Comprehensive Security Assessment of Holy Stone Drones: Examining Attack Vectors

Sandesh More, Sneha Sudhakaran, Terrence O'Connor and Marco Carvalho
Florida Institute of Technology, Melbourne, USA

smore2022@my.fit.edu
ssudhakaran@fit.edu
tj@tjoconnor.org
mcarvalho@fit.edu

Abstract: In an era where unmanned aerial vehicles (UAVs) are becoming indispensable across various sectors, from agriculture and logistics to emergency response and warfare, the security of these devices has never been more critical. However, the very features that make drones indispensable also expose them to significant security risks. As UAVs become more pervasive, their vulnerabilities, particularly in commercial off-the-shelf (COTS) models, present escalating threats to privacy, safety, and national security. This study offers a meticulous security analysis of four Holy Stone drone models HS175D, HS430, HS360S, and HS720 chosen for their relevance across varying regulatory frameworks and user bases. Our research uncovers critical vulnerabilities within these UAVs, including exposed Telnet services and unsecured RTSP links, which are particularly concerning due to their potential for unauthorized access and control. Through a combination of rigorous attack simulations and forensic analyses, we demonstrate how these weaknesses can be exploited to intercept sensitive data and disrupt drone operations. The forensic component of our study involved extracting and visualizing flight logs using advanced techniques, revealing how easily attackers can access and manipulate crucial information, raising alarm about the security of drone operations. In addition to identifying these vulnerabilities, we conducted comprehensive reliability testing on the tools and techniques employed in our analysis. This testing was performed across all drone models, utilizing multiple commands and time-based evaluations to ensure the consistency and accuracy of our findings. Moreover, our work validates existing research by simulating a case study that analyzes the traces of attack vectors using reliable forensic tools currently available. This not only confirms the persistent vulnerabilities in UAV technology but also underscores the necessity for robust security measures that can withstand sophisticated cyber threats. Our study concludes with the identification of two critical vulnerabilities, which were reported to the manufacturer, underscoring the urgent need for enhanced security measures in UAV design and operation. By highlighting these vulnerabilities and proposing targeted mitigation strategies, this research contributes to the ongoing discourse on UAV security, advocating for robust industry-wide standards to safeguard against evolving cyber threats.

Keywords: Remote ID, UAV security, Attack model simulation, Forensic analysis, Drone forensics

1. Introduction

The proliferation of small-scale unmanned aerial vehicles (UAVs), also known as drones, has marked a significant technological evolution, presenting vivid opportunities and challenges across various sectors. From agriculture and logistics to entertainment and surveillance, drones have transitioned from being niche hobbyist gadgets to essential tools that drive innovation and efficiency. The accessibility of drones, fuelled by advancements in technology and reduction in costs, has led to their widespread adoption, evidenced by the substantial numbers of drones registered for recreational and commercial purposes in the U.S. as of July 2023 (Statista, 2023). Amidst the expanding diversity in drone technology, the surge in commercial off-the-shelf (COTS) drones has underscored the necessity for stringent security measures. The ease of access and affordability of these drones have not only democratized aerial technology but also exposed potential vectors for misuse, catalyzing security concerns (Kong, 2021; Gowrishetty et al., 2023). The documentation of UAV exploits and the evolving cyber threat landscape targeting drone operations necessitate a robust security posture to safeguard drone technology (Kulp & Mei, 2020; Lounis et al., 2022). Regulatory frameworks by entities like the FAA aim to balance innovation with security; however, the adaptability and enforcement of such regulations, including the new Remote ID rule, remain critical in mitigating risks and ensuring safe airspace for all (Souli et al., 2022; Rathore & Kumar, 2023). This introduction sets the stage for a comprehensive examination of UAV vulnerabilities, leveraging the case studies of specific drone models: HS175D, HS430, HS360S, and HS720 to illustrate broader industry challenges. Our research aims to contribute to this discourse by examining popular Holy Stone models, uncovering vulnerabilities, and proposing effective countermeasures. Inspired by the comprehensive vulnerability analysis (Vattapparamban et al., 2016), this study seeks to provide an in-depth understanding of the attack vectors and security challenges facing drones today. Therefore, our research objective mainly confines to:

- What are the existing vulnerabilities in the targeted drones that was left not mitigated in recent HolyStone models HS 175D, HS 430, HS360, and HS 720?
- What are the success rate of attacks being simulated on these targeted drones and how to mitigated the existing vulnerabilities?

