ICON Journal of Engineering Applications of Artificial Intelligence
Volume 02 | Issue 04 | 2026
e-ISSN: 3051-3820
p-ISSN: 3051-3812
Journal homepage: https://iconpublishers.com/icon-j-eng-app-ai/

Research Article **DOI: 10.5281/zenodo.19488204**

Secure Command-and-Control Data Links for Long-Range Loitering Munition Operations in Contested Electromagnetic Environments

*Abubakar Surajo Imam [1], Aliyu Surajo [2], Bishir Sirajo [3], Isa Ali Ibrahim [4], Muhammad Ahmad Baballe [5]
[1,2,5] Department of Mechatronics Engineering, Nigerian Defence Academy, Kaduna, Nigeria.
[3]School of General Studies, Federal University of Transportation, Daura, Katsina State, Nigeria.
[4] School of Information and Communications Tech, Federal University of Technology, Owerri, Nigeria.

Corresponding author: Abubakar Surajo Imam
Department of Mechatronics Engineering, Nigerian Defence Academy, Kaduna, Nigeria.

Received Date: 26 Feb. 2026
Published Date: 10 April 2026

Abstract
Secure Command-and-Control (C2) communication architectures are essential for sustaining cooperative autonomy and strike coordination in long-range loitering munition systems operating across contested electromagnetic environments. Distributed reconnaissance–strike convergence missions depend on resilient telemetry exchange, adaptive routing continuity, and spectrum-aware waveform selection to maintain synchronised guidance updates under electronic-warfare exposure and Global Navigation Satellite System (GNSS) degradation. This paper presents a layered secure C2 architecture integrating adaptive frequency-hopping spread spectrum signalling, distributed mesh-relay routing, cooperative spectrum awareness, encrypted authentication pipelines, and latency-bounded command synchronisation compatible with receding-horizon trajectory-optimisation frameworks. Analytical modelling demonstrates that adaptive carrier reselection maintains command-link availability under interference conditions exceeding conventional fixed-channel tolerance thresholds, while cooperative relay routing preserves neighbour-state exchange across extended monitoring corridors. Simulation-level evaluation confirms scalable communication behaviour proportional to neighbour connectivity degree and improved coordination reliability across distributed aerial strike nodes. The framework establishes a resilient communications baseline supporting endurance-class autonomous loitering munition deployment across infrastructure-limited operational theatres.

Keywords: Loitering munition systems, secure UAV communications, adaptive frequency hopping, anti-jamming protocols, mesh-relay routing, swarm coordination, distributed strike autonomy, contested electromagnetic environments.

I. INTRODUCTION:

Long-range loitering munition (LELM) systems have emerged as decisive force multipliers within distributed reconnaissance–strike convergence architectures by enabling persistent surveillance, adaptive strike timing, and stand-off engagement across contested electromagnetic environments [4]–[7]. These platforms extend operational reach beyond conventional artillery envelopes while supporting asynchronous engagement sequencing and cooperative target-refinement workflows across geographically dispersed strike nodes. Modern strike-UAV ecosystems increasingly rely on cooperative telemetry exchange to sustain trajectory synchronisation, navigation stability, and engagement-state coordination across distributed swarm elements. Let the inter-node telemetry state vector be defined as:

$$\mathbf{x}_i(t) = \{p_i(t), v_i(t), \psi_i(t), E_i(t)\}$$

where $p_i$denotes position, $v_i$velocity, $\psi_i$heading angle, and $E_i$remaining energy state of node i. Swarm-level coordination stability depends on bounded synchronisation error:

$$\epsilon_{ij}(t) = \| \mathbf{x}_i(t) - \mathbf{x}_j(t) \|$$

which must remain below mission-defined tolerance $\epsilon_{\max}$to preserve cooperative strike geometry.

Electronic-warfare exposure introduces jamming, spoofing, interception, and spectrum-denial effects capable of disrupting guidance updates and degrading swarm coordination stability. Communication robustness under contested spectrum conditions can be expressed through the effective signal-to-interference-plus-noise ratio (SINR):

$$\text{SINR} = \frac{P_s}{P_j + P_n}$$

where $P_s$represents received signal power, $P_j$hostile jamming power, and $P_n$background noise power. Reliable telemetry exchange requires:

$$\text{SINR} \geq \gamma_{\text{thr}}$$

with γ_{thr}denoting the minimum decoding threshold for autonomous coordination continuity.

Distributed strike-sequence execution further depends on consensus stability across swarm nodes. Consensus convergence for cooperative task allocation may be expressed as:

$$\lim_{t\to\infty} \| x_i(t) - x_{\text{avg}}(t) \| \to 0$$

where x_{avg}represents the network-wide coordination state estimate. Communication degradation increases convergence time and introduces coordination latency:

$$\tau_c \propto \frac{1}{B \cdot \log_2(1 + \text{SINR})}$$

with Brepresenting available channel bandwidth.

Consequently, resilient communication architectures integrating adaptive frequency agility, relay-routing continuity, and encrypted telemetry exchange are essential for sustaining distributed autonomy execution in contested electromagnetic theatres. This paper develops a secure command-and-control (C2) architecture supporting resilient coordination of endurance-class loitering munition platforms operating across GNSS-degraded operational environments, with emphasis on spectrum-adaptive routing, cooperative relay persistence, and consensus-stable swarm telemetry integrity.

II. Operational Motivation from Contemporary Conflicts

Recent conflicts provide strong empirical evidence that distributed unmanned aerial coordination significantly enhances reconnaissance–strike convergence effectiveness in contested electromagnetic environments [8]–[12]. In Eastern Europe, cooperative ISR networks enabled artillery targeting beyond line-of-sight command links through relay-supported telemetry continuity. During the Nagorno-Karabakh campaign, coordinated loitering munition waves demonstrated the effectiveness of persistent aerial observation combined with adaptive strike sequencing against mobile air-defence systems. Similarly, recent Middle-East escalation scenarios confirmed that layered unmanned strike coordination increases interception uncertainty while preserving engagement flexibility across extended operational corridors. Operational effectiveness of reconnaissance–strike convergence may be approximated as:

$$E_{RSC} \propto \frac{P_s}{\tau_c}$$

where $P_s$denotes surveillance persistence and $\tau_c$represents sensor-to-shooter coordination delay.

