SECURITY ANALYSIS OF DRONE COMMUNICATION METHODS

Kymani Brown
Kymani.brown@udc.edu
University of the District of Columbia

Anteneh Girma
anteneh.girma@udc.edu
University of the District of Columbia

Abstract

The use of drones in various applications has increased significantly in recent years, including agriculture, transportation, and military operations. Drones are equipped with various communication technologies that enable them to transmit and receive data to and from their operators or other drones. However, the use of these communication technologies can also pose significant security risks, as they can be vulnerable to cyberattacks that can compromise the confidentiality, integrity, and availability of the data transmitted. This research paper presents a comprehensive security analysis of drone communication methods. The paper explores the different communication methods used in drones, such as wireless communication protocols, including Wi-Fi, Bluetooth, and cellular networks. The analysis aims to identify security risks associated with these communication methods and assess the security of the drone's software and hardware components. The research paper reviews the current state of drone communication security identifies the most significant security risks and discusses the impact of cyberattacks on drones and their operators.

Key words: Drone Security, Drone Communications, Drone Layer Securiy, Drone and Wireless

1. INTRODUCTION

The increasing popularity of drones has led to a rise in their use in both the public and private sectors. Drones are used for a variety of purposes, including aerial photography, search and rescue operations, package delivery, and military reconnaissance. However, this increase in drone usage has also led to an increase in cybersecurity risks. Drones are equipped` with a variety of sensors and cameras that can be used to collect and transmit sensitive information. If this information falls into the wrong hands, it can be used for criminal or terrorist activities. Additionally, drones themselves can be targeted and hijacked, posing a significant threat to public safety and national security.

Cybersecurity threats to drones are numerous and diverse. They include unauthorized access, theft of data, sabotage, and jamming of communication systems. Drone manufacturers are making efforts to enhance the security of their products, but this is not enough. Operators of drones also need to take measures to protect their devices and the data they collect. There is a need for a comprehensive approach to drone
cybersecurity that addresses both hardware and software vulnerabilities, as well as the human factor.

This research paper aims to contribute to the development of such an approach. The paper provides an overview of the cybersecurity risks associated with drones and identifies the most significant threats. It also proposes effective solutions for mitigating these threats, such as encryption of data, implementation of security protocols, and training of drone operators on cybersecurity best practices. By presenting a comprehensive understanding of the cybersecurity risks associated with drones, this research paper aims to promote the safe and secure operation of drones in both the public and private sectors. Ultimately, this research paper seeks to contribute to the development of a more secure and resilient drone ecosystem.

2. Literature Review

According to Manimaran Mohan, the author of the paper "Cybersecurity in Drones," the data that drones collect and transmit endangers the safety of the drone and those in its vicinity. [2] The paper identifies several vulnerabilities in drones that make them vulnerable to cyberattacks, including weak encryption, unsecured wireless networks, and a lack of authentication mechanisms. Mohan proposes a variety of cybersecurity measures to mitigate these risks, including the use of strong encryption protocols, secure communication channels, and the implementation of authentication mechanisms to prevent unauthorized access to the drone's systems. [2] The paper also emphasizes the importance of ongoing monitoring and testing in order to detect and address any vulnerabilities that may emerge over time. [7]

Chia-Nan Wang et al. emphasize the importance of efficient and secure wireless communication

technologies in order to meet the growing demand for data security.[3] The authors argue that unmanned aerial vehicles (UAVs) are a promising application for improving data security in the cybersecurity industry. The authors also propose a UAV-based wireless communication system for secure data transmission in remote and inaccessible locations.[7] A UAV equipped with a wireless communication module and a ground station that communicates with the UAV comprise the proposed system. The authors demonstrate the effectiveness of the proposed system through experiments carried out in a real-world setting.[3] The results demonstrate that the proposed system is capable of providing secure and efficient wireless communication for data transmission in remote and inaccessible areas.