2. Background

2.1 Drone Regulations

The Federal Aviation Administration (FAA) is instrumental in defining the operational framework for Unmanned Aircraft Systems (UAS), emphasizing the necessity for drones weighing more than 0.55 lbs (250 grams) and less than 55 lbs to be registered. This mandate, aimed at enhancing airspace safety and compliance, exposes operators to civil and criminal penalties for non-compliance, highlighting the FAA's commitment to enforcing responsible drone usage (FAA, 2023b). Through educational initiatives like the B4UFLY app and the "Know Before You Fly" campaign, the FAA endeavours to inform drone users about safe flight practices, reinforcing the importance of adherence to established guidelines (FAA, 2023c). Regulations stipulate that small UAVs must operate below 400 feet, maintain visual line of sight, and steer clear of airport vicinities without prior consent, ensuring public safety and minimizing interference with manned aircraft (FAA (2023a)). The Remote ID rule, set to take effect on March 16, 2024, marks a pivotal advancement in drone regulation by requiring most drones operating in U.S. airspace to broadcast identification, location, and altitude data. The FAA categorizes drone operations into four distinct groups: recreational flyers, certified remote pilots or commercial operators, public safety or government users, and educational users. This classification underscores the diverse regulatory landscape navigated by drone operators. Notably, the differentiation based on drone weight and operational intent, particularly under the Remote ID regulations, highlights the complexity within the regulatory framework.

2.2 Study Focus

Our study zeroes in on Holy Stone drones, selected for their blend of affordability, feature richness, and increasing popularity. We examine models which weigh less than 250g (HS175D, HS430, HS360S) and more than 250g (HS720), each showcasing unique features catering to diverse user needs and complying with regulatory frameworks. The models underscore the varying degrees of regulatory compliance, from exemption due to weight to the necessity of a Part 107 FAA drone pilot license for operation, reflecting the broader regulatory and operational landscape of drone usage.

3. Previous Work

The increasing adoption of UAVs across industries has introduced new security concerns. Vulnerabilities to interference attacks, such as jamming and spoofing of GPS, RF, and Wi-Fi signals, are critical, especially for medical delivery systems (Kulp & Mei, 2020). The affordability and ease of use of small UAVs make them vulnerable to detection and disruption (Gordon et al., 2019). The integration of cyber-physical systems introduces unique challenges, exposing communication protocol weaknesses that threaten confidentiality and integrity (Gowrishetty et al., 2023; Kadripathi et al., 2020). Robust tracking and monitoring systems are essential to counter potential malicious use of UAVs (Bertoli et al., 2021; Clark et al., 2017).

The use of UAVs in military environments through the Internet of Battlefield Things (IoBT) creates risks of data compromise via unencrypted channels (Gowrishetty et al., 2023). Spread spectrum communication, though widely employed, can also suffer from vulnerabilities, leading to operational disruptions (Kadripathi et al., 2020). Differentiating normal network behavior from anomalies requires advanced techniques, with deep learning offering potential solutions for UAV protection (Alrefaei et al., 2022). Autonomous counter-drone systems, using software-defined radio (SDR) for spectrum sweeping, provide promising avenues for jamming attacks (Souli et al., 2022). The feasibility of DoS and MouseJack attacks further highlights the need for secure communication protocols (Bertoli et al., 2021; Gowrishetty et al., 2023). Wi-Fi-based drones are particularly susceptible to network attacks, emphasizing the need for enhanced security measures (Westerlund & Asif, 2019).

Drone forensics has evolved alongside these challenges, with research focusing on methodologies for extracting digital evidence from UAVs. Several studies have developed forensic frameworks to retrieve flight logs and other operational data from compromised drones, enhancing understanding of incidents (Mohammed et al., 2023; Yousef & Iqbal, 2019). Tailored procedures specific to different drone models have also advanced the field, offering improved techniques for forensic analysis and event reconstruction (Lan &

Lee, 2021; Hamdi et al., 2019; Kumar & Mohanty, 2021). As UAVs continue to see widespread use, expanding forensic methodologies remains essential for countering emerging cyber-physical threats (Studiawan et al., 2021).

4. Study Design

Our investigation into the security of Holy Stone drones adopts a comprehensive approach, focusing on a spectrum of cyber-attacks that reflect both historical precedents in cybersecurity and contemporary vulnerabilities. The study evaluates multiple attack vectors, including TCP SYN Flood, TCP ACK Flood, UDP Flood, Ping of Death, 802.11 De-authentication, Exposed Telnet Service, Exposed RTSP Service, and Authentication Bypass. These attacks were selected based on their significant impact on the confidentiality, availability, and integrity of the drone.

4.1 Rationale Behind Attack Selection

The selection of attacks for simulation encompassing four flood attacks and four specific vulnerabilities stems from an extensive review of historical and current cybersecurity challenges facing UAV technology (Bogdanoski et al., n.d.; Muthurajkumar et al., 2023). Flood attacks, including TCP SYN, TCP ACK, UDP Flood, and Ping of Death, represent foundational threats in network security (Liu & Sheng, 2008; Tedesco & Aickelin, 2005). These attacks, prevalent in the 1990s, continue to test the resilience of modern systems against volumetric denial-of-service (DoS) threats. The choice to include specific attacks such as the 802.11 De-authentication, Exposed Telnet Service, Exposed RTSP Service, and Authentication Bypass, highlights concerns over confidentiality and control integrity unique to UAV operations (Kadripathi et al., 2020; Chibi et al., 2021). These vulnerabilities are selected based on documented instances within the drone and broader IoT ecosystems, illustrating potential exploitation paths for unauthorized access and control disruption (Rudo & Zeng, 2020; Vattapparamban et al., 2016).