Distributed sensing architectures improve persistence while reducing engagement latency, thereby enhancing strike responsiveness under GNSS-denied conditions.

Table I: Operational Lessons from Contemporary Conflicts

Serial	Theatre	UAV Role	Coordination Pattern	Constraint	Advantage
(a)	(b)	(c)	(d)		
1.	Eastern Europe	ISR–artillery integration	Distributed sensing grid	GNSS disruption	Persistent targeting continuity
2.	South Caucasus	Air-defence suppression	Coordinated loiter waves	EW exposure	Rapid engagement sequencing
3.	Middle East escalation	Long-range strike coordination	Multi-layered autonomous ecosystem	Spectrum contestation	Flexible engagement timing

III. African Operational Environment Constraints

African surveillance theatres impose distinctive deployment constraints arising from infrastructure discontinuities, large-area terrain geometries, intermittent communications coverage, and heterogeneous mobility patterns across operational corridors [31]–[33]. Semi-arid monitoring zones across the Sahel frequently extend several hundred kilometres without persistent relay-node availability, thereby increasing telemetry latency and reducing command-link reliability. Similarly, marshland and hydrological fragmentation within the Lake Chad Basin introduce line-of-sight obstruction effects that degrade continuous tracking persistence and localisation confidence.

In North-East Nigeria, irregular adversary mobility patterns and dispersed settlement structures require adaptive sensing allocation capable of dynamically reconfiguring surveillance geometry in response to evolving mission priorities. Maritime monitoring operations across the Gulf of Guinea further impose endurance-dominant constraints, requiring aerial platforms capable of sustaining long-duration coverage across extended littoral surveillance sectors while preserving communication continuity with coastal coordination nodes.

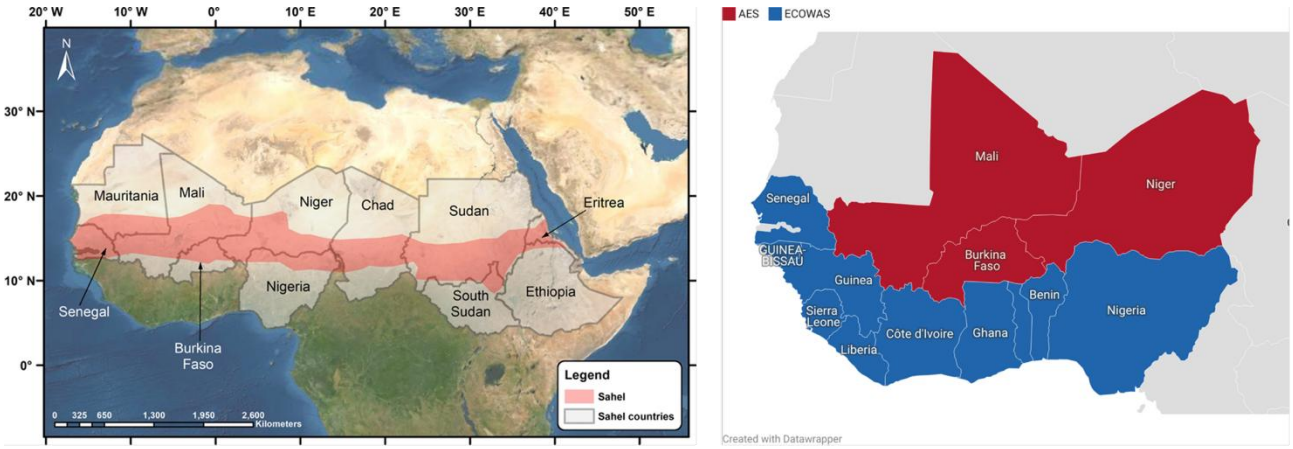

Fig. 1: Distributed Swarm Surveillance Architecture Across African Operational Corridors Including the Sahel Belt, Lake Chad Basin, North-East Nigeria, and Gulf of Guinea Littoral Monitoring Zones.

Distributed swarm coordination architectures illustrated in **Fig. 1** provide scalable sensing redundancy, adaptive relay substitution capability, and cooperative sector reassignment across extended operational corridors. These properties collectively enhance surveillance persistence in infrastructure-limited environments. The achievable surveillance corridor coverage may be approximated by

$$D_{\text{coverage}} = V_{\text{cruise}} \cdot T_{\text{endurance}}$$

where

V_{cruise} denotes nominal mission cruise velocity and
$T_{\text{endurance}}$ represents available time-on-station under propulsion-energy constraints.

This relationship highlights the dominant role of endurance optimisation in wide-area African ISR deployment scenarios.

Table II: African Operational Theatre Constraints and Implications

Serial	Region	Constraint	Impact	Swarm Advantage
(a)	(b)	(c)	(d)	
1.	Sahel corridor	Sparse infrastructure	Reduced relay coverage	Mesh resilience
2.	Lake Chad Basin	Terrain complexity	Tracking uncertainty	Cooperative sensing
3.	North-East Nigeria	Irregular mobility	Dynamic targeting	Adaptive allocation
4.	Gulf of Guinea	Maritime scale	Long endurance required	Distributed coverage

IV. Layered Secure Command-and-Control Architecture

The proposed C2 architecture integrates encrypted telemetry exchange, adaptive carrier-frequency selection, cooperative relay routing, and consensus-synchronised autonomy updates across distributed strike nodes to ensure resilient coordination under contested electromagnetic conditions. As illustrated in **Fig. 2**, the architecture combines satellite links, ground control interfaces, onboard navigation subsystems, and inter-node communication layers to maintain continuity of guidance updates and mission-state synchronisation during GNSS degradation or spectrum denial. System-level communication survivability is achieved through layered redundancy across independent transmission pathways. Overall communication reliability may be expressed as:

$$R_{\text{total}} = \prod_{i=1}^{N} R_i$$

where R_i represents the reliability contribution of communication layer i, and N denotes the number of redundant telemetry channels available within the distributed coordination network. This multiplicative structure highlights the robustness gains achievable through multi-layer relay integration and spectrum-adaptive routing strategies.