Abdulaziz Aldaej, et al, proposes a smart cybersecurity framework for IoT-empowered drones based on machine learning. The paper highlights the increasing cybersecurity threats to IoT-empowered drones, including hacking attacks, data breaches, and unauthorized access. [1] The authors argue that traditional cybersecurity measures are insufficient to address these threats and propose a smart cybersecurity framework that leverages machine learning techniques to identify and mitigate potential security breaches.
The proposed framework consists of several components, including a data collection module, a machine learning-based intrusion detection system, and a response and mitigation module.[1] The data collection module collects data from various sources, such as drone sensors and network traffic, and feeds it into the intrusion detection system, which uses machine learning algorithms to identify anomalous behavior and potential threats. The response and mitigation module then takes the necessary steps to avoid or mitigate the identified threats.
Experiments on a real-world drone platform are used by the authors to demonstrate the effectiveness of the proposed framework. The results show that the framework can detect a variety of cyber threats, such as denial-of-service attacks, man-in-the-middle attacks, and data exfiltration attacks. [7] This paper's findings are supported by a growing body of research on cybersecurity for IoT-enabled drones. For example, Kaur et al. (2021) proposed a blockchain-based security framework for drones that improves drone security and privacy. Al-Jarrah et al. (2018) proposed a secure communication framework for drones that employs elliptic curve cryptography and digital signatures to prevent unauthorized access.

The paper written by Hani Ismael, et al. describes an efficient linearly homomorphic authenticated encryption (LinHAE) scheme designed for a multi-rotor drone's ground control center. The proposed LinHAE ensures real-time operation for safe autonomous flight, security against eavesdropping and forgery attacks, and state updates via additions and multiplications by a system-specific constant. LinHAE, unlike homomorphic encryption alone, allows the drone to verify the authenticity of received signals. [6]
The authors describe the integration of a LinHAE with security and computational tractability into standard drone system architecture and the implementation of the specific controller.[6] The paper describes the first successful operation of a multi-rotor flying robot flying autonomously under the control of a ground controller while using real-time homomorphic authenticated encryption.

The research paper by Tippenhauer, N., et al. presents a novel deep learning approach using Convolutional Neural Networks (CNNs) to detect GPS spoofing attacks on Unmanned Aerial Vehicles (UAVs). GPS spoofing is a cyberattack that manipulates the GPS signals received by a drone, causing incorrect positioning information and potential deviations from its intended path.[7] The authors developed a CNN-based model to classify legitimate and spoofed GPS signals by analyzing raw radio frequency (RF) data.[4] The model was trained on a dataset containing both genuine and spoofed GPS signals, and its performance was evaluated using accuracy, precision, recall, and F1 score metrics. Experimental results demonstrated that the proposed deep learning approach achieved high accuracy in detecting GPS spoofing attacks on UAVs, significantly outperforming traditional signal-processing-based methods. Furthermore, the model exhibited robustness against various types of spoofing attacks, highlighting its potential as a promising solution for enhancing UAV security.

This paper by Chao, L., et al. discusses the security and privacy challenges associated with the Internet of Drones (IoD) as drones become increasingly integrated into various industries and applications. The authors outline various security and privacy issues, potential attack vectors, and propose several solutions, including cryptographic techniques and secure communication protocols.[5] They emphasize the need for a comprehensive security framework and collaboration between academia, industry, and policymakers to ensure the protection of drones and their users.

This paper addresses the cybersecurity challenges associated with drone data communication systems, particularly when monitoring critical infrastructure. Common security gaps include insufficient encryption, vulnerable communication protocols, weak authentication and access control, insecure firmware and software updates, lack of intrusion detection and prevention systems, physical security vulnerabilities, and inadequate cybersecurity awareness and training among operators.[7] These vulnerabilities expose drones to various cyber threats, such as denial-of-service, man-in-the-middle, malware injections, and GPS spoofing, potentially leading to compromised data integrity or loss of control over the drones.[7] To mitigate these risks, it is essential to implement robust security measures, including encryption, secure communication protocols, and intrusion detection systems, while fostering cybersecurity awareness among stakeholders.[1]

3. Proposed Solution Approach

To conduct this research comprehensively and produce actionable insights, the approach is organized into the following structured phases:

Phase 1:Tailored Investigation of Communication Methods

- **Segmentation of Drone Categories:**

Classify drones into Consumer-grade and Military-grade, considering cost, operational time, complexity, and legal constraints.

- **Focused Analysis of Communication Channels:**

Investigate the most commonly used communication methods for each category, focusing on their distinct security challenges.

Phase 2: Differentiated Security Risk Assessment

- **Vulnerability Mapping:**

Identify unique vulnerabilities for Consumer-grade and Military-grade drones, particularly in encryption, communication protocols, and access controls.

