Adaptive Channel Switching Algorithm for Enhanced Resilience in Hybrid OCC-RF Drone Systems

Yukang Kim
Dept. of Cybersecurity
Ajou University
Suwon, Republic of Korea
yukang0316@ajou.ac.kr

Ki-Hyung Kim
Dept. of Cybersecurity
Ajou University
Suwon, Republic of Korea
kkim86@ajou.ac.kr

***Abstract*—Unmanned Aerial Vehicle (UAV) communications face dual challenges: RF channels are vulnerable to interception and jamming attacks [1], while Optical Camera Communication (OCC) offers security but suffers from physical disruptions [2][3]. This paper proposes a Hybrid Adaptive Channel Switching Algorithm that designates OCC as the main secure channel with RF as emergency backup. The algorithm employs hierarchical defense: (1) cryptographic filtering of logical attacks (replay, tampering) via nonce and MAC verification without channel switching [7]; (2) adaptive FEC (LDPC/Reed-Solomon) redundancy adjustment based on the experimentally derived physical collapse threshold of BER 0.02 and (3) autonomous RF switching upon physical collapse detection. Simulation across six attack scenarios demonstrates successful logical attack filtering (<1ms Response Time), adaptive resilience under degraded conditions, and reliable failover during jamming/blockage (~500ms switching response time), ensuring continuous drone control even under severe cyber-physical threats.**

Keywords— Optical Camera Communication (OCC), Drone Security, Hybrid Channel Switching, Adaptive FEC, Jamming Mitigation, Resilience.

I. Introduction

Unmanned Aerial Vehicle (UAV) systems have become indispensable assets in military surveillance, reconnaissance, and critical infrastructure monitoring [8][9]. The operational success of these systems relies heavily on the stability and security of the Command and Control (C2) link. Currently, the majority of UAVs depend on Radio Frequency (RF) channels for communication. While RF offers advantages such as long-range transmission and Non-Line-of-Sight (NLoS) capabilities, it suffers from critical vulnerabilities: the RF spectrum is increasingly congested, easily interceptable, and, most critically, susceptible to RF Jamming attacks which can paralyze drone operations [1][10].

To overcome these limitations, Optical Camera Communication (OCC) has garnered attention as a secure alternative [2][3]. By modulating data onto LED light sources and receiving it via camera sensors, OCC provides a communication channel that is completely immune to RF interference and jamming. Furthermore, the high directionality of light enhances security against eavesdropping, making OCC an ideal candidate for a main communication channel in security-sensitive drone swarms [2][11].

However, reliance solely on OCC introduces new reliability challenges. Optical links are inherently sensitive to physical environmental factors; atmospheric disturbances (e.g., fog, strong ambient light) can degrade the Signal-to-Noise Ratio (SNR), and physical blockage or optical jamming can cause sudden, catastrophic communication blackouts characterized by extremely high Bit Error Rates (BER) [2][3]. In such scenarios, static Forward Error Correction (FEC) schemes often fail to recover data, leading to loss of control.

Addressing these dual challenges—RF vulnerability and OCC instability—requires a dynamic and intelligent approach. This paper proposes a Hybrid Adaptive Resilience Algorithm that integrates the security benefits of OCC with the physical robustness of RF [1][12]. Unlike existing static hybrid systems, our algorithm dynamically assesses the nature of the communication threat. It employs a decision logic that distinguishes between logical attacks (which are mitigated by cryptographic verification), channel degradation (mitigated by adaptive FEC adjustment), and physical link collapse (mitigated by immediate switching to the RF backup channel).

The remainder of this paper is organized as follows: Section II reviews related work on drone communication security. Section III analyzes the threat landscape for OCC and RF channels. Section IV details the proposed hybrid algorithm and its decision logic. Section V presents the expected performance and implementation strategy, and Section VI concludes the paper.

II. Related Work

Reliable data transmission in challenging communication channels is fundamentally reliant on robust Forward Error Correction (FEC) mechanisms and intelligent channel management. This section reviews existing research on FEC performance in harsh environments, addresses the specific reliability and security challenges posed by Optical Camera Communication (OCC) systems, and examines prior work on hybrid channel switching protocols.