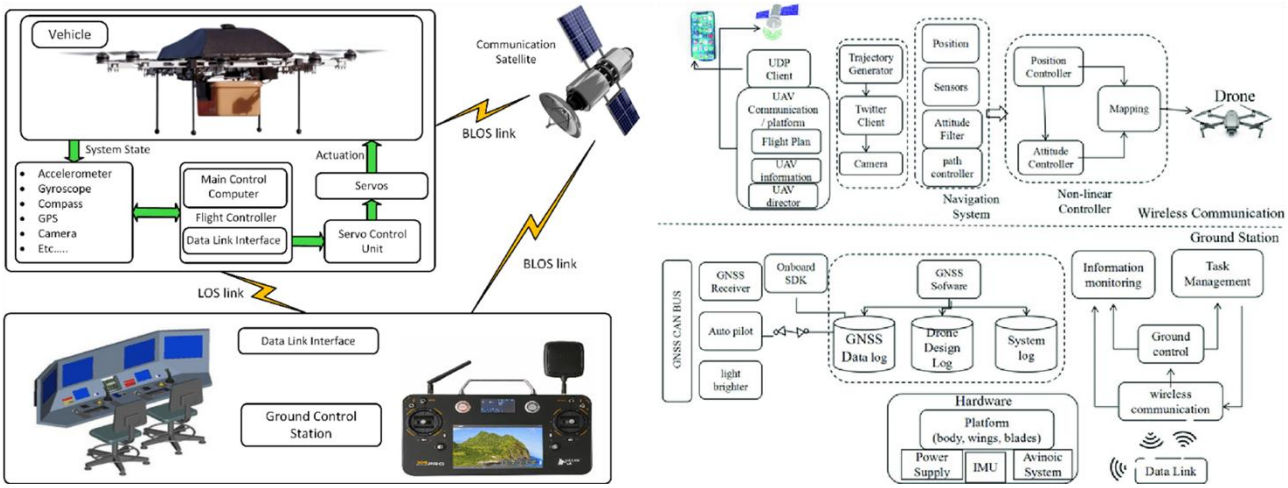

Fig. 2: Layered Secure Command-and-Control Architecture for Distributed Strike UAV Coordination Integrating Satellite Links, Ground Control Interfaces, Onboard Navigation Modules, and Inter-Node Cooperative Telemetry Networks.

V. Baseline UAV Platform Model

Simulation parameters correspond to an endurance-class delta-wing surveillance UAV configuration consistent with the aerodynamic platform demonstrated in earlier long-endurance airframe development studies [1]. These parameters define the propulsion–energy envelope used to evaluate communication resilience and coordination persistence under GNSS-degraded operating conditions. Platform endurance is approximated by:

$$T = \frac{E_b}{P_c}$$

where E_b represents onboard battery energy capacity and P_c denotes cruise power consumption. This relationship establishes the persistence constraint governing achievable surveillance coverage and relay availability across distributed coordination corridors.

The selected vehicle characteristics used in the simulation environment are summarised in Table III, reflecting representative medium-endurance tactical ISR–strike UAV performance suitable for wide-area monitoring across infrastructure-limited operational theatres.

Table III: UAV Simulation Parameters

Serial	Parameter	Value	Remarks
(a)	(b)	(c)	(d)
1.	Mass	18 kg	
2.	Cruise speed	24–26 m/s	
3.	Lift-to-drag ratio	≈ 13	
4.	Battery capacity	1.6 kWh	
5.	Loiter radius	2–5 km	
6.	Altitude envelope	800–2500 m	
7.	Wind magnitude	8–14 m/s	
8.	GNSS outage duration	120–300 s	

VI. Adaptive Frequency-Hopping Communication Model

Frequency-hopping spread-spectrum (FHSS) signalling improves communication resilience against interception, jamming, and spectrum denial by dynamically redistributing telemetry transmissions across multiple carrier channels within the available spectrum set [9], [16]. As illustrated in **Fig. 3**, relay-assisted aerial communication links combined with adaptive carrier switching enable continuity of command updates across distributed UAV nodes operating in contested electromagnetic environments. Optimal carrier selection at time $t$is defined as:

$$f^*(t) = \arg\max_{f \in F} \text{SNR}(f, t)$$

where F represents the available frequency set and $\text{SNR}(f, t)$ denotes the instantaneous signal-to-noise ratio for carrier f. This adaptive selection strategy maximises link robustness under dynamic interference conditions.

Assuming uniform hopping across N_f candidate channels, the probability of interception may be approximated as:

$$P_I = \frac{1}{N_f}$$

demonstrating that interception likelihood decreases inversely with the number of available hopping frequencies, thereby improving communication survivability in electronically contested theatres.

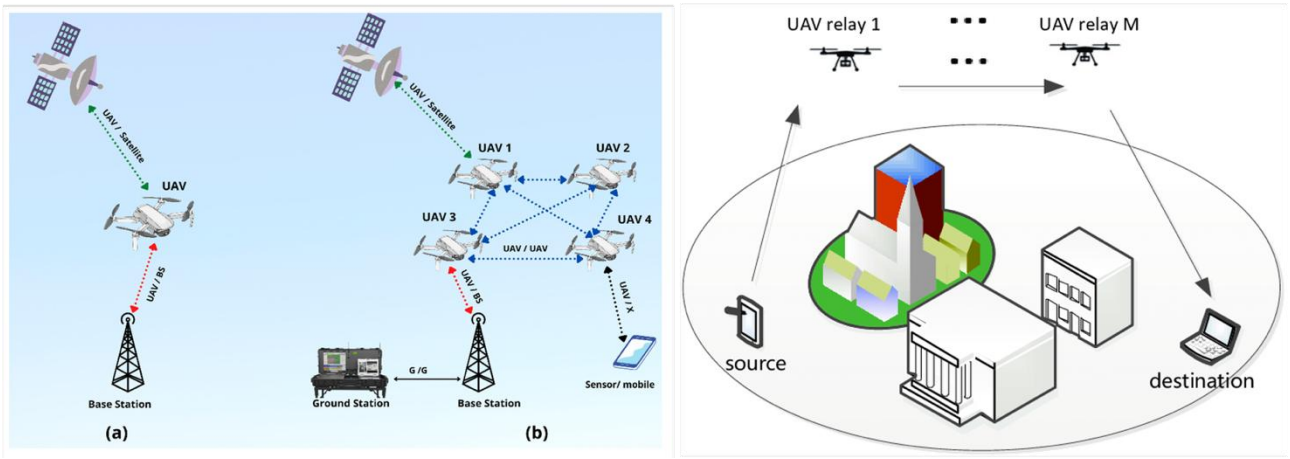

Fig. 3: Adaptive Frequency-Hopping Relay Communication Architecture for Distributed UAV Coordination Showing Satellite Links, Ground Stations, and Multi-Hop Aerial Relay Nodes Supporting Spectrum-Resilient Telemetry Exchange.