We proposed an architectural diagram for our work on the security analysis of Holy Stone drones as shown in Figure 1. Our research study comprises of attack simulation module mentioning state of analysis with two roles, Role 1- Attacker and Role 2- User.

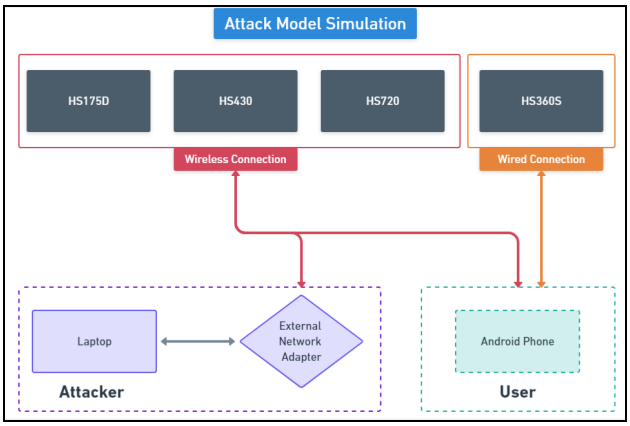

Figure 1: Design Architecture of Holy Stone Vulnerability Assessment

4.2 Attack Model Simulation

The Attack simulation, as shown in Figure 1, involved various participants assuming distinct roles to identify scenarios in which users interact with drones and attackers attack the drones. Therefore, we established the "Attacker's role" and the "User's role." We created specific environments for each role to carry out their respective operations for the simulations to be practical. As depicted in Figure 1, the architectural diagram offers a detailed visualization of the attack model simulation. It illustrates the connection of the target drone primarily to an Android Phone, simulating the user scenario. Simultaneously, our setup also included an external network adapter and laptop, simulating the attacker scenario.

4.3 Attacks Tested with Attack Model Simulation

Vulnerability testing involves simulating several attacks on Holy Stone drone models. The attacks examined in this research include TCP SYN Flood, TCP ACK Flood, 802.11 De-authentication, UDP Flood, Ping of Death, Exposed Telnet with Default Credentials, Exposed RTSP Service, and Authentication Bypass. We have simulated

four flood attacks and three attacks that are specific only to specified drones among the drones we analysed. Flood attacks aim to overwhelm the drone's network capabilities, leading to service disruption. These includes TCP SYN Flood attack, TCP ACK Flood attack, UDP Flood attack, and Ping of Death attack. The commands and success on simulating attacks are explained in Figure 2.