- **Segment-Specific Impact Analysis:**

Conduct an impact analysis that takes into consideration the specific requirements and constraints of each category (Consumer-grade vs. Military-grade), evaluating risks to the CIA triad.

Phase 3: Security Measure Design

- **Cost-Effective Solutions for Consumer-Grade Drones:**

Develop security measures that are effective but also cost-sensitive, ensuring accessibility and affordability.

- **Advanced Security Protocols for Military-Grade Drones:**

Develop high-end, advanced security measures with less concern for cost but focusing on robustness and mission-critical reliability.

- **Layered Security Approach:**

For both categories, focus on multiple layers of security, from robust encryption algorithms to intrusion detection systems, that are tailored to the unique characteristics of each drone category.

- **Human Factors:**

Propose comprehensive training modules to increase cybersecurity awareness among drone operators in both sectors, given the identified lack of such awareness.

Phase 4:Risk Mitigation Strategy Formulation

- **Threat Modeling and Strategy Formulation:**

Employ threat modeling techniques to prioritize risks and formulate category-specific mitigation strategies.

- **Cost-Benefit Analysis for Risk Mitigation:**

Conduct a comparative cost-benefit analysis to identify the most cost-effective mitigation strategies for Consumer-grade and Military-grade drones, factoring in the results from the Comparative Analysis.

- **Implementation Roadmap:**

Develop a phased roadmap for each category, identifying milestones, required resources, and timelines for the implementation of the security measures.

- **Continual Review and Update:**

Establish protocols for regular reviews and updates of security measures, factoring in evolving threats and technological advancements in drone capabilities.

4. Analysis & Discussion of Drone Communications Techniques

To provide a clear and comprehensive comparison between Consumer-grade and Military-grade drones in terms of their communication systems, security measures, and overall performance, the information is presented in the form of a matrix below:

Criteria	Consumer-Grade Drones	Military-Grade Drones
Communication System		
- Radiofrequency (RF)	2.4GHz & 5.8GHz	Satellite links, dedicated frequ
- Wi-Fi	Commonly used	Rarely used
- Latency	High	Low
- Data Transfer Rate	Lower	Higher
- Range	Limited	Extended
Security Measures		
- Encryption	Basic (WAP2, WAP3)	Advanced protocols
- Vulnerability	Susceptible to hacking	Highly secure
- Authorized Access	Open	Restricted
Overall Performance		
- Responsiveness	May be slow	Highly responsive
- Data-Intensive Payloads	Limited	Capable
- Resilience	Lower	Higher (System redundancies)

Consumer-grade drones typically employ RF communication in the 2.4GHz and 5.8GHz bands and Wi-Fi, which, although cost-effective, suffer from high latency and reduced range, making them prone to interference. Their security measures, such as WAP2 and WAP3 encryption, are basic and often inadequate against serious threats. The performance of these drones is also compromised due to their communication system limitations. In contrast, military-grade drones utilize advanced RF systems, including satellite links, which reduce latency and enhance data transfer. They also incorporate advanced encryption and security protocols, safeguarding against cyber-attacks, signal jamming, and other threats. Additionally, they are equipped with secure hardware and redundant systems, ensuring superior performance suitable for specialized and critical missions.

5. Comparative Analysis

Consumer-grade drones typically employ RF communication in the 2.4GHz and 5.8GHz bands and Wi-Fi, which, although cost-effective, suffer from high latency and reduced range, making them prone to interference. Their security measures, such as WAP2 and WAP3 encryption, are basic and often inadequate against serious threats. The performance of these drones is also compromised due to their communication system limitations. In contrast, military-grade drones utilize advanced RF systems, including satellite links, which reduce latency and enhance data transfer. They also incorporate advanced encryption and security protocols, safeguarding against cyber-attacks, signal jamming, and other threats. Additionally, they are equipped with secure hardware and redundant systems, ensuring superior performance suitable for specialized and critical missions.Several factors differentiate consumer-grade drones from military-grade drones, such as cost, time of operation, complexity, security and legal concerns, size and weight, and battery life. Consumer-grade drones are designed to be affordable and accessible, using off-the-shelf components and lower-cost communication systems like Wi-Fi and standard RF bands. Due to smaller battery capacities and less efficient energy management systems, they have limited operational time, usually around 20-30 minutes. These drones are built for simplicity and ease of use, with user-friendly controls and straightforward navigation systems. However, they face various security and legal concerns, and their battery life is typically shorter than that of military-grade drones.

