Cybersecurity For Unmanned Aerial Vehicles, Concerns, Practices and Conceptual Measures

Nordine Quadar [1], Abdellah Chehri [1], Benoit Debaque [2]
[1] Royal Military College of Canada, Department of Mathematics and Computer Science
E-mail : nordine.quadar@rmc-cmr.ca; chehri@rmc.ca
[2] Thales SA, Thales Digital Solutions (TDS) Canada
E-mail : Benoit.Debaque@thalesgroup.com

Abstract- Unmanned aerial vehicles (UAVs) are quickly advancing technology with high mobility, allowing them to cooperate and perform various tasks. They have commercial uses like goods delivery, military surveillance, and civil operations like search-and-rescue missions. However, malicious UAV attacks have been on the rise recently, causing significant damage. While artificial intelligence (AI) and machine learning can bring "enormous benefits" to society, the same technologies can also bring a range of threats that can enhance current forms of crime or even lead to the evolution of new malicious activities. As a result, industries and standardization bodies are looking for ways to secure UAV systems. We concentrate on cyberattacks rather than physical attacks, which require some form of mechanical contact or physical tools to capture, trap or intercept a targeted UAV. We first categorize UAV cyberattacks based on the communication layer. This leads to five attack categories: physical, data link, network, transport, and application attacks. With this classification in mind, we review the existing literature for appropriate countermeasures. These solutions are organized into three categories: prevention, detection, and mitigation. Thus, the final objective of this paper is to examine previous research, consolidate its findings, and focus on the security of unmanned aerial vehicles. To ensure a more targeted approach, we formulated three research questions, as shown below:

- What are the primary attacks targeting UAVs?
- What are recent advances in UAV security countermeasures?
- What are the limitations and gaps in this area of research?

Lastly, we discuss open challenges in developing these countermeasures and suggest future research directions.

Keywords: Unmanned Aerial Vehicle, UAV, Drones, Cybersecurity, Cyberattack, Countermeasure.