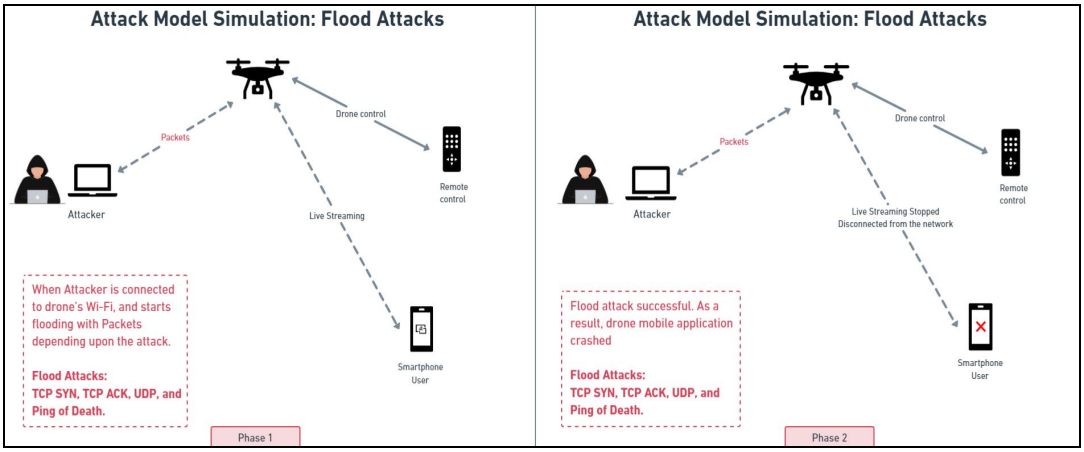

Figure 2: Attack Model Simulation: Flood Attacks

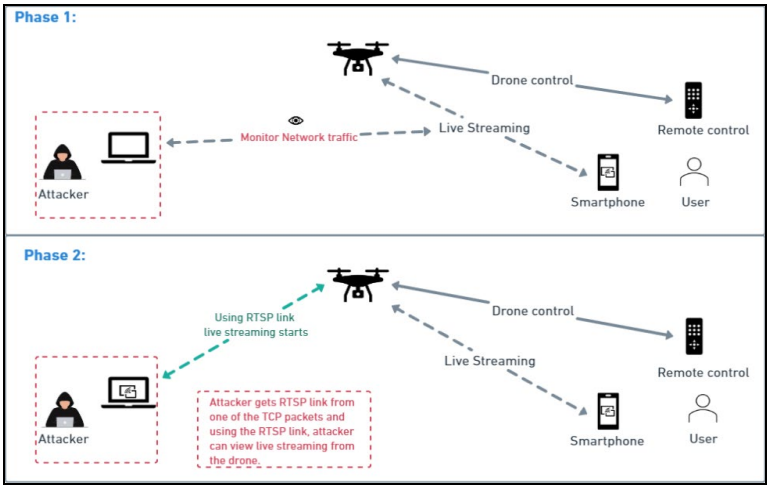

Figure 3: HS175D Exposed RTSP service

4.3.1 TCP SYN Flood

The TCP SYN Flood attack, which floods the target with TCP SYN packets, was successful on the HS175D, HS430, and HS720 models (Zhang et al., 2022; Liu et al., 2008). This attack overloads the server's resources, causing the drone's mobile application to crash and halt live streaming and other functionalities. The attacker uses tools like hping3 to send large number of SYN packets to the drone's network (Zhang, Chen & Bai, 2022). The simulation is shown in Figure 2.

4.3.2 TCP ACK Flood

The TCP ACK Flood attack, targeting the HS430 and HS720 models, involved sending numerous TCP ACK packets (Liu et al., 2008). This attack led to significant delays and crashes in the drone’s network services, impacting their ability to process connections. The simulation is shown in Figure 2.

4.3.3 UDP Flood

The UDP Flood attack was successful on the HS430 and HS720 models (Liu et al., 2008). It entailed sending large number of UDP packets from random ports, causing the drone’s system to become unresponsive due to the inability to process these requests (Liu et al., 2008). The simulation is shown in Figure 2.

4.3.4 Ping of Death

Performed on the HS175D, HS430, and HS720 models, the Ping of Death attack involves sending oversized or malformed ICMP packets (Liu et al., 2008). This overwhelmed the drone's system, leading to the crashing of their mobile applications and halting their operations. The simulation is shown in Figure 2.

4.3.5 802.11 De-authentication

This attack is effective on drone models (HS175D, HS430, and HS720), which involves sending De-authentication frames to disconnect the user from the drone's Wi-Fi network. It resulted in disrupting control and live streaming capabilities from the user (Kadripathi et al., 2020).

4.3.6 Exposed RTSP Service in HS175D

The HS175D model utilizes the RTSP service for broadcasting live video streams to connected smartphones. An attacker can exploit this by monitoring network traffic between the user's smartphone and the drone's Wi-Fi access point. Upon the user starting the live feed via the drone's mobile app, the attacker captures network packets and identifies the RTSP service link, which is transmitted from the drone to the smartphone (Fu et al., 2022). This link allows unauthorized access to the drone's live video feed, posing a significant privacy risk. Figure 3 demonstrates the RTSP vulnerability exploitation process.

4.3.7 Exposed Telnet service with default credentials

This section highlights critical vulnerabilities identified in two distinct Holy Stone drone models, underscoring a broader security concern prevalent across the UAV industry. The HS720 model and the HS175D model both exhibit vulnerabilities that compromise their security posture, albeit through different mechanisms. The HS720 model exposes a critical vulnerability when connected to its Wi-Fi network: an open Telnet service. This allows potential attackers to gain root access to the drone's system. By logging in via Telnet, attackers can access crucial system files and processes, giving them the ability to disrupt Wi-Fi connectivity and disable the drone's application (Dey et al., 2018). This vulnerability is a significant risk, as it can lead to complete loss of control and functionality of the drone.

4.3.8 Authentication bypass

The HS175D drone is prone to an authentication bypass vulnerability. This allows the drone to be controlled by mobile applications designed for other drone brands and are available on both PlayStore and AppStore. Mobile applications such as Bwine, Ruko MINI, and others can fully control the HS175D drone when connected to its Wi-Fi network, bypassing any need for authentication. This poses a significant security threat as it grants unauthorized users complete control over the drone (Chibi et al., 2021).

5. Evaluation

This section evaluates the security vulnerabilities of Holy Stone drone models HS175D, HS430, and HS720 through a series of cyber-attack simulations. By executing each attack type under controlled conditions, we aim to highlight the potential security risks associated with these drones and underscore the importance of enhanced cybersecurity measures.