In contrast, military-grade drones are developed with advanced technologies and high-grade materials, resulting in a higher cost. They are built for extended missions, featuring efficient power management systems and larger battery capacities, allowing them to operate for several hours or even days. These drones are more complex, require specialized training, and are subject to strict security and legal protocols. Military-grade drones come in various sizes and weights, designed for specific purposes with mission requirements and payload capabilities determining their dimensions. Applying military-grade security to consumer-level drones would increase their cost, complexity, and weight, making them less affordable and accessible. However, it is crucial to continue improving consumer drone security and implementing best practices to protect user data and privacy without necessarily employing military-grade solutions.

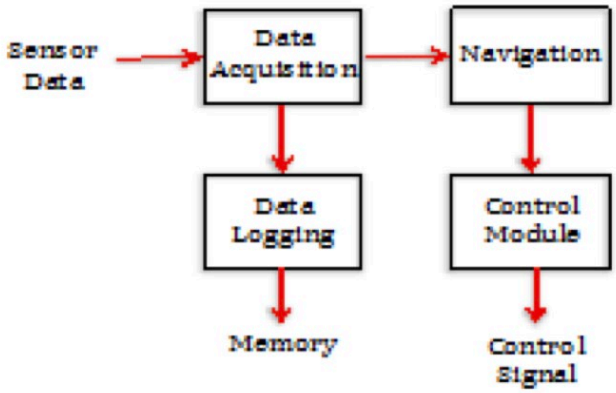

Figure 1. UAV Data Collection Module

This analysis focuses on the security gaps found in drone data communication systems used for monitoring critical infrastructure. Insufficient encryption is a significant concern, as weak or non-existent encryption methods can lead to intercepted and deciphered data, compromising sensitive information. To address this, it is crucial to

implement robust encryption algorithms and regularly update cryptographic keys to ensure data security during transmission.

Vulnerable communication protocols, such as Wi-Fi or Bluetooth, expose drones to attacks like man-in-the-middle, eavesdropping, or signal jamming. Adopting secure and resilient communication protocols, along with measures like mutual authentication and message integrity checks, is essential to mitigate these risks.

Weak authentication and access control mechanisms can allow unauthorized users to access the drone's communication system or even gain control of the drone. Implementing strong authentication methods, such as multi-factor authentication and role-based access controls, can help prevent unauthorized access.

Insecure firmware and software updates allow attackers to inject malware or malicious code into the drone's system. To counter this, ensuring secure update processes through measures like digital signing, encrypted transmission, and verification of update integrity is vital.

The absence of intrusion detection and prevention systems hinders the ability to identify and respond to cyberattacks in real time. Implementing these systems, preferably with AI and machine learning capabilities, can enhance the drone's resilience to cyber threats and enable timely responses to potential attacks.

Physical security vulnerabilities, such as GPS spoofing, can cause drones to lose accurate position information or be led astray. Countermeasures like multi-sensor fusion techniques and anti-spoofing algorithms can help drones maintain precise positioning data and resist spoofing attempts.

Lastly, inadequate cybersecurity awareness and training among drone operators and organizations contribute to the increased vulnerability of drone communication systems. Providing comprehensive training and promoting a culture of cybersecurity awareness can help mitigate human-related risks and ensure that stakeholders are well-equipped to prevent and respond to cyber threats effectively.

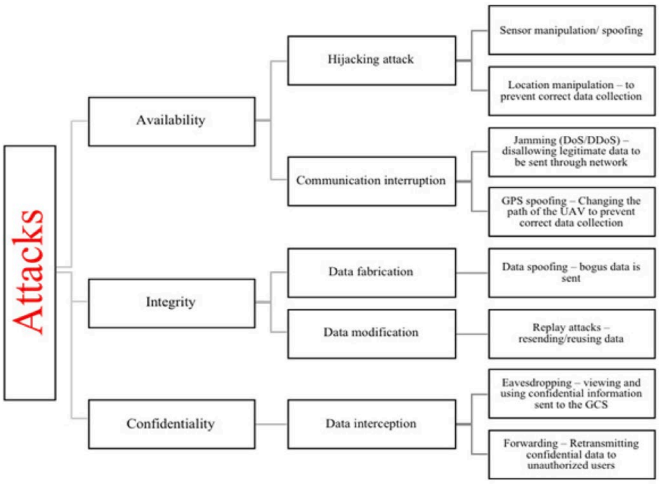

Figure 2. Taxonomy of attacks on the UAV-to-GCS communication links and data.