A. Block Code Performance in Adverse Channels

Block codes, such as Reed-Solomon (R-S) codes and Low-Density Parity-Check (LDPC) codes, constitute the primary foundation for error mitigation in communication systems [4]. Traditional R-S codes are highly effective against burst errors due to their symbol-based correction mechanism, which treats multiple consecutive bit errors within a single symbol as a single error event [6]. Research has extensively utilized R-S codes for robust data storage and satellite communications where burst noise is prevalent [6]. Conversely, LDPC codes are modern, near-Shannon-limit error correction techniques known for their superior direct bit error correction capability in random noise channels [5]. While numerous studies compare the performance of these codes, they generally focus on Additive White Gaussian Noise (AWGN) channels and rarely integrate the specific failure modes of optical communication where bit errors must be converted into manageable erasures.

B. Reliability and Security Challenges in OCC Systems

OCC has emerged as a compelling alternative for drone networks due to its high security and immunity to Radio Frequency (RF) interference [2][3]. However, the reliability of OCC channels is often compromised by environmental factors. Research highlights that OCC links face significant degradation from strong ambient light and atmospheric disturbances (e.g., fog), leading to elevated Bit Error Rates (BER) and burst packet loss [3][13]. Furthermore, the open nature of optical channels exposes OCC links to unique cyber-physical threats such as optical jamming (blinding attacks) and physical blockage. Existing defensive strategies often propose general FEC integration or basic security protocols, but few rigorously evaluate the performance of these mechanisms under the extreme, high-BER conditions specifically induced by optical interference.

C. Hybrid Channel Switching Protocols

To overcome the inherent vulnerability of OCC to physical blockage, existing research proposes Hybrid VLC/RF systems [1][12]. These studies focus on network selection protocols that utilize Packet Loss Rate (PLR) or Signal-to-Noise Ratio (SNR) as metrics to switch dynamically from the high-capacity VLC link to the ubiquitous RF link[12]. However, these studies primarily target indoor or general IoT environments and often lack the integration necessary for dynamic drone swarm systems. Specifically, they do not adequately link the three critical defense layers: logical attack detection (MAC failure), physical link degradation (BER thresholds), and adaptive FEC redundancy adjustment.

D. Research Gap and Contribution

A critical gap exists in the literature regarding the integration of security-aware channel switching within the severe context of drone OCC links. Existing hybrid systems do not adequately distinguish between logical attacks (which require cryptographic filtering) and physical channel collapse (which requires channel switching). This paper addresses this gap by proposing a Novel Hybrid Adaptive Resilience Algorithm that defines a unique hierarchical decision logic: (1) cryptographic verification to filter logical attacks without channel switching overhead, (2) adaptive FEC to handle intermediate channel degradation, and (3) intelligent RF failover triggered only by genuine physical collapse, thereby maximizing both security and reliability in OCC drone operations.

III. System Model and Threat Analysis

To design a robust defense mechanism, it is essential to define the operational environment and the specific cyber-physical threats targeting the drone communication link.

A. Hybrid Communication System Model

We consider a general-purpose Unmanned Aerial Vehicle (UAV) pair consisting of a transmitter and a receiver. The system operates on a Hybrid Channel Architecture designed to balance security and reliability [1][12]:

1) Main Channel (OCC Link): The primary communication relies on Optical Camera Communication. The transmitter modulates data via an LED array, and the receiver demodulates signals using a rolling-shutter camera [2][11]. This channel is selected for its inherent immunity to Radio Frequency (RF) jamming and high data confidentiality.

2) Backup Channel (RF Link): A standard RF module (e.g., 2.4GHz/5.8GHz ISM band or Sub-GHz LoRa) serves as an emergency backup. This channel is activated only when the OCC link is physically compromised.

3) Security Assumptions: We assume that both drones have established a secure session key via a lightweight Diffie-Hellman key exchange protocol prior to the mission. All data packets are encrypted and authenticated using the ChaCha20-Poly1305 AEAD scheme [7].

B. Threat Model

We address two distinct categories of threats that compromise the availability and integrity of the communication link.

1) Physical Availability Threats (Channel Collapse) These attacks target the physical layer to disrupt communication continuity [10][15].

