Network Working Group
Internet-Draft
Intended status: Informational
Expires: 7 October 2025

Y. Yang, Ed.
Zhixin Technology Co., Ltd. (Kercore)

5 April 2025

Drone-Based IP over Avian Carriers
draft-zhixin-tech-ip-oac-drone-00

Abstract

This document proposes an experimental protocol, IP over Avian Carriers using Drones (IPoAC-Drone), as an extension to the classic IPoAC (RFC 1149) for modern low-altitude economy applications. It describes how UAVs (Unmanned Aerial Vehicles) can be utilized as network carriers to provide a store-and-forward data transmission model. The document covers protocol design, operational considerations, and potential applications, including emergency communication, rural networking, and disaster recovery.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 7 October 2025.

Copyright Notice

Table of Contents

1. Introduction

IPoAC (RFC 1149) introduced a method for transmitting IP packets via avian carriers (pigeons). Later, RFC 2549 improved its reliability with Quality of Service (QoS). However, the limited payload capacity and unpredictable behavior of biological carriers make them impractical for modern high-speed communication. The advancement of drone technology enables a more reliable and scalable implementation of the IPoAC concept. IPoAC-Drone replaces avian carriers with autonomous UAVs, providing a programmable, high-bandwidth, and predictable alternative.

2. Protocol Overview

2.1. Transmission Mechanism

1. Data packets are encapsulated into storage devices (e.g., SSD, microSD, or encrypted flash drives) attached to UAVs.

2. UAVs operate on pre-defined flight paths to relay packets between nodes.

3. Upon reaching the destination, UAVs transfer the data to ground stations via wireless or physical offloading.

4. Acknowledgments (ACKs) are either relayed back via the same UAVs or an alternative communication channel.

2.2. Addressing & Routing

1. IPv6-Compatible Headers: UAVs are assigned virtual IP addresses for tracking.

2. Routing Protocol: Modified Delay/Disruption Tolerant Network (DTN) approach with a scheduled delivery model.

3. Multi-hop Support: Drones act as relays between ground stations, ensuring wider network coverage.

3. Implementation Considerations

3.1. Drone Specifications

1. Payload Capacity: Sufficient to carry lightweight storage devices.

2. Flight Range: Dependent on battery efficiency and weight distribution.

3. Communication Interface: Wi-Fi, LoRa, 5G, or direct physical offloading.

4. Autonomous Navigation: Pre-defined routes with GPS & AI-based adjustments.

3.2. Security Concerns

1. Data Encryption: AES-256 encryption to prevent unauthorized access.

2. Tamper-Proofing: Secure storage compartments for physical data integrity.

3. Access Control: Only authorized stations can read/write data.

3.3. Network Performance

1. Latency: Variable based on drone speed and travel distance.

2. Packet Loss: Mitigated by redundant UAVs or re-transmission policies.

3. Throughput: Higher than traditional IPoAC, but constrained by drone storage limits.

4. Applications

4.1. Emergency & Disaster Recovery

UAVs can establish a temporary communication network where traditional infrastructure is damaged.

4.2. Rural Internet Deployment

Drones can serve as periodic data carriers between remote villages and urban data centers.

4.3. Military & Secure Data Transport

In high-risk areas, IPoAC-Drone provides a secure and physically isolated communication method.

5. Conclusion

IPoAC-Drone offers a modernized approach to packet transport in areas where conventional networking is unavailable. While latency remains high, its predictable routing, security enhancements, and scalability make it a viable solution for specialized use cases.

Future work includes optimizing flight paths for reduced delays, AI-driven adaptive routing, and hybrid networks integrating UAVs with existing infrastructure.

6. IANA Considerations

This document does not request any changes to IANA registries.

7. Security Considerations

1. Data Integrity: Storage devices must implement cryptographic verification.

2. Physical Interception: Drones must employ anti-tampering mechanisms.

3. Interference & Jamming: UAVs should support frequency-hopping for secure communication.

8. Normative References

[RFC1149] 1149, RFC., "Standard for the transmission of IP datagrams on avian carriers", April 1990.

[RFC2549] 2549, RFC., "IPoAC with QoS", March 1999.

[RFC4838] 4838, RFC., "Delay-Tolerant Networking Architecture", April 2007.

[IEEE2023] 2023, IEEE., "UAV-based Communication Networks: A Survey", 2023.

Author’s Address

YangWeichen (editor)
Zhixin Technology Co., Ltd. (Kercore)
ShiJiazhuang,
China
Email: hbzx@kercore.com.cn
URI: http://www.kercore.com.cn