Analyzing the Digital Footprint Of Small UAVs in Conflict: A Cyber Forensics Approach

Pranav Waghmare

Abstract:

In recent years, during the Ukraine Conflict, the use of small unmanned aerial vehicles (UAVs) has increased significantly during war. Their price point and ease of use have attracted various warzones, which has provided significant challenges to military operations and intelligence. Due to their small size, low-altitude flight, and low radar signature, it is challenging to trace them. In this research paper, we will explore methodologies and create a framework for the analysis of the digital footprints of small UAVs.

Introduction:

Using Drones in wars or conflict is not a new phenomenon, but the Ukraine and Russia conflict is significantly different. This is the first time that hobbyist drones, which are meant for civilian usage, have been weaponized to a great extent. The drones used in Ukraine-Russia warfare are for surveillance, intelligence gathering, propaganda, and strikes. This has significantly changed warfare tactics from the past, and due to cost-effectiveness and ease of implementation, this trend is likely to continue. A massive database of drones used in this warfare is available for the public to view, and many aspects of the warfare can be studied based on videos posted by these drones in action and screenshots available. This can be used to create a framework for the future that can help analyze the digital footprint left by small UAVs in war zones.

Methodologies & Framework for Analyzing:

Identification & Automation:

The vast availability of digital footage can provide screenshots and user interface details, as shown in Figure 1 from the drone footage display. This can be later used in the automatic identification of UAVs used in warfare and can give more information about the software used and flight data such as altitude, GPS, and speed. It also offers details about the camera settings. This data can help deduct the approximate location of the drone launch, range, and operation station. The automatic identification system can be developed as more data becomes available.

UAV Classification:

By observing and analyzing the digital footage, UAVs can be classified based on usage. The drones can be classified as follows:

Surveillance UAVs: The focus of these drones is mainly intelligence gathering.

Combat UAVs: These drones are used for strike and impact, delivering the payload to the target.

Logistic UAVs: These drones are mainly used for supply chain operations and logistical purposes.

Propaganda UAVs: These drones are used primarily for psychological warfare, such as dropping leaflets, broadcast messages, etc, to convey propaganda messages and spread misinformation.

AI-based Anomalous flight pattern detection:

A small UAV swarm can overwhelm the opposing side. Based on the footage, an AI-based model can be developed to identify anomalies in drone flight patterns if they are being used for a strike.

Data Collection Strategy:

Data collection strategies can be developed with open-source intelligence analysts, academics, investigative journalists, military, government, and non-government agencies. The collaboration between these agencies is likely to be challenging, but it can help build training data sets and create robust strategies for tackling challenges small UAVs present.

3-D Models:

In the warzone, even if satellite communication may or may not be available sometimes, the 3-D models can be reconstructed based on the footage the small UAVs provide. The footage provided by small UAVs can help create a real-time 3D reconstruction of terrain and structure.

Ethical Considerations:

Operational security is a priority in developing frameworks and methodologies. Secure data handling strategies to maintain privacy can be developed with the collaboration of the government, Military, researchers, journalists, and non-government organizations. Adhering to regulatory and legal standards from the respective jurisdictions should be a priority in developing such a framework.

Mitigation Strategies Development:

Signal Jamming: As shown in **Figure 2**, The drone operator signals can be jammed and obfuscated once the known drone launch station and range of the drones are determined based on the most frequently used drone footage and the display associated with them.

Signal Decryption: Forensic signal decryption can help gather intelligence and provide more operational details.

Drone Hacking: Digital Forensics can eventually help to hack the drone and take control of the drone during the flight, and it can also help enhance operational security.

Conclusion:

Ukraine-Russia has changed the landscape for warfare by using hobbyist and civilian drones in war zones, which has given rise to various challenges. The small drone will be likely to be more popular in future warfare as the Ukraine -Russia war has demonstrated their ease of use, operational impact, and price point associated with them. There are bound to be many changes in this warfare over time. Still, this framework, created by analyzing the digital footprint of small UAVs, can act as one of the foundation and building blocks to track, analyze, and develop mitigation strategies.

Reference:

1. Salamh, Fahad & Karabiyik, Umit & Rogers, Marcus & Matson, Eric. (2021). A Comparative UAV Forensic Analysis: Static and Live Digital Evidence Traceability Challenges.(Figure 2)
2. Królikowski, Hubert. (2022). The Use of Unmanned Aerial Vehicles in Contemporary Armed Conflicts – Selected Issues
3. P. -Y. Kong, "A Survey of Cyberattack Countermeasures for Unmanned Aerial Vehicles," in IEEE Access, vol. 9, pp. 148244-148263, 2021
4. Thompson, K. D. (2024, January 16). How the Drone War in Ukraine Is Transforming Conflict. *Council on Foreign Relations*. https://www.cfr.org/article/how-drone-war-ukraine-transforming-conflict
5. Greenwood, F. (2024, January 19). *Identifying Small Drones from Screenshots and Displays*. Https://www.Bellingcat.com/

   https://www.bellingcat.com/resources/2024/01/19/identifying-small-drones-from-screenshots-and-displays/

6. Franke , U. (2023, August 11). *Drones in Ukraine and beyond: Everything you need to know*. Https://Ecfr.eu/ https://ecfr.eu/article/drones-in-ukraine-and-beyond-everything-you-need-to-know/