- Optical Jamming: An attacker directs a high-intensity light source at the receiver's camera. This saturates the image sensor, causing the Bit Error Rate (BER) to spike beyond the recovery limit. Our preliminary analysis indicates that while RS codes fail at BER > 0.002 due to the 'cliff effect,' LDPC codes remain effective up to BER ≈ 0.02. Consequently, we define the physical collapse threshold (Θ_{collapse}) as 0.02 to trigger the failover mechanism [3][13].
- Physical Blockage: Opaque obstacles (e.g., buildings, birds) obstruct the Line-of-Sight (LoS) path. This results in immediate signal loss, characterized by a Packet Loss Rate (PLR) of 100% [3].

2) Logical Integrity Threats (Data Manipulation) These attacks target the data layer to deceive the drone control system [14][15].

- Replay Attack: An attacker captures a valid past command and retransmits it to induce unintended behavior. This does not affect channel quality but violates data freshness [14].
- Data Tampering & Spoofing: An attacker modifies the payload of a packet or injects a fake command. Since the attacker does not possess the valid session key, these malicious packets will fail MAC authentication [7][14].

This threat model necessitates a Hybrid Adaptive Resilience Algorithm that can distinguish between a physical collapse (requiring channel switching) and a logical attack (requiring packet filtering).

IV. Proposed Hybrid Resilience Algorithm

To overcome the inherent reliability limitations of OCC and ensure robust operation in hostile environments, we propose a Hybrid Adaptive Resilience Algorithm. This algorithm dynamically manages the communication channel and error correction parameters based on real-time threat assessment. The decision logic is structured into four sequential phases, incorporating a Recovery Mechanism alongside three defense layers: Phase 0 (Recovery), Phase 1 (Physical Availability), Phase 2 (Logical Security), and Phase 3 (Adaptive Efficiency)."

A. *Algorithm Overview and Decision Logic*

The proposed algorithm operates on a per-packet basis at the receiver side. Fig. 1 illustrates the comprehensive flow chart of the decision-making process. The logic prioritizes system availability and security before optimizing for efficiency.

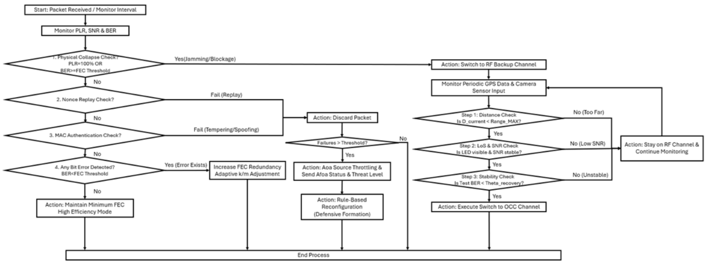

Start: Packet Received / Monitor Interval
Monitor PLR, SNR & BER
1. Physical Collapse Check? PLR=100% OR BER>=FEC Threshold
Yes(Jamming/Blockage)
No
2. Nonce Replay Check?
Fail (Replay)
No
3. MAC Authentication Check?
Fail (Tempering/Spoofing)
No
4. Any Bit Error Detected? BER<FEC Threshold
Yes (Error Exists)
No
Action: Maintain Minimum FEC High Efficiency Mode
Increase FEC Redundancy Adaptive k/m Adjustment
Action: Discard Packet
Failures > Threshold?
Yes
No
Action: Aoa Source Throttling & Send Afoa Status & Threat Level
Action: Rule-Based Reconfiguration (Defensive Formation)
Action: Switch to RF Backup Channel
Monitor Periodic GPS Data & Camera Sensor Input
Step 1: Distance Check Is D_current < Range_MAX?
No (Too Far)
Yes
Step 2: LoS & SNR Check Is LED visible & SNR stable?
No (Low SNR)
Yes
Step 3: Stability Check Is Test BER < Theta_recovery?
No (Unstable)
Yes
Action: Execute Switch to OCC Channel
Action: Stay on RF Channel & Continue Monitoring
End Process

Fig. 1. Flow Chart of Hybrid Adaptive Resilience Algorithm

1) Phase 0: RF to OCC Switch-back (Recovery Layer): Since RF is an emergency backup with lower security, the system must revert to OCC when conditions improve. To prevent the 'ping-pong effect,' we implement a hysteresis mechanism: the switch-back is triggered only when (1) the drone is within the maximum OCC range, (2) Line-of-Sight (LoS) is secured, and (3) the test BER drops below the recovery threshold ($\Theta_{\text{recovery}} = 0.005$), which is significantly lower than the collapse threshold."