5.1 Methodology

Our evaluation methodology involves conducting a series of attack simulations, each repeated five times to account for variability and ensure reproducibility of results (Kadripathi et al., 2020; Zhang et al., 2022). This approach allows for a comprehensive analysis of the drones' resilience against cyber threats, with a focus on understanding how different attacks affect each model. The choice of attacks was informed by their relevance to real-world security threats facing UAVs, as well as their potential impact on drone operations (Kong, 2021; Alrefaei et al., 2022).

5.2 Statistical Analysis

In this section, we deliver a detailed statistical analysis, grounding our findings in the average execution times and their standard deviations for each type of attack targeting the drone models. To guarantee the robustness and consistency of our observations, we repeated each attack scenario five times, thus ensuring the reliability of our data. This analysis helps in understanding the potential variability in an actual attack scenario and emphasizes the urgency of addressing these security issues (Liu et al., 2008).

5.3 Detailed Time-Based Evaluation

Here, we detail the findings from our time-based evaluation of attack models, as shown in Figure 4, considering the feedback for including all performed attacks:

Attack	HS 175D 2.4G	HS 175D 5G	HS430 2.4G	HS720 5G
TCP-SYN	8.57 ± 0.50	-	9.20 ± 0.45	39.05 ± 2.00
TCP-ACK	-	-	9.40 ± 0.30	18.11 ± 1.50
De-auth	2.12 ± 0.60	3.79 ± 0.40	4.60 ± 0.50	2.95 ± 0.25
UDP	-	37.11 ± 1.75	3.08 ± 0.20	35.35 ± 1.65
Ping-of-Death	2.47 ± 0.15	-	4.66 ± 0.35	8.56 ± 0.45

Figure 4: Consolidated Attack Times for Drones

- TCP SYN and ACK Flood Attacks: These attacks were particularly effective against the HS720 model, demonstrating its vulnerability to DoS attacks. The substantial delay observed in response times underlines the need for robust network security measures. The choice of these attacks reflects their common use by attackers to disrupt service and gain unauthorized access (Liu & Sheng, 2008).
- De-authentication Attack: Achieved consistent success across all models with minimal variance, highlighting a universal susceptibility to this form of network disruption (Kadripathi et al., 2020). This attack's effectiveness underscores the importance of secure authentication protocols.
- UDP Flood and Ping of Death: These attacks showed varied effectiveness across the models, indicating different levels of network protection (Muthurajkumar et al., 2023). The HS720 model was notably more vulnerable to UDP Flood attacks, suggesting that its network stack might be less resilient to flood-based attacks.
- Exposed RTSP and TELNET Services: The HS175D's vulnerability to RTSP and Authentication Bypass attacks, along with the HS720's exposed TELNET service, point to significant security oversights (Chibi et al., 2021). These vulnerabilities allow attackers to gain unauthorized access and control, emphasizing the need for secure configuration and firmware updates (Dey et al., 2018).

The Figure 5 shows the statistical analysis, grounding our findings in the average execution times and their standard deviations for each type of attack targeting the drone models. The observed variability in response times across different attacks and models underscores the complex nature of these vulnerabilities. Our findings highlight the imperative need for ongoing security enhancements and the adoption of comprehensive cybersecurity measures to safeguard UAV operations against evolving threats.

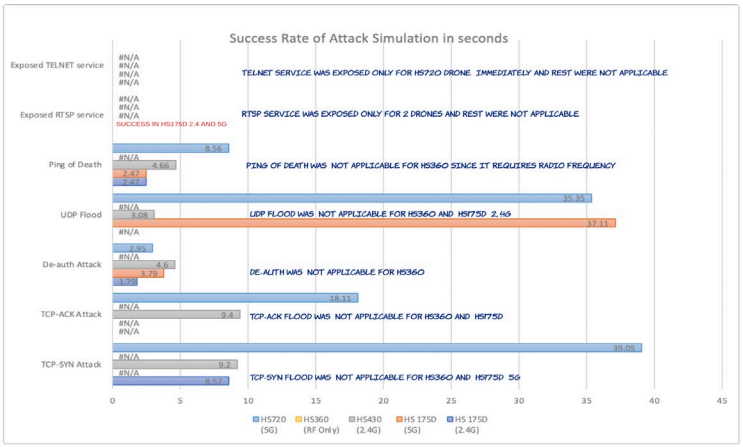

Figure 5: Graphical visualization depicting the average time to launch attacks, highlighting the variance in response times

6. Discussion

Our comprehensive investigation into the security posture of Holy Stone drones, through rigorous cyber-attack simulations, offers significant insights into vulnerabilities that permeate current UAV technologies. This section synthesizes our primary findings, discusses their broader implications for UAV manufacturers and end-users, and outlines actionable recommendations to enhance drone security.

6.1 Insights from Vulnerability Assessment

The study reveals a nuanced vulnerability landscape within Holy Stone drones, with discrepancies in security resilience across different communication standards (2.4G and 5G). Notably, drones operating on 5G frequencies exhibited enhanced resistance to certain cyber-attacks, such as TCP SYN Flood, underscoring the potential of advanced wireless technologies to fortify UAV security (Ferreira et al., 2020). However, the discovery of RTSP and TELNET vulnerabilities across various models highlights a pervasive challenge within the UAV industry: the need for a holistic approach to security, encompassing both hardware and software components (Chibi et al., 2021; Gowrishetty et al., 2023).