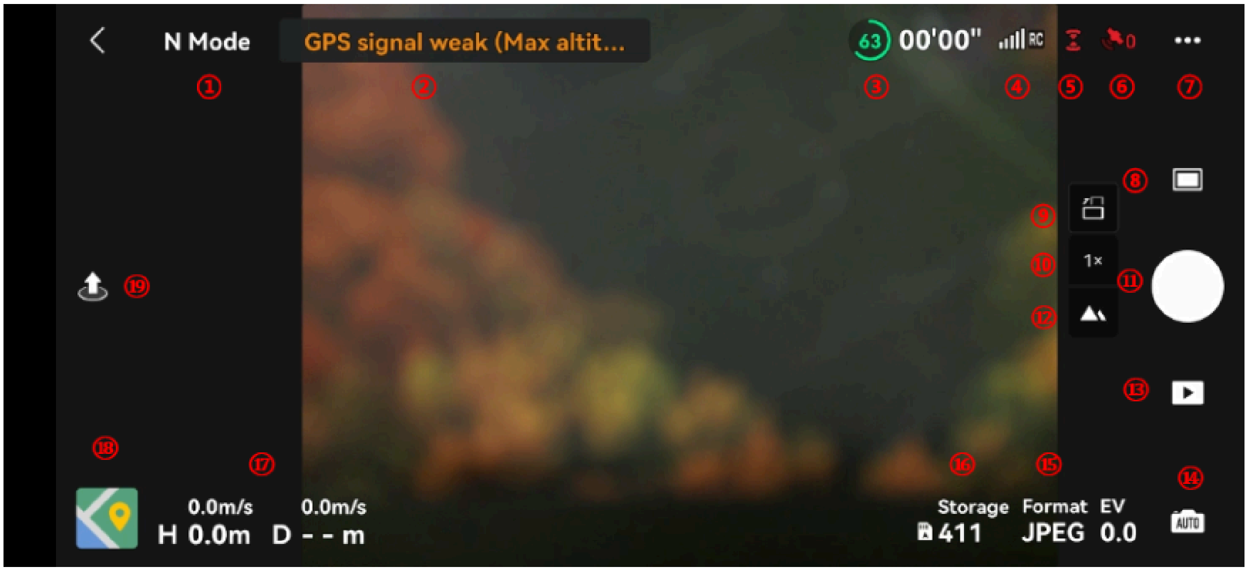
7. DJI drones (2024, January). *Introduction to the DJI Fly App Page*.

(Figure 1)

Https://www.dji.com/Camera-Drones

https://support.dji.com/help/content?customId=en-us03400006562&spaceId=34&re=US&lang=en&documentType=artical&paperDocType=paper

Figure 1



N Mode

GPS signal weak (Max altit...

63 00'00"

0.0m/s H 0.0m

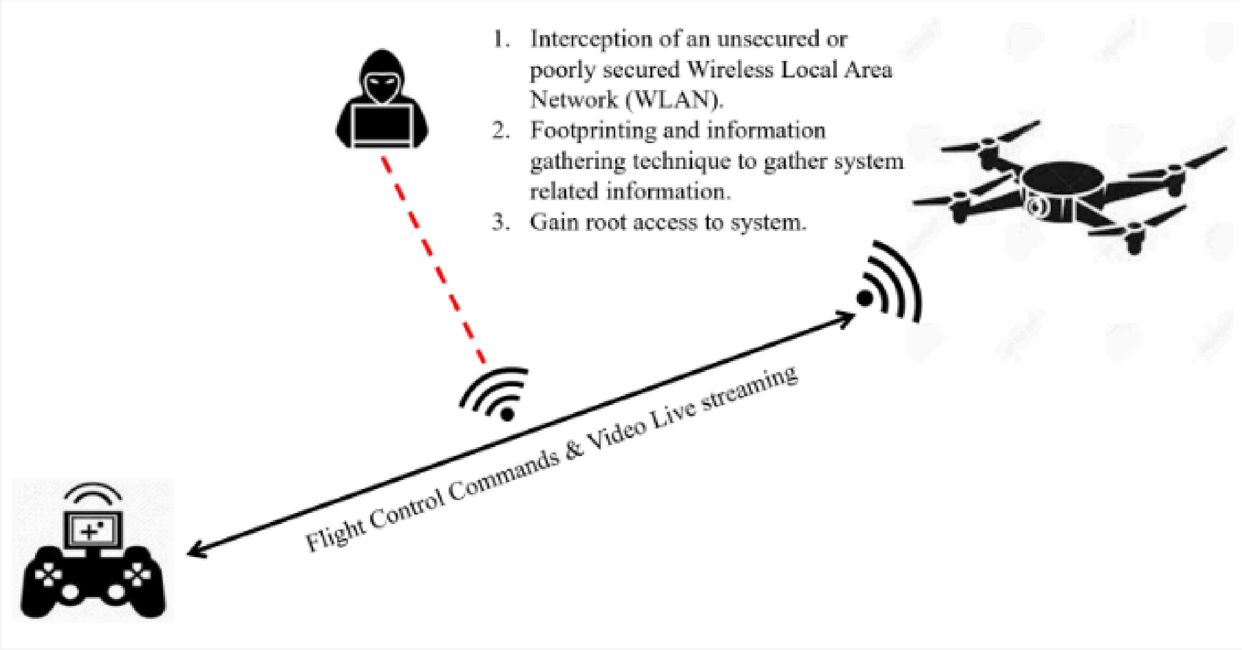
0.0m/s D - - m

Storage 411

Format JPEG

EV 0.0

Figure 2. Scenario layout.



1. Interception of an unsecured or poorly secured Wireless Local Area Network (WLAN).
2. Footprinting and information gathering technique to gather system related information.
3. Gain root access to system.