6.. Risk Mitigation Techniques

Table

No.	Risk Mitigation Technique	Description
6.1	Performing a threat model	Systematically analyze security threats and countermeasures for drone communication. Identify assets, define potential adversaries, and understand attack vectors. This comprehensive model helps prioritize risks and decide on effective countermeasures.
6.2	Formulating strategies	Based on the threat model, create strategies to counteract risks in drone communication. This might involve robust encryption, secure protocols, and frequent security updates. Also, consider redundancy in communication systems to ensure drone operation in case of attacks or system failures.
6.3	Generating a proposal	Develop a document outlining security measures based on the analysis. This proposal should serve as a roadmap for necessary protections against cyberattacks targeting drone communication. It should be regularly reviewed and updated for evolving threats and technological advancements.
6.4	Categorizing significant security risks	Classify security risks of each communication method based on impacts on confidentiality, integrity, and data availability. This helps prioritize resources and efforts for security implementation. Focus on high-impact risks first and keep monitoring and reassessing lower-impact ones.
6.5	Conduct penetration tests	Regularly simulate real-world cyberattacks to find vulnerabilities. Target various parts of the drone's communication systems, such as encryption, protocols, and hardware. Use these test results to address vulnerabilities, enhance security, and ensure resilience against potential attacks.

7. Conclusion

In conclusion, secure communication is of paramount importance for the safe and reliable operation of drones, whether they are consumer or military-grade. As drones continue to proliferate and integrate into various aspects of our lives, ensuring the integrity, confidentiality, and availability of their communication systems is crucial.

The key factors differentiating consumer and military drones, such as cost, complexity, and size, impact their communication systems and security measures. While military-grade drones incorporate advanced encryption, secure channels, and robust systems to protect against cyber threats, consumer-grade drones often face

limitations due to affordability and accessibility concerns.

To enhance the security of drone communication, it is essential to employ risk mitigation techniques, including threat modeling, formulating strategies, generating security proposals, categorizing risks, and conducting penetration tests. These methods help identify vulnerabilities and develop appropriate countermeasures to safeguard drones from potential cyberattacks.

Collaboration among industry stakeholders, governments, and researchers is vital for promoting best practices, developing regulations, and addressing emerging security challenges. By fostering a culture of security awareness and proactively addressing potential threats, we can ensure the safe and secure operation of drones across various applications, benefiting consumers and military personnel.

8. REFERENCES

[1] *Aldaej, Abdulaziz, et al. "Smart Cybersecurity Framework for IoT-Empowered Drones: Machine Learning Perspective." Sensors, vol. 22, no. 7, Mar. 2022, p. 2630. DOI.org (Crossref), https://doi.org/10.3390/s22072630.*

[2] *Mohan, M. "Cybersecurity in Drones." Semantic Scholar, 1 Jan. 1970, https://www.semanticscholar.org/paper/Cybersecurity-in-drones-Mohan/a6f36c4c9bd34d1b4e092b5b33fb44a725fd26dc.*

[3] *Wang, Chia-Nan, et al. "Wireless Communications for Data Security: Efficiency Assessment of Cybersecurity Industry-a Promising Application for Uavs." MDPI, Multidisciplinary Digital Publishing Institute, 19 Nov. 2022, https://www.mdpi.com/2504-446X/6/11/363.*

[4] *Tippenhauer, N., Pöpper, C., & Rasmussen, K. (n.d.). On the Requirements for Successful GPS Spoofing Attacks. Retrieved March 27, 2023, from https://www.cs.ox.ac.uk/files/6489/gps.pdf*

[5] *Chao, L., Debiao, H., Neeraj, K., Kim-Kwang, R. C., Alexey, V., & Xinyi, H. (n.d.). Security and Privacy for the Internet of Drones: Challenges and Solutions. Ieeexplore.ieee.org. Retrieved March 27, 2023, from https://ieeexplore.ieee.org/abstract/document/8255739*