6.2 Impact of Attack Models on CIA

As Figure 6 illustrates, various attack models affect the Confidentiality, Integrity, and Availability (CIA) of Holy Stone Drones differently. Flood attacks like TCP-SYN, TCP-ACK, de-authentication, and UDP primarily compromise Availability by overwhelming the network, leading to operational disruptions (Bogdanoski et al., n.d.; Muthurajkumar et al., 2023). Ping of Death Attacks, targeting Availability, exploit vulnerabilities to cause system failures through malformed packets (Gordon et al., 2019). Confidentiality is endangered by Exposed RTSP Services, which allow unauthorized access to live video feeds (Chibi et al., 2021). TELNET Service and Authentication Bypass Attacks threaten both Integrity and Confidentiality by enabling unauthorized modifications and access to the drone's systems and data (Gowrishetty et al., 2023; Bertoli et al., 2021).

Attack Type	HS 175D	HS 430	HS 360S	HS 720	Impact on CIA
TCP SYN Flood	Successful	Successful	-	Successful	Availability
TCP ACK Flood	-	Successful	-	Successful	Availability
802.11 De-authentication	Successful	Successful	-	Successful	Availability
UDP Flood	-	Successful	-	Successful	Availability
Ping of Death	Successful	Successful	-	Successful	Availability
Exposed RTSP Service	Vulnerable	-	-	-	Confidentiality
Exposed Telnet Service with Default Credentials	-	-	-	Vulnerable	Confidentiality, Integrity, Availability

Figure 6: Comprehensive Attack Model Simulation on Holy Stone Drone Models and Their Impact on CIA Triad

6.3 Evaluating UAV Security through Flight Log Analysis

A pivotal aspect of our security assessment involved a meticulous evaluation of flight logs, aimed at uncovering potential data leaks and unauthorized access vulnerabilities. By employing forensic techniques, including the use of digital forensic tools such as Autopsy and ADB, we were able to extract and analyze flight data, revealing the extent to which cyber-attacks could compromise drone operations (Yousef & Iqbal, 2019; Hamdi et al., 2019). For an in-depth evaluation we analyzed the data using methodology developed as shown in Figure 7.

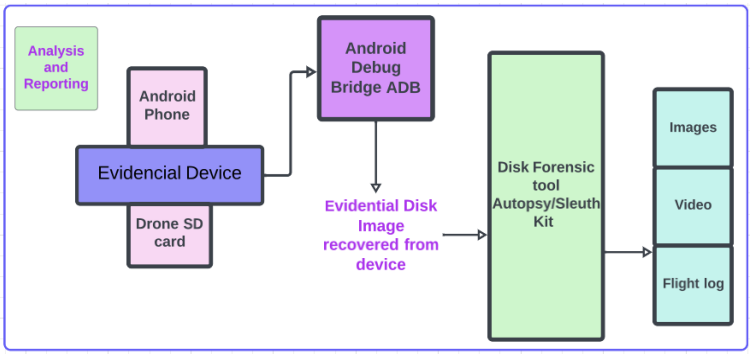

Figure 7: Forensic Workflow for UAV Flight Log Extraction and Analysis

Our approach to analyzing flight logs underscores their value as a forensic tool, offering insights into potential security breaches and operational anomalies. By converting flight data into a format compatible with visualization tools like Google Earth, we could vividly illustrate the drone's flight path, providing a clear depiction of operational behaviors under normal and compromised conditions (Studiawan et al, 2022). This level of analysis not only aids in the forensic investigation of UAV incidents but also serves as a deterrent by highlighting the tangible consequences of security lapses (Lan & Lee, 2021; Bouafif et al., 2018).

Figure 8: Visualization of Drone Flight Path

Figure 9: Visualization of Drone Flight Path with Timeline

The visualizations shown in the Figure 8 and Figure 9, not only demonstrate the efficacy of forensic analysis in UAV security assessment but also highlight the critical need for comprehensive security measures to protect against unauthorized access and ensure the privacy and integrity of flight data.

6.4 Reliability of the Drone Usage

Ensuring the reliable operation of drones requires a comprehensive assessment framework that extends beyond attack simulations. In addition to evaluating potential vulnerabilities, operators must assess the broader operational environment to verify the drone's safety and resilience. Key reliability factors include monitoring for external tampering attempts, evaluating network integrity, and ensuring the drone operates within a patched and secure environment. At the firmware level, operators need to track critical parameters, such as voltage levels, firmware updates, and potential exploits that could compromise the drone's functionality or security. User awareness also plays a pivotal role, as vigilant monitoring of vulnerabilities and environmental conditions is essential for maintaining operational integrity. Future work should explore the development of automated frameworks to monitor these parameters in real time, offering continuous insights into the drone's security and reliability (Sudhakaran et al., 2022).