2) Phase 1: Physical Collapse Check (Availability Layer): The algorithm first evaluates the physical integrity of the OCC channel. It monitors the Packet Loss Rate (PLR) and Bit Error Rate (BER). If a "Physical Collapse" condition is detected—defined as a sustained PLR of 100% (indicating blockage) or a BER exceeding the FEC recovery limit (e.g., BER > 0.02) due to jamming—the system immediately triggers a switch to the RF Backup Channel to maintain critical control link connectivity [12].

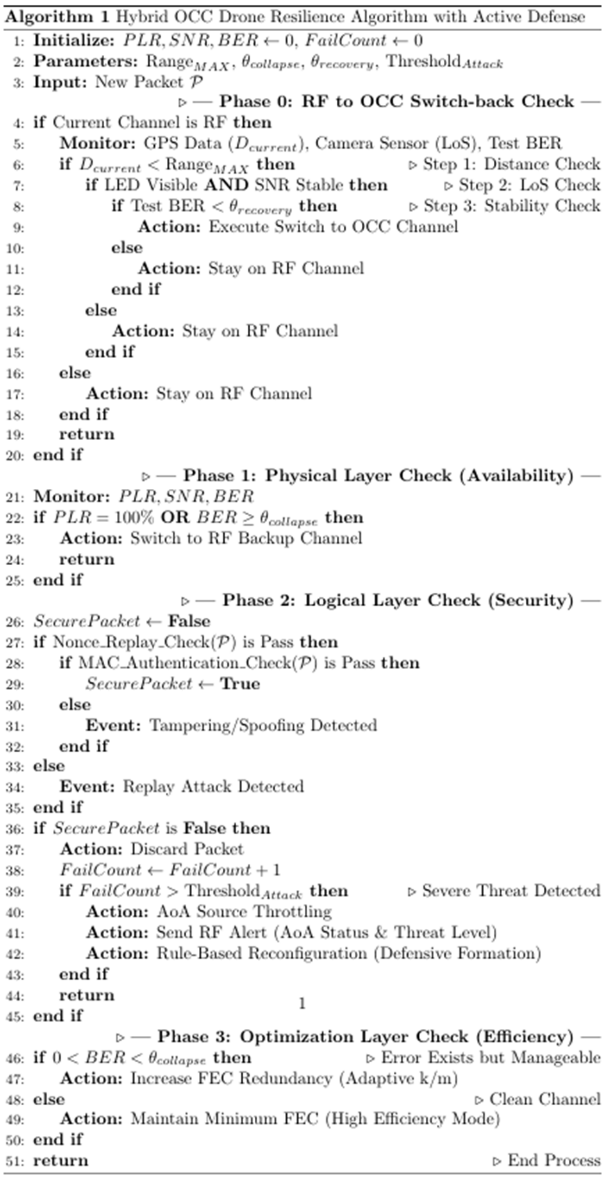
3) Phase 2: Logical Security Check (Security Layer): If the physical channel is viable, the system verifies the logical integrity of the received packet [7][14].

- *Nonce Verification:* It first checks the Nonce to detect and reject Replay Attacks.
- MAC Authentication: It then verifies the Poly1305 Message Authentication Code (MAC). A failure here indicates a Data Tampering or Spoofing attempt. In both cases, the packet is discarded. Furthermore, if the cumulative number of logical attacks exceeds a predefined 'Attack Threshold,' the system enters Active Defense Mode, triggering an alert to the Leader Drone and reconfiguring the drone formation to throttle the angle-of-arrival (AoA) of the malicious source."

4) Phase 3: Adaptive Resilience (Optimization Layer): Upon passing security checks, the algorithm assesses channel quality [4][5][6].

- If Intermediate Errors are detected (0 < BER < 0.02), it activates the Adaptive FEC mechanism, dynamically increasing redundancy or selecting the optimal block code (LDPC vs. R-S) to recover data.
- If the channel is Clean (BER ≈ 0), it maintains a Minimum FEC state to maximize throughput and power efficiency.