[6] *Ismael, H. M. 1, & Al-Ta'i, Z. T. M. 1 1 D. of computer science. (2021). Authentication and encryption drone communication by using hight lightweight algorithm. 5891–5908. https://www.proquest.com/docview/2639740375?parentSessionId=mJoo0j5AyRcz0kHLJlQCRkQr9WQCrkhhpj0D21uOUfQ%3D&pq-origsite=primo&forcedol=true*

[7] *H. Benkraouda, E. Barka, and K. Shuaib, "Cyber-attacks on the data communication of drones monitoring critical infrastructure," in Computer Science & Information Technology (CS & IT), 2018. https://doi.org/10.5121/csit.2018.81708.*

[8] *K. Wesson and T. Humphreys, "Hacking drones," Scientific American, vol. 309, no. 5, pp. 54–59, 2013.*

[9] *Javaid, A. Y., Sun, W., Devabhaktuni, V. K., & Alam, M. (2012). Cyber security threat analysis and modeling of an unmanned aerial vehicle system. 2012 IEEE Conference on Technologies for Homeland Security (HST). doi:10.1109/ths.2012.6459914*

[10] *5 Ways Drones Could Come to Your Rescue." Popular Mechanics. November 14, 2017. Accessed April 24, 2018. https://www.popularmechanics.com/military/g1437/5-ways-dronescould-come-to- your-rescue/.*

[11] *SADEGHI, M., SOLTAN, H., & KHAYYAMBASHI, M. (n.d.). The study of hardware redundancy techniques to provide a fault tolerant system.Retrieved from http://dergi.cumhuriyet.edu.tr/cumuscij/article/view/5000121174*

[12] *Researchers Found They Could Hack Entire Wind Farms. (n.d.). Retrieved April 25, 2018, from https://www.wired.com/story/wind-turbine-hack/*

[13] *Acharya, S.; Dvorkin, Y.; Karri, R. Causative Cyberattacks on Online Learning-Based Automated Demand Response Systems. IEEE Trans. Smart Grid **2021**, 12, 3548–3559. [Google Scholar] [CrossRef]*

[14] *Alazab, M.; Priya, R.M.S.; Parimala, M.; Maddikunta, P.K.R.; Gadekallu, T.R.; Pham, Q.V. Federated Learning for Cybersecurity: Concepts, Challenges, and Future Directions. IEEE Trans. Ind. Inform. **2022**, 18, 3501–3509.*

[15] *Bin Arfaj, B.A.; Mishra, S.; AlShehri, M. Efficacy of Unconventional Penetration Testing Practices. Intell. Autom. Soft Comput. **2022**, 31, 223–239.*

[16] *Kara, I.; Aydos, M. The rise of ransomware: Forensic analysis for windows based ransomware attacks. Expert Syst. Appl. **2022**, 190, 116198.*

[17] *Alqarni, A.A.; Alsharif, N.; Khan, N.A.; Georgieva, L.; Pardade, E.; Alzahrani, M.Y. MNN-XSS: Modular Neural Network Based Approach for XSS Attack Detection. CMC-Comput. Mater. Contin. **2022**, 70, 4075–4085.*

[18] *Khanduzi, R.; Peyghami, M.R.; Sangaiah, A.K. Data envelopment analysis and interdiction median problem*

with fortification for enabling IoT technologies to relieve potential attacks. Future Gener. Comput. Syst. ***2018****, 79, 928–940.*

[19] Li, G.D. Spatiotemporal Dynamics of Ecological Total-Factor Energy Efficiency and Their Drivers in China at the Prefecture Level. Int. J. Environ. Res. Public Health ***2019****, 16, 3480.*

[20] Y. Ganesh, R. Ramya and H. Rajeshwari, "Surveillance Drone for Landmine Detection", Advanced Computing and Commun., pp. 33-38, 2015.

[21] F. Flammini et al., "Towards Automated Drone Surveillance in Railways: State-of-the-Art and Future Directions", Int'l. Conf. Advanced Concepts for Intelligent Vision Systems, pp. 336-48, 2016.

[22] M. Gharibi, R. Boutaba and S.L. Waslander, "Internet of Drones", IEEE Access, vol. 4, pp. 1148-62, 2016.

[23] H.Y. Chao, Y.C. Cao and Y.Q. Chen, "Autopilots for Small Unmanned Aerial Vehicles: A Survey", Int'l. J. Control Automation and Systems, vol. 8, no. 1, pp. 36-44, 2010.