7. Mitigation Strategies for Identified Vulnerabilities

Figure 6 outlines the vulnerabilities discovered across various Holy Stone drone models. Notably, the HS 175D model exhibited frequency-specific vulnerabilities, with the TCP-SYN attack affecting only the 2.4G band, while the UDP Flood attack was unique to the 5G band. Below are detailed mitigation strategies to address each identified attack vector, focusing on strengthening the drones defense mechanisms against cyber threats:

- TCP SYN Flood: Mitigate SYN queue overflows by enabling TCP SYN cookies, reducing the impact of SYN Flood attacks (Liu & Sheng, 2008).
- TCP ACK Flood: Apply rate limiting on incoming TCP ACK packets to prevent network saturation from ACK Flood attacks (Bogdanoski et al., n.d.).
- 802.11 De-authentication: Implement 802.11w standards to secure management frames, preventing de-authentication and disassociation attacks (Lounis et al., 2022).

- UDP Flood: Use entropy algorithms and token bucket filtering to detect abnormal traffic patterns and manage UDP packet flow effectively (Muthurajkumar et al., 2023).
- Ping of Death: Configure systems to drop oversized ICMP packets and apply rate limits to mitigate Ping of Death attacks (Tedesco & Aickelin, 2005).
- Telnet Service: Secure Telnet services with port knocking techniques, restricting unauthorized access to the service.
- RTSP Streams: Encrypt RTSP links to protect video streams from interception and ensure confidentiality.

8. Conclusion

Our comprehensive examination of Holy Stone drone models HS175D, HS430, HS360S, and HS720 have uncovered significant vulnerabilities, highlighting critical security concerns in these popular consumer drones. Through a series of methodical attack simulations, such as TCP SYN and TCP ACK flood attacks, De-authentication attacks, UDP flood attacks, Ping of Death attacks, and exposure of RTSP and TELNET services, we have documented varying degrees of susceptibility in each model. All targeted drone models showed specific vulnerabilities in several scenarios, especially under 2.4G frequency conditions. Our research also extended into forensic analysis, emphasize the unique challenges each model's distinct file system poses, particularly in extracting photos, videos, and flight logs. The Holy Stone HS360S model stood out for its capability to save drone flight log files, a feature missing in the other models. Overall, we identified the security vulnerabilities in the targeted drone models. Also simulated attacks in a controlled environment, where these attacks were successful in less than a minute. The vulnerabilities are reported to ensure that these vulnerabilities are patched. Moreover, the examination underscores a broader, industry-wide issue, suggesting that clear, comprehensive, strong measures are imperative to fortify drone security against evolving cyber threats while harnessing their vast potential for innovation and utility.

References

Alrefaei, F., Alzahrani, A., Song, H. & Alrefaei, S. (2022). A Survey on the Jamming and Spoofing Attacks on the Unmanned Aerial Vehicle Networks. 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 1-7. IEEE.

Bertoli, G. de C., Pereira, L. A. & Saotome, O. (2021). Classification of Denial of Service Attacks on Wi-Fi-based Unmanned Aerial Vehicles. 2021 10th Latin-American Symposium on Dependable Computing (LADC), 1-6. IEEE.

Bogdanoski, M., Shuminoski, T., & Risteski, A. (2012). TCP SYN Flooding Attack in Wireless Networks. https://doi.org/10.13140/2.1.3487.3282

Bouafif, H., Kamoun, F., Iqbal, F., Marrington, A., 2018. Drone Forensics: Challenges and New Insights, in: 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), IEEE, Paris, pp. 1–6.

Chibi, N. T., Ghazi, H. E. & Fihri, W. F. (2021). Drone Cyber-Attack: An Intrusion Detection Technique Based on RSSI and Trilateration. 2021 Third International Conference on Transportation and Smart Technologies (TST), 42-45. IEEE.

Clark, D. R., Meffert, C., Baggili, I. & Breitinger, F. (2017). DROP (Drone Open source Parser) your drone: Forensic analysis of the DJI Phantom III. Digital Investigation, 22(S3), S3-S14.

Dey, V. *et al.* (2018) 'Security Vulnerabilities of Unmanned Aerial Vehicles and Countermeasures: An Experimental Study', in *2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID)*. *2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID)*, Pune: IEEE, pp. 398–403.

FAA. (2023a). UAS Recreational Flyers: Authorization. Available at: https://www.faa.gov/uas/recreational_flyers/authorization.

FAA. (2023b). UAS Getting Started: User Identification Tool. Available at: https://www.faa.gov/uas/getting_started/user_identification_tool.

Ferreira, R., Gaspar, J., Sebastião, P. & Souto, N. (2020). Effective GPS Jamming Techniques for UAVs Using Low-Cost SDR Platforms. Wireless Personal Communications, 115(4), 2705-2727.

