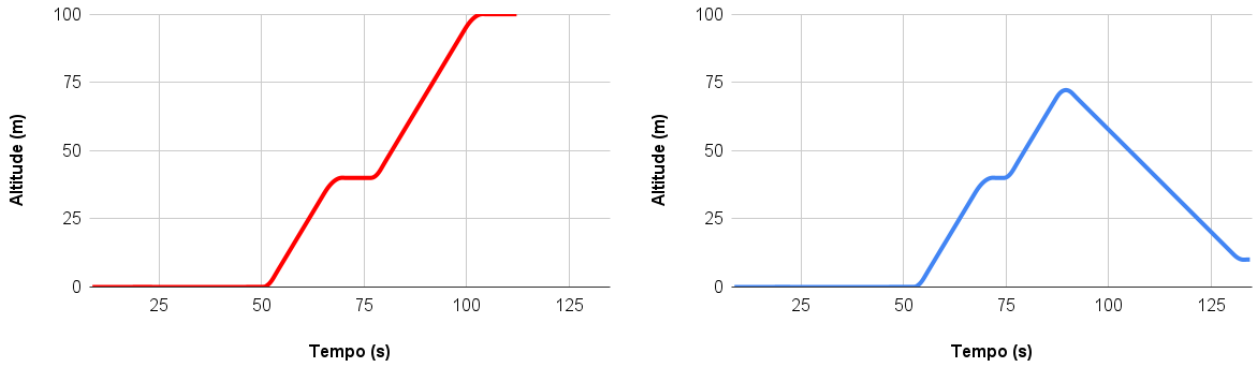
Figura 4 – Longitude capturada ao longo do tempo durante a execução dos experimentos: (a) em condições normais da missão, (b) com a execução do ataque iniciada durante a execução da missão.



(a) **(b)**

Fonte: Elaborado pelos autores (2023).

Figura 5 – Altitude capturada ao longo do tempo durante a execução dos experimentos: (a) em condições normais da missão, (b) com a execução do ataque iniciada durante a execução da missão.



(a) **(b)**

Fonte: Elaborado pelos autores (2023).

CONCLUSÃO

Este trabalho mostrou que, no geral, redes de comunicação de veículos aéreos não tripulados sem nenhum tipo de certificação de segurança estão suscetíveis a ataques e interferências. Os mecanismos de segurança que poderiam contribuir para a defesa contra esses ataques são a criptografia de dados para garantir a confidencialidade e o acesso apenas a dispositivos autorizados ou o uso de mecanismos de autenticação de dispositivos, como o uso da assinatura digital ou de códigos de autenticação de mensagem (STALLINGS, 2015). Em trabalhos futuros, espera-se observar o comportamento dessa comunicação com a implementação desses mecanismos, que provavelmente tornariam os ataques inviáveis. Também é possível investigar novas formas de ataques, como de negação de serviço (DoS ou *Denial of Service*) e ataques de replicação.

Agradecimentos

Agradeço à Universidade Tecnológica Federal do Paraná pelo apoio concedido para a realização desta pesquisa.

Disponibilidade de Código

O *script* utilizado na simulação do ataque e o código para obtenção dos dados estão disponíveis no repositório do GitHub em `https://github.com/Giik4/IC-ataques-VANTS`.

Conflito de interesse

Não há conflito de interesse.

REFERÊNCIAS

ARDUPILOT DEV TEAM. **ArduPilot**. Tokyo, 2023. Disponível em: `https://ardupilot.org/`. Acesso em: 10 ago. 2023.

CONSTANTINIDES, Chris; PARKINSON, Paul. Security challenges in UAV development. In: 2008 IEEE/AIAA 27th Digital Avionics Systems Conference. St. Paul, USA: IEEE, 2008. P. 1.c.1-1-1.c.1–8. DOI: `10.1109/DASC.2008.4702757`.

SHAKHATREH, Hazim et al. Unmanned Aerial Vehicles (UAVs): A Survey on Civil Applications and Key Research Challenges. **IEEE Access**, v. 7, p. 48572–48634, 2019. DOI: `10.1109/ACCESS.2019.2909530`.

SHEPARD, D.P.; BHATTI, Jahshan; HUMPHREYS, Todd. Drone Hack: Spoofing Attack Demonstration on a Civilian Unmanned Aerial Vehicle. **GPS World**, v. 23, p. 30–33, ago. 2012.

STALLINGS, William. **Criptografia e Segurança de redes: princípios e práticas**. 6. ed. São Paulo: Pearson Education do Brasil, 2015. ISBN 978-85-430-1450-0.