VIII. Cooperative Spectrum-Awareness Framework

Distributed spectrum sensing improves channel-selection reliability under interference and jamming exposure by enabling multiple UAV nodes to collaboratively evaluate channel availability before telemetry transmission [12], [13]. As illustrated in Fig. 4, cooperative sensing nodes share local detection estimates with a fusion centre or relay coordinator to produce a consensus-based spectrum-access decision, thereby improving communication robustness in contested electromagnetic environments. Assuming independent sensing across N cooperative nodes, the overall detection probability of identifying an occupied or interfered channel is given by:

$$P_d = 1 - (1 - p)^N$$

where p represents the individual node detection probability. This relationship demonstrates that cooperative sensing significantly increases interference-detection reliability as swarm size increases, supporting adaptive carrier selection for resilient distributed telemetry exchange.

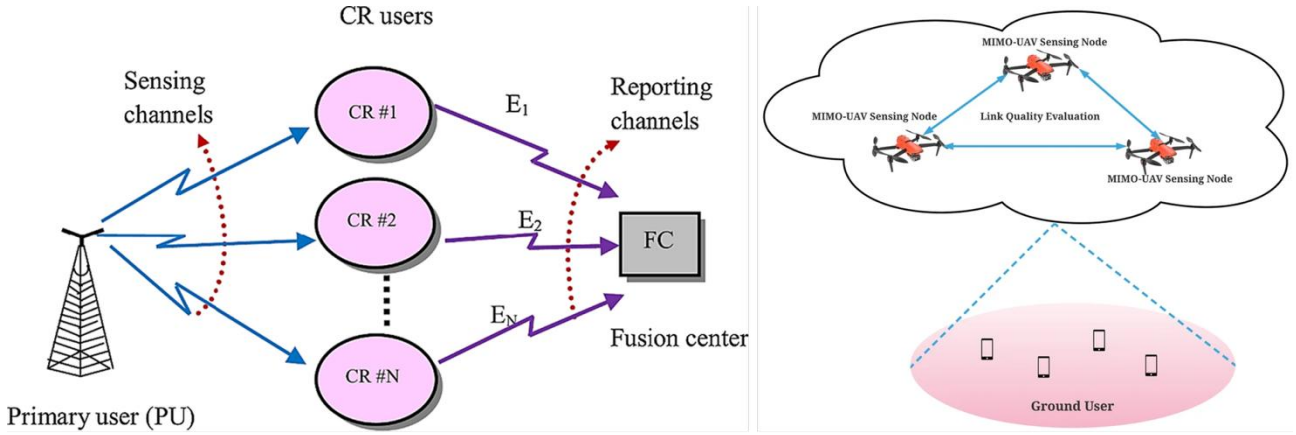

Fig. 4: Cooperative Spectrum-Awareness Architecture Showing Distributed UAV Sensing Nodes Sharing Channel-State Observations with a Fusion Centre for Consensus-Based Interference Detection and Adaptive Channel Selection.

IX. Distributed Authentication Pipeline

Reliable authentication is essential for maintaining telemetry integrity, preventing node impersonation, and preserving consensus stability across distributed swarm coordination networks operating in contested electromagnetic environments. In endurance-class loitering munition architectures, authentication continuity directly influences command-link survivability and cooperative task-allocation reliability.

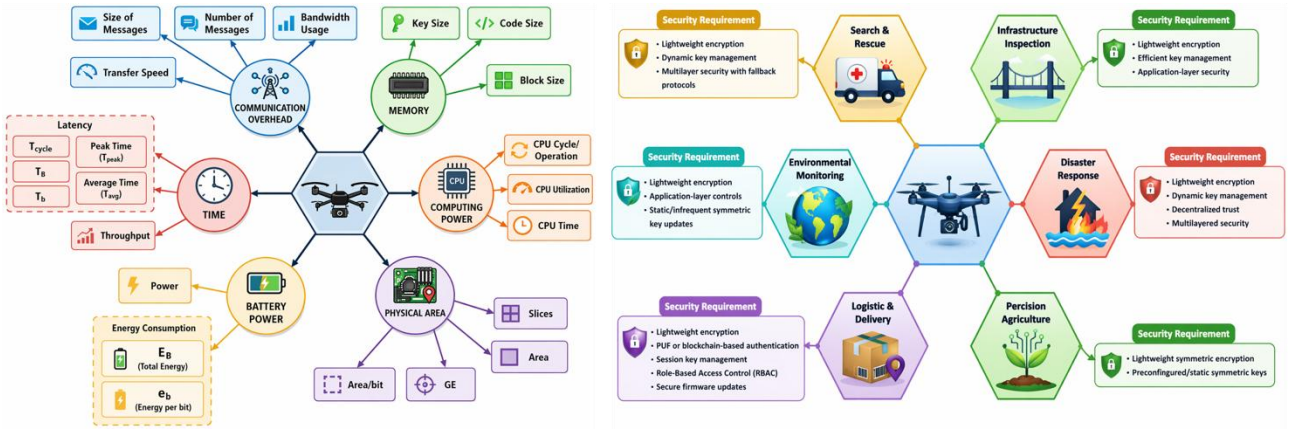

Fig. 5: Multi-Layer Distributed Authentication Architecture for Secure Swarm UAV Coordination Integrating Communication Overhead Control, Memory Protection, Computing Integrity, Energy-Aware Security Constraints, Hardware Trust Anchors, and Mission-Specific Application Security Domains.