Gordon, J., Kraj, V., Hwang, J. H. & Raja, A. (2019). A Security Assessment for Consumer WiFi Drones. 2019 IEEE International Conference on Industrial Internet (ICII), 1-5. IEEE.

Gowrishetty, N. M., Chukkapalli, S. S. L. & Joshi, A. (2023). Bewitching the Battlefield: Repurposing the MouseJack Attack for Crazyflie Drones. IEEE INFOCOM 2023 Workshops (INFOCOM WKSHPS), 1-6. IEEE.

Hamdi, D. A., Iqbal, F., Alam, S., Kazim, A. & MacDermott, A. (2019). Drone Forensics: A Case Study on DJI Phantom 4. 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), 1-6. IEEE.

Kadripathi, K., Ragav, L. Y., Shubha, K. & Chowdary, P. H. (2020). De-Authentication Attacks on Rogue UAVs. 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), 1178-1182. IEEE.

Kong, P.-Y. (2021). A Survey of Cyberattack Countermeasures for Unmanned Aerial Vehicles. IEEE Access, 9, 148244-148263.

Kulp, P. & Mei, N. (2020). A Framework for Sensing Radio Frequency Spectrum Attacks on Medical Delivery Drones. 2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC), 408-413. IEEE.

Lan, J. K. W. & Lee, F. K. W. (2021). Drone Forensics: A Case Study on DJI Mavic Air 2. 2021 23rd International Conference on Advanced Communication Technology (ICACT), 291-296. IEEE.

Liu, P.-E. & Sheng, Z.-H. (2008). Defending against tcp syn flooding with a new kind of syn-agent. 2008 International Conference on Machine Learning and Cybernetics, 1218-1221. IEEE.

Lounis, K., Ding, S.H.H., Zulkernine, M., 2022. Cut It: Deauthentication Attacks on Protected Management Frames in WPA2 and WPA3, in: Aïmeur, E., Laurent, M., Yaich, R., Dupont, B., Garcia-Alfaro, J. (Eds.), Foundations and Practice of Security. Springer International Publishing, Cham, pp. 235–252.

Mohammed, A. S., Hasanaath, A. A., Moinuddeen, A. & Mohammad, N. (2023). A Comparative Study of Drone Forensic Tools and Techniques. 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), 752-758. IEEE.

Muthurajkumar, S., Geetha, A., Aravind, S. & Meharajnisa, H. B. (2023). UDP Flooding Attack Detection Using Entropy in Software-Defined Networking. In: Proceedings of International Conference on Communication and Computational Technologies, 549-560. Springer Nature Singapore.

Rathore, A. & Kumar, C. (2023). Cyber Forensics Analysis of FPV-Non FPV Drones. 2023 International Conference for Advancement in Technology (ICONAT), 1-6. IEEE.

Rudo, D., Zeng, D.K., 2020. Consumer UAV Cybersecurity Vulnerability Assessment Using Fuzzing Tests.

Souli, N., Kolios, P. & Ellinas, G. (2022). An Autonomous Counter-Drone System with Jamming and Relative Positioning Capabilities. ICC 2022 - IEEE International Conference on Communications, 5110-5115. IEEE.

Statista. (2023). Number of UAS Drone Registrations in the United States as of July 2023. Available at: https://www.statista.com/statistics/1221517/uas-drone-registrations-united-states/.

Studiawan, H., Ahmad, T. & Shiddiqi, A. M. (2021). Forensic Event Reconstruction for Drones. 2021 4th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), 41-45. IEEE.

Sudhakaran, S., Ali-Gombe, A., Case, A., & Richard III, G. (2022). Evaluating the Reliability of Android Userland Memory Forensics. ICCWS 17, 423–432. https://doi.org/10.34190/iccws.17.1.54

Tedesco, G., Aickelin, U., 2005. Strategic Alert Throttling for Intrusion Detection Systems. SSRN Journal.

Vattapparamban, E., Guvenc, I., Yurekli, A. I., Akkaya, K. & Uluagac, S. (2016). Drones for smart cities: Issues in cybersecurity, privacy, and public safety. 2016 International Wireless Communications and Mobile Computing Conference (IWCMC), 216-221. IEEE.

Westerlund, O., Asif, R., 2019. Drone Hacking with Raspberry-Pi 3 and WiFi Pineapple: Security and Privacy Threats for the Internet-of-Things.

Yousef, M. & Iqbal, F. (2019). Drone Forensics: A Case Study on a DJI Mavic Air. 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), 1-3. IEEE.

Zhang, X., Chen, L. & Bai, J. (2022). SYN Flood Attack Detection and Defense Method Based on Extended Berkeley Packet Filter. In: Advances in Natural Computation, Fuzzy Systems and Knowledge Discovery, 1416-1427. Springer International Publishing.