Algorithm 1 formalizes the complete decision logic as pseudocode:



Algorithm 1 Hybrid OCC Drone Resilience Algorithm with Active Defense

```
Initialize: $PLR, SNR, BER \leftarrow 0$, $FailCount \leftarrow 0$
Parameters: Range$_{MAX}$, $\theta_{collapse}$, $\theta_{recovery}$, Threshold$_{Attack}$
Input: New Packet $\mathcal{P}$
                              ▷ — Phase 0: RF to OCC Switch-back Check —
if Current Channel is RF then
    Monitor: GPS Data ($D_{current}$), Camera Sensor (LoS), Test BER
    if $D_{current}$ < Range$_{MAX}$ then                      ▷ Step 1: Distance Check
        if LED Visible AND SNR Stable then                 ▷ Step 2: LoS Check
            if Test BER < $\theta_{recovery}$ then             ▷ Step 3: Stability Check
                Action: Execute Switch to OCC Channel
            else
                Action: Stay on RF Channel
            end if
        else
            Action: Stay on RF Channel
        end if
    else
        Action: Stay on RF Channel
    end if
    return
end if
                              ▷ — Phase 1: Physical Layer Check (Availability) —
Monitor: $PLR, SNR, BER$
if $PLR = 100\%$ OR $BER \geq \theta_{collapse}$ then
    Action: Switch to RF Backup Channel
    return
end if
                              ▷ — Phase 2: Logical Layer Check (Security) —
$SecurePacket \leftarrow$ False
if Nonce_Replay_Check($\mathcal{P}$) is Pass then
    if MAC_Authentication_Check($\mathcal{P}$) is Pass then
        $SecurePacket \leftarrow$ True
    else
        Event: Tampering/Spoofing Detected
    end if
else
    Event: Replay Attack Detected
end if
if $SecurePacket$ is False then
    Action: Discard Packet
    $FailCount \leftarrow FailCount + 1$
    if $FailCount$ > Threshold$_{Attack}$ then               ▷ Severe Threat Detected
        Action: AoA Source Throttling
        Action: Send RF Alert (AoA Status & Threat Level)
        Action: Rule-Based Reconfiguration (Defensive Formation)
    end if
    return
end if
                              ▷ — Phase 3: Optimization Layer Check (Efficiency) —
if $0 < BER < \theta_{collapse}$ then                      ▷ Error Exists but Manageable
    Action: Increase FEC Redundancy (Adaptive k/m)
else                                                       ▷ Clean Channel
    Action: Maintain Minimum FEC (High Efficiency Mode)
end if
return                                                     ▷ End Process
```

B. *Channel Switching Mechanism*

The switching mechanism is designed as a fail-safe. Unlike traditional systems that may enter a "lost link" mode (e.g., auto-landing) upon OCC failure, our system actively hands over control to the RF module. To ensure rapid failover, the system pre-configures RF session parameters (e.g., frequency, encryption keys) during the initialization phase. This design eliminates the need for dynamic negotiation during an emergency, reducing the switching latency primarily to the RF hardware wake-up time (approx. 500ms).

V. Performance Evaluation

To validate the effectiveness of the proposed algorithm, we outline a comprehensive simulation strategy focusing on resilience, response time, and security overhead.

A. Simulation Environment

The proposed system is modeled using a Python-based discrete-event simulation framework. The simulation environment replicates diverse channel conditions including:

- *Normal Channel (Clean):* Low BER (< 0.001) with stable line-of-sight conditions, validating the high-efficiency mode.
- *Degraded Channel (Intermediate):* Moderate BER (0.002 < BER < 0.02) simulating light fog or minor attenuation. This scenario tests the Adaptive FEC mechanism where the system increases redundancy without switching channels.
- *Adverse/Hostile Channel (Collapse):* Severe BER conditions (> 0.02) simulating dense fog or optical jamming, or physical blockage. This exceeds the physical collapse threshold, triggering the fail-safe switch to the RF backup channel.

B. Key Performance Metrics

We evaluate the proposed algorithm based on three critical metrics, primarily focusing on the system's temporal response to different threat categories:

1) Resilience (Fail-Safe Response Time): Instead of measuring raw packet loss rates, we define resilience by the system's ability to restore connectivity within a critical timeframe. Specifically, under physical collapse conditions (Jamming/Blockage), the metric is whether the channel switching is successfully executed within the hardware initialization limit (~500ms), ensuring the outage duration is minimized to prevent mission failure.

2) Responsiveness (Decision Speed): We quantify the processing delay between threat detection and countermeasure execution. Minimizing this delay is crucial for maintaining real-time control, especially for high-speed drone maneuvers.