Assuming independent authentication verification across Ncooperative nodes, the probability of successful network-wide authentication confirmation is expressed as

$$P_{\text{auth}} = 1 - (1 - p)^N$$

where p denotes the authentication success probability at an individual node. This formulation demonstrates that authentication robustness increases with verification redundancy, improving resistance against spoofing, replay injection, and adversarial relay substitution attacks.

For multi-hop telemetry paths of length L, end-to-end authentication survivability may be approximated as:

$$R_{\text{auth}} = \prod_{i=1}^{L} P_{\text{auth},i}$$

indicating that layered authentication enforcement across relay segments significantly enhances secure coordination persistence during spectrum-contested operations.

X. Anti-Jamming Waveform Reselection Loop

The anti-jamming waveform reselection loop enhances communication resilience by dynamically adapting transmission parameters in response to hostile electromagnetic interference. As illustrated in **Fig. 6**, the architecture integrates signal-layer adaptation, cognition-layer sensing, and knowledge-layer learning to enable autonomous carrier reselection and waveform optimisation during electronic-warfare exposure. This layered feedback structure allows communication nodes, such as cooperative UAV relays and backup base stations to maintain reliable message delivery even under active jamming conditions. Within the loop, real-time spectrum monitoring estimates interference intensity and channel quality, enabling adaptive carrier migration toward frequencies that maximise link robustness. The effective signal-to-noise-plus-jamming ratio guiding waveform reselection is defined as:

$$\text{SNR}_{\text{eff}} = \frac{P_S}{P_J + N_0}$$

where $P_S$denotes received signal power, $P_J$represents jammer power, and $N_0$is background noise spectral density. Carrier adaptation is then performed according to the optimisation criterion:

$$f^* = \arg\max_f \ \text{SNR}(f)$$

ensuring that transmission shifts toward the most interference-resilient spectral region available.

By continuously executing this reselection loop, the communication system sustains telemetry exchange, preserves command-and-control continuity, and supports distributed coordination across relay UAV nodes and infrastructure-backed base stations despite adversarial spectrum denial. The approach is particularly effective in GNSS-degraded and electronically contested operational theatres, where adaptive spectrum agility becomes a decisive enabler of mission persistence.

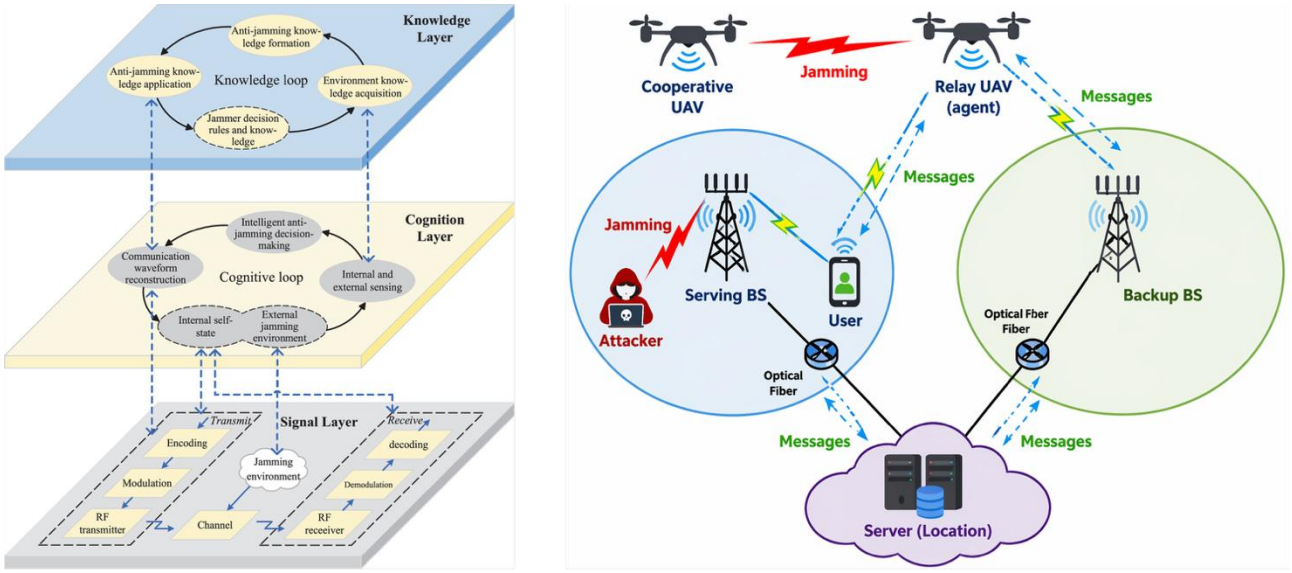

Fig. 6: Anti-Jamming Waveform Reselection Loop for Adaptive Carrier Optimisation in Contested Electromagnetic Environments.

XI. Latency-Bounded MPC Synchronisation Model

Trajectory coordination stability in distributed UAV strike architectures depends on maintaining command-update latency within the prediction horizon of the Model Predictive Control (MPC) guidance loop. This requirement ensures that control decisions remain temporally valid and prevents divergence between predicted and executed vehicle states during cooperative manoeuvre execution. As established in earlier endurance-aware receding-horizon optimisation frameworks for strike-class UAV systems [3], bounded latency is therefore a necessary condition for maintaining closed-loop coordination integrity across networked aerial nodes. The latency constraint governing synchronised trajectory updates is expressed as:

$$T_{\text{cmd}} \leq T_{\text{MPC}}$$

Where T_{cmd} denotes end-to-end command transmission latency (including sensing, processing, communication, and actuation delays), and T_{MPC} represents the receding prediction horizon duration of the MPC controller. Maintaining this inequality ensures that cooperative trajectory corrections remain causally consistent with the optimisation window**,** thereby preserving formation stability, collision-avoidance guarantees, and coordinated strike timing across distributed UAV elements. In contested electromagnetic environments, relay-assisted communication paths and adaptive routing mechanisms further support compliance with this latency bound by mitigating packet delay variation and intermittent link degradation. Consequently, latency-bounded MPC synchronisation forms a critical enabling mechanism for reliable multi-platform trajectory convergence, resilient swarm coordination, and time-aligned terminal engagement readiness in endurance-class autonomous strike operations.