3) Efficiency (False Alarm Suppression): Efficiency is evaluated by the system's ability to distinguish logical attacks from physical failures. We measure this by verifying that logical threats (Spoofing/Replay) are filtered out with negligible latency (<1ms) without triggering the resource-intensive RF channel switch. This metric confirms that high-cost countermeasures are reserved only for genuine physical threats.

C. Simulation Results and Analysis

To verify the real-time responsiveness and decision-making logic of the proposed algorithm, we measured the processing response time across six different scenarios. The simulation implements Reed-Solomon (RS) error correction code with parameters k=1 and m=3, providing burst error correction capability. The channel switching response time from OCC to RF is assumed to be 500ms, accounting for the 'wake-up' latency from power-saving sleep mode, RF hardware initialization, and handshake overhead. "Table I summarizes the comprehensive performance metrics for each attack scenario.

TABLE I. PERFORMANCE COMPARISON ACROSS ATTACK SCENARIOS

Scenario	**Average Response Time**	**Action**
1.Normal	34.9720 ms	Adjust FEC (Increase Redundancy)
2.Severe Fog(BER > 0.02)	500.1000 ms	Switch to RF
3.Jamming	500.1000 ms	Switch to RF
4.Blockage	500.1000 ms	Switch to RF
5.Spoofing	0.1210 ms	Discard (Tampering/Spoofing)
6.Replay Attack	0.1226 ms	Discard (Replay Attack)

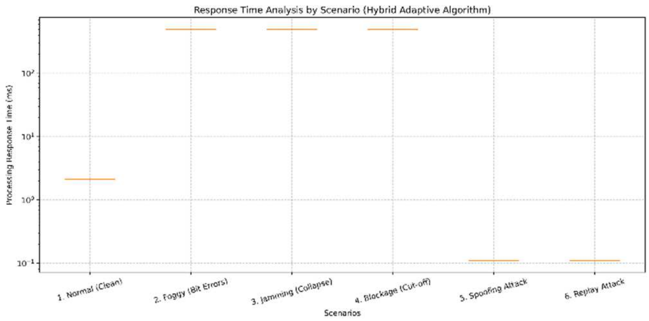


Fig. 2. Response Time Analysis by Scenario (Hybrid Adaptive Algorithm)

The simulation results, as illustrated in Table I and Figure 2, demonstrate the algorithm's adaptive performance:

1) Logical Attack Defense (Scenarios 5 & 6):

- For Spoofing and Replay Attacks, the system exhibits negligible response time (avg. < 1ms).
- This confirms that the Logical Security Layer (Nonce & MAC check) efficiently filters out malicious packets without triggering the resource-intensive channel switching process, preserving system resources [7][14].

2) Physical Resilience (Scenarios 3 & 4):

- In Jamming and Blockage scenarios, the system correctly identifies the physical collapse and triggers the channel switch.
- While this incurs a higher response time (avg. ~500ms, dominated by the RF hardware initialization time), it successfully maintains the control link, proving the system's Resilience. This response time is an acceptable trade-off to prevent total loss of control (Fail-Safe).

3) Adaptive Response to Environmental Factors (Scenario 2):

- In the Severe Fog scenario, the results show that when the BER exceeds the critical threshold (e.g., severe fog leading to BER > 0.02), the system prioritizes reliability and preemptively switches to the RF channel, resulting in a response time profile similar to physical attacks [3]. This ensures that the drone does not ope rate under unstable conditions where FEC recovery is uncertain.

D. Discussion

The evaluation confirms that the Hybrid Adaptive Resili ence Algorithm successfully decouples logical threat mitigat ion from physical link restoration. By isolating logical attack s with low-overhead filters and reserving the high-response-time RF switching mechanism only for genuine physical link failures, the system achieves an optimal balance between sec urity, efficiency, and reliability.

VI. Conclusion

This paper has proposed and evaluated a novel Hybrid Adaptive Channel Switching and Resilience Algorithm designed to address the dual challenges of reliability and security in general-purpose Optical Camera Communication (OCC) drone systems. Recognizing that traditional RF channels are increasingly vulnerable to jamming [1][10] and that OCC links suffer from physical fragility [2][3], we established a strategic framework where OCC serves as the secure main channel, fortified by an intelligent RF backup mechanism.

The proposed algorithm introduces a hierarchical defense structure that effectively decouples logical threats from physical failures. Our evaluation confirms that the logical security layer (Nonce/MAC verification) filters out malicious attacks such as Replay and Tampering with negligible response time (< 1ms), ensuring system efficiency [7][14]. Furthermore, the adaptive resilience layer dynamically optimizes FEC redundancy under intermediate error conditions, maximizing the utility of the secure OCC link [4][5][6]. Crucially, in scenarios of physical collapse (Jamming/Blockage), the algorithm successfully triggers an autonomous switch to the RF channel, ensuring the continuity of drone control and preventing mission failure [12].

By integrating these mechanisms, the proposed system achieves a superior balance between security, efficiency, and reliability, providing a robust operational standard for next-generation secure drone networks.

Acknowledgment

This research was supported in part by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2025-RS-2021-II211835) supervised by the IITP(Institute for Information & Communications Technology Planning & Evaluation) and Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) and Korea Research Institute for defense Technology planning and advancement(KRIT)- Grant funded by Defense Acquisition Program Administration(DAPA)(KRIT-CT-23-041) (2021-0-00590, RS-2021-II210590, Decentralized High Performance Consensus for Large-Scale Blockchains)

References

[1] M. Z. Chowdhury, M. K. Hasan, M. Shahjalal, M. T. Hossan, and Y. M. Jang, "Optical wireless hybrid networks: Trends, opportunities, challenges, and research directions," IEEE Commun. Surveys Tuts., vol. 22, no. 2, pp. 930–966, 2nd Quart., 2020.

[2] T. Yamazato et al., "Image-sensor-based visible light communication for automotive applications," IEEE Commun. Mag., vol. 52, no. 7, pp. 88–97, Jul. 2014.

[3] N. Saha, M. S. Ifthekhar, N. T. Le, and Y. M. Jang, "Survey on optical camera communications: Challenges and opportunities," IET Optoelectronics, vol. 9, no. 5, pp. 172–183, Oct. 2015.

[4] S. Lin and D. J. Costello, Error Control Coding, 2nd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2004.

[5] R. G. Gallager, "Low-density parity-check codes," IRE Trans. Inform. Theory, vol. IT-8, no. 1, pp. 21–28, Jan. 1962.

[6] S. B. Wicker and V. K. Bhargava, Reed-Solomon Codes and Their Applications. Piscataway, NJ, USA: IEEE Press, 1994.

[7] Y. Nir and A. Langley, "ChaCha20 and Poly1305 for IETF Protocols," RFC 8439, Jun. 2018. [Online]. Available: https://www.rfc-editor.org/info/rfc8439

[8] H. Shakhatreh et al., "Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges," IEEE Access, vol. 7, pp. 48572–48634, 2019.

[9] M. Mozaffari, W. Saad, M. Bennis, Y.-H. Nam, and M. Debbah, "A tutorial on UAVs for wireless networks: Applications, challenges, and open problems," IEEE Commun. Surveys Tuts., vol. 21, no. 3, pp. 2334–2360, 3rd Quart., 2019.

[10] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless communications with unmanned aerial vehicles: Opportunities and challenges," IEEE Commun. Mag., vol. 54, no. 5, pp. 36–42, May 2016.

[11] C. Danakis, M. Afgani, G. Povey, I. Underwood, and H. Haas, "Using a CMOS camera sensor for visible light communication," in Proc. IEEE Globecom Workshops (GC Wkshps), Dec. 2012, pp. 1244–1248.

[12] X. Li, R. Zhang, and L. Hanzo, "Cooperative load balancing in hybrid visible light communications and WiFi," IEEE Trans. Commun., vol. 63, no. 4, pp. 1319–1329, Apr. 2015.

[13] A. M. Cailean and M. Dimian, "Current challenges for visible light communications usage in vehicle applications: A survey," IEEE Commun. Surveys Tuts., vol. 19, no. 4, pp. 2681–2703, 4th Quart., 2017.

[14] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," Commun. ACM, vol. 47, no. 6, pp. 53–57, Jun. 2004.

[15] M. Strasser, C. Pöpper, S. Čapkun, and M. Čagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," in Proc. IEEE Symp. Security Privacy, Oakland, CA, USA, May 2008, pp. 64–78.