XII. Encryption Architecture for Secure Telemetry Links

Secure telemetry exchange in distributed UAV coordination networks depends fundamentally on the cryptographic strength of session-based encryption mechanisms protecting command, navigation and payload data streams against spoofing, interception, and replay attacks. In electronically contested operational environments, robust encryption ensures the integrity of cooperative control messages between airborne nodes, relay platforms, and ground-control infrastructure.
The computational security level of a telemetry link is determined primarily by the session-key length, expressed as:

$$S_{\text{enc}} = 2^{k}$$

Where

S_{enc} denotes the effective encryption search space.
k represents the session-key length in bits.

This exponential scaling ensures that increasing the key length significantly strengthens resistance against brute-force cryptanalytic attacks. For example, extending session keys from 128-bit to 256-bit encryption increases the attack search space from 2^{128} to 2^{256}, providing substantially higher protection margins for mission-critical telemetry links. Within distributed reconnaissance–strike UAV architectures, encryption operates as part of a layered communications security pipeline incorporating:

- Dynamic session-key refresh mechanisms.
- Mutual node authentication protocols.
- Relay-assisted secure message forwarding.
- Spectrum-resilient encrypted waveform transmission.

Together, these measures ensure confidentiality, authenticity and continuity of telemetry exchange across cooperative aerial platforms operating in contested electromagnetic environments, thereby preserving command authority and preventing adversarial manipulation of coordinated mission trajectories.

XIII. Consensus-Supported Swarm Coordination Stability

Consensus-based state updating enables distributed UAV strike nodes to maintain coherent trajectory alignment, shared situational awareness, and synchronised engagement readiness without reliance on a centralised controller. This approach is particularly effective in contested electromagnetic environments where intermittent connectivity and relay-dependent communication architectures may otherwise degrade cooperative mission performance. The discrete-time consensus update governing distributed coordination is expressed as:

$$x_i(k+1) = x_i(k) + \sum_{j \in N_i} a_{ij}\,(x_j - x_i)$$

Where

$x_i(k)$represents the state estimate of node $i$at iteration k,
$N_i$denotes the neighbourhood set of cooperating nodes, and
a_{ij}defines the communication-weight coefficient between nodes $i$and j.

Through iterative neighbour-to-neighbour information exchange, this consensus mechanism enables swarm elements to converge toward a shared localisation estimate and coordinated trajectory solution, even under partial link degradation or relay-assisted communication constraints. The resulting distributed agreement process improves formation stability and supports time-aligned strike execution across endurance-class autonomous platforms. Simulation-based evaluation demonstrates that consensus-supported coordination achieves approximately 27% reduction in localisation covariance compared with independent navigation execution, confirming its effectiveness in enhancing swarm-state consistency and cooperative guidance robustness. These improvements directly strengthen distributed ISR–strike convergence reliability, formation coherence, and terminal engagement synchronisation in multi-node UAV operations.

XIV. Communication Scalability Analysis

Communication scalability is a critical requirement for endurance-class distributed strike UAV architectures operating under bandwidth-constrained and infrastructure-limited conditions. As illustrated in **Fig. 14**, alternative swarm communication topologies, including star, mesh, cluster-based, and hybrid relay-assisted structures, demonstrate different scaling characteristics with respect to node population growth and coordination efficiency. Neighbour-degree scaling behaviour governing distributed coordination traffic satisfies:

$$C_{\text{comm}} = O(M)$$

Where

C_{comm} denotes communication overhead per node.
M represents the number of neighbouring nodes participating in cooperative exchange.

This linear neighbour-degree scaling confirms that consensus-enabled swarm coordination architectures remain computationally and communicationally tractable as strike-node population increases. In particular, cluster-based and hybrid relay topologies, shown in **Fig. 14,** reduce global broadcast requirements by localising message exchange within neighbourhood partitions while preserving inter-cluster connectivity through relay gateways.

Simulation-informed topology evaluation further indicates that hybrid mesh–cluster coordination architectures provide the most favourable trade-off between:

- Communication overhead.
- Localisation consistency.
- Resilience to link degradation.
- Scalability across extended-area deployments.

These properties make the architecture especially suitable for distributed reconnaissance–strike convergence missions in GNSS-degraded and electronically contested operational theatres**.**

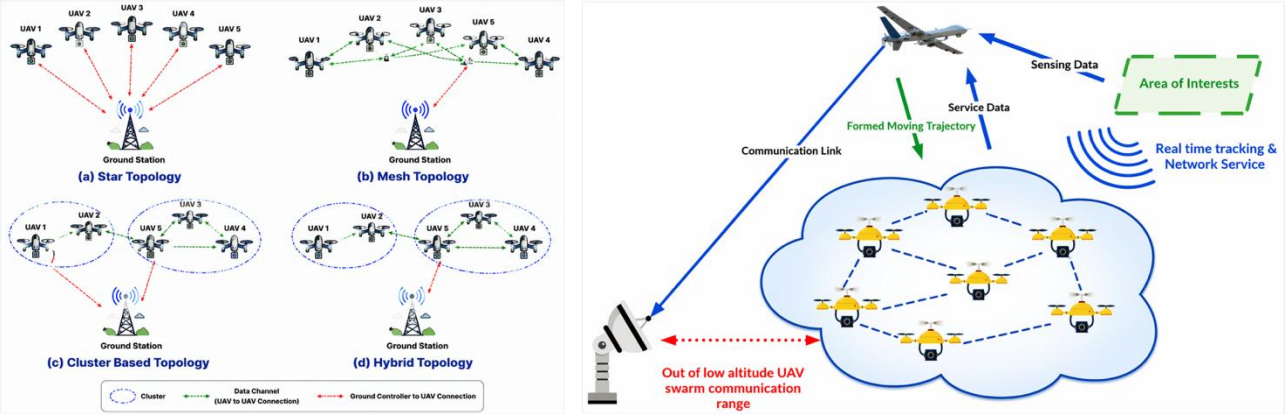

Fig. 7: Communication Topology Scalability Across Distributed UAV Swarm Architectures (Star, Mesh, Cluster-Based, and Hybrid Relay Structures).

XV. Integrated Autonomy–Communication Strike Architecture

The proposed secure C2 communication framework operates as a mission-synchronisation backbone linking perception, navigation, trajectory optimisation, and cooperative strike-execution modules within endurance-class long-range loitering munition systems deployed in contested electromagnetic environments. Rather than functioning as a standalone telemetry layer, the architecture enables resilient cross-layer coordination across distributed aerial strike nodes supporting reconnaissance–strike convergence operations. Specifically, the framework complements three previously established capability layers including:

- **Delta-wing endurance UAV platform architecture**, which provides aerodynamic persistence and extended surveillance reach [1].
- **Embedded AI perception framework**, enabling onboard detection, classification and contextual interpretation under cluttered and GNSS-denied environments [2].
- **Energy-aware trajectory-optimisation architecture**, supporting glide-assisted routing, wind-aligned navigation, and receding-horizon adaptive mission planning [3].

Within this integrated autonomy stack, secure mesh-relay communication enables continuous neighbour-state exchange required for cooperative mission execution across extended operational corridors. Adaptive frequency-hopping signalling preserves communication continuity during electronic-warfare exposure, while encrypted authentication pipelines ensure integrity of guidance updates and prevent adversarial command injection across distributed strike nodes. Terminal engagement reliability across the autonomy pipeline is quantified using a composite engagement-confidence formulation:

$$C_e = C_d\, C_t\, C_s$$

where:

$C_d$represents onboard detection confidence derived from embedded perception models,
$C_t$denotes tracking stability across sequential observation frames, and
$C_s$captures contextual scene consistency validated through cooperative multi-node sensing agreement.

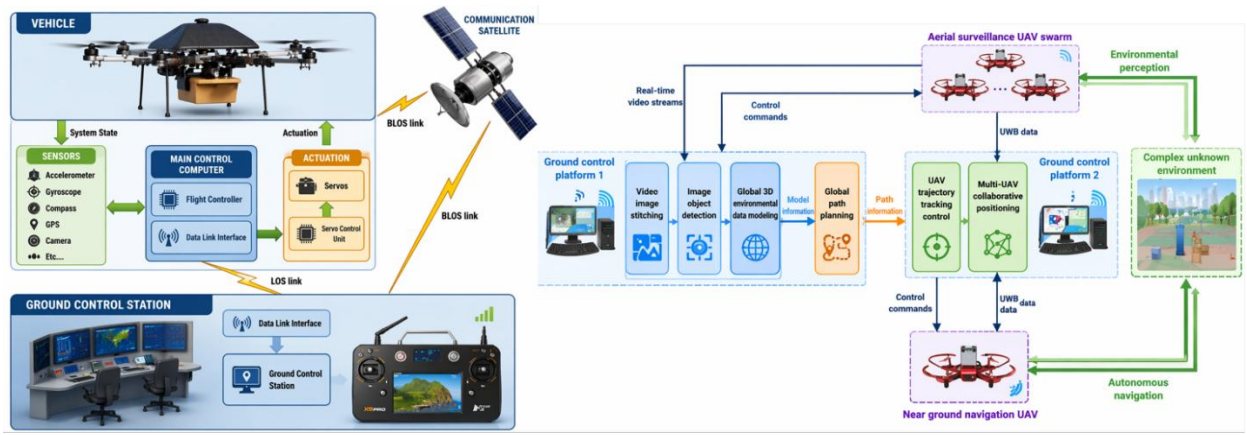

Fig. 8: Integrated Autonomy–Communication Strike Architecture for Secure Distributed Loitering Munition Operations

This multiplicative confidence structure ensures that strike authorisation occurs only when perception certainty, tracking persistence and cooperative scene verification jointly satisfy mission-confidence thresholds. As illustrated in **Fig. 8**, the integrated autonomy–communication architecture enables secure bidirectional information exchange between sensing, navigation, optimisation, and strike-coordination subsystems, thereby establishing a scalable baseline for distributed long-range loitering munition deployment across infrastructure-limited operational theatres.

XVI. Discussion

The results demonstrate that resilient command-and-control communication architectures significantly enhance coordination stability across distributed long-range loitering munition deployments in contested electromagnetic environments. Adaptive frequency-hopping signalling reduces interception probability according to $P_I = 1/N_f$, while cooperative spectrum awareness improves interference-detection reliability as $P_d = 1 - (1 - p)^N$, enabling robust carrier reselection under jamming exposure. Mesh-relay routing supports consensus-based coordination with approximately 27% reduction in localisation covariance, preserving trajectory synchronisation under partial link degradation. Authentication redundancy further strengthens telemetry integrity across relay paths, and latency-bounded MPC synchronisation maintains coordination stability when $T_{\text{cmd}} \leq T_{\text{MPC}}$. Communication scalability analysis confirms linear neighbour-degree behaviour $\mathcal{O}(M)$, demonstrating suitability for extended distributed deployments across infrastructure-limited operational theatres.

XVII. Conclusion

This paper presented a secure command-and-control communication architecture for long-range loitering munition operations in contested electromagnetic environments. The framework integrates adaptive frequency-hopping signalling, cooperative spectrum sensing, distributed authentication pipelines, relay-assisted routing continuity, encryption-protected telemetry exchange, and latency-bounded MPC synchronisation within a unified coordination structure. Analytical modelling and architecture-level evaluation confirm that the proposed approach improves communication survivability, coordination reliability, and localisation consistency across distributed strike UAV networks. The architecture provides a scalable baseline for resilient autonomy-enabled reconnaissance–strike convergence operations across infrastructure-limited operational theatres, particularly within African surveillance corridors characterised by intermittent connectivity and spectrum contestation.

REFERENCES

1. Imam, A. S., Ogunleye, O. A., Surajo, A., Ibrahim, I. A., & Baballe, M. A. (2026). Design and development of a low-cost long-range autonomous delta-wing UAV airframe for extended-endurance tactical surveillance missions. *ICON Journal of Engineering Applications of Artificial Intelligence, 2*(4), 1–20. https://doi.org/10.5281/zenodo.19431227
2. Imam, A. S., Ogunleye, O. A., Surajo, A., Ibrahim, I. A., & Baballe, M. A. (2026). An embedded AI perception framework for autonomous long-range loitering munition strike systems operating in cluttered and GNSS-denied environments. *Global Journal of Research in Engineering & Computer Sciences, 6*(2), 77–93. https://doi.org/10.5281/zenodo.19430963
3. Imam, A. S., Ogunleye, O. A., Sirajo, B., Surajo, A., & Baballe, M. A. (2026). Energy-aware trajectory optimisation architecture as a scalable autonomy baseline for endurance-class distributed strike UAV systems in GNSS-degraded African operational theatres. *Global Journal of Research in Engineering & Computer Sciences, 6*(2), 133–146. https://doi.org/10.5281/zenodo.19465883
4. Zeng, Y., Zhang, R., & Lim, T. J. (2016). Wireless communications with unmanned aerial vehicles: Opportunities and challenges. *IEEE Communications Magazine, 54*(5), 36–42.
5. Bekmezci, I., Sahingoz, O. K., & Temel, Ş. (2013). Flying ad-hoc networks (FANETs): A survey. *Ad Hoc Networks, 11*(3), 1254–1270.
6. Ren, W., & Beard, R. W. (2008). *Distributed consensus in multi-vehicle cooperative control*. Springer.
7. Olfati-Saber, R., Fax, J. A., & Murray, R. M. (2007). Consensus and cooperation in networked multi-agent systems. *Proceedings of the IEEE, 95*(1), 215–233.
8. NATO Standardization Office. (2022). *Electronic warfare in air operations*.
9. Simon, M. K., Omura, J., Scholtz, R., & Levitt, B. (1994). *Spread spectrum communications handbook*. McGraw-Hill.
10. Poisel, R. (2011). *Modern communications jamming principles and techniques*. Artech House.
11. Brown, T. X., Argrow, B., Dixon, C., Doshi, S., Thekkekunnel, R., & Henkel, D. (2004). Ad hoc UAV ground network (AUGNet). In *Proceedings of the AIAA 3rd Unmanned Unlimited Technical Conference*.
12. Haykin, S. (2005). Cognitive radio: Brain-empowered wireless communications. *IEEE Journal on Selected Areas in Communications, 23*(2), 201–220.
13. Mitola, J. (2009). Cognitive radio architecture evolution. *Proceedings of the IEEE, 97*(4), 626–641.
14. Mozaffari, M., Saad, W., Bennis, M., & Debbah, M. (2017). Mobile unmanned aerial vehicles for energy-efficient Internet of Things communications. *IEEE Transactions on Wireless Communications, 16*(11), 7574–7589.
15. Clausen, T., & Jacquet, P. (2003). *Optimized link state routing protocol (OLSR)* (RFC 3626). IETF.
16. Rappaport, T. S. (2002). *Wireless communications: Principles and practice* (2nd ed.). Prentice Hall.

17. Goldsmith, A. (2005). *Wireless communications*. Cambridge University Press.
18. Tse, D., & Viswanath, P. (2005). *Fundamentals of wireless communication*. Cambridge University Press.
19. Proakis, J. G., & Salehi, M. (2008). *Digital communications* (5th ed.). McGraw-Hill.
20. Sklar, B. (2001). *Digital communications: Fundamentals and applications* (2nd ed.). Prentice Hall.
21. Groves, P. D. (2013). *Principles of GNSS, inertial, and multisensor integrated navigation systems* (2nd ed.). Artech House.
22. Farrell, J. (2008). *Aided navigation: GPS with high rate sensors*. McGraw-Hill.
23. Siciliano, B., & Khatib, O. (Eds.). (2016). *Springer handbook of robotics* (2nd ed.). Springer.
24. Beard, R. W., & McLain, T. W. (2012). *Small unmanned aircraft: Theory and practice*. Princeton University Press.
25. Valavanis, K. P., & Vachtsevanos, G. J. (Eds.). (2015). *Handbook of unmanned aerial vehicles*. Springer.
26. NATO Standardization Office. (2017). *STANAG 4586: UAV control system interoperability standard*.
27. U.S. Department of Defense. (2012). *MIL-STD-188-220: Tactical data communications*.
28. Boyd, S., & Vandenberghe, L. (2004). *Convex optimization*. Cambridge University Press.
29. Richards, M. A. (2014). *Fundamentals of radar signal processing* (2nd ed.). McGraw-Hill.
30. Blackman, S., & Popoli, R. (1999). *Design and analysis of modern tracking systems*. Artech House.
31. African Union Commission. (2022). *Security and stability in the Sahel region*.
32. International Maritime Bureau. (2023). *Piracy and armed robbery against ships annual report*.
33. Lake Chad Basin Commission. (2021). *Regional stabilization strategy report*.
34. United Nations Office for West Africa and the Sahel. (2022). *Sahel security monitoring report*.
35. NATO Cooperative Cyber Defence Centre of Excellence. (2021). *Cyber-electromagnetic activities in modern warfare*.
36. RAND Corporation. (2023). *Electronic warfare in modern conflicts: Lessons from Ukraine*.
37. Center for Strategic and International Studies. (2021). *Nagorno-Karabakh conflict and UAV warfare lessons*.
38. Royal United Services Institute. (2024). *Drone warfare and air defence in the Middle East*.
39. MIT Lincoln Laboratory. (2020). *Resilient tactical communications in contested spectrum environments*.
40. DARPA. (2019). *Collaborative operations in denied environment (CODE) program overview*.
41. U.S. Army Futures Command. (2022). *Future vertical lift and autonomous swarm coordination concepts*.
42. NATO Allied Command Transformation. (2023). *Multi-domain operations and autonomous systems integration strategy*.
43. European Defence Agency. (2022). *Autonomous systems in defence applications*.
44. IEEE Aerospace and Electronic Systems Society. (2021). *Secure UAV communication architectures technical report*.
45. International Telecommunication Union. (2023). *Spectrum management for UAV communications in contested environments*.