Adaptive software architecture for managing autonomous robotic logistics in contested environments*

Oleksandr Romaniak[1,†,*], Yevheniya Levus[1,†]

[1]Department of Software, Lviv Polytechnic National University, Ukraine

Abstract

The modern battlefield is undergoing a rapid transformation driven by the widespread deployment of unmanned aerial vehicles (UAVs) and robotic systems, which are redefining tactical logistics. However, high-intensity conflicts have exposed critical vulnerabilities in conventional communication protocols, particularly under conditions of electronic warfare (EW). This paper presents the concept and experimental validation of an adaptive software architecture designed to control autonomous and semi-autonomous robotic logistics platforms. The proposed solution addresses the degradation of communication channels, characterized by high latency and packet loss, through three core pillars: region-of-interest (ROI) extraction for semantic video compression, distributed buffering to prevent stalls during link instability, and a finite-state machine (FSM) that manages transitions to autonomous modes. In simulated degraded-link scenarios, the proposed architecture reduced average video bandwidth demand from 8.0 to 0.4 Mbit/s and decreased lost/expired commands from 45% to 8% relative to a non-adaptive baseline. These values should be interpreted as scenario-dependent point estimates obtained for the evaluated cases. The study compares the control performance of the proposed adaptive architecture against a baseline non-adaptive architecture and does not aim to provide a full comparison against all alternative communication or control methods.

Keywords

autonomous robotic logistics, contested environments, electronic warfare resilience, adaptive software architecture, intermittent communication networks, finite-state machine control, edge computing for robotics, teleoperation systems

1. Introduction

The integration of unmanned platforms into all combat domains has reshaped tactical and strategic frameworks, making the mass adoption of autonomous and remotely piloted systems a defining characteristic of modern warfare [1]. Specifically, the use of aerial drones and ground robotic platforms for logistical purposes, such as ammunition delivery and casualty evacuation, imposes rigorous requirements on the reliability of control systems.

However, the large-scale application of electronic warfare technologies has revealed critical vulnerabilities in traditional communication protocols [2]. While fiber-optic communication currently remains the most reliable and nearly fully secure method against EW interference, it significantly restricts platform mobility and operational flexibility [1]. Furthermore, the physical limitations of fiber optics expose operators to significant security risks by requiring them to remain near the line of contact.

To mitigate these risks, there is a strategic necessity to transition toward remote network-based control architectures [3], enabling the relocation of control stations to safer areas. Yet, this shift introduces new challenges, including limited bandwidth, high latency (often exceeding 1–10 seconds), and elevated cybersecurity risks [4]. Consequently, there is an urgent need for adaptive, AI-powered command and control systems that can function effectively despite uncertainty, poor connectivity, and interference.

*SmartIndustry 2026: 3rd International Conference on Smart Automation & Robotics for Future Industry, March 26–27 , Lviv, Ukraine

1,* Corresponding author.

† These authors contributed equally.

oleksandr.i.romaniak@lpnu.ua (O. Romaniak); yevheniia.v.levus@lpnu.ua (Y. Levus)

0009-0003-5713-0543 (O. Romaniak); 0000-0001-5109-7533 (Y. Levus)

2. Vulnerability analysis of current communication protocols

The analysis of existing robotic combat communication architectures reveals that current protocols often lack the resilience required for active combat zones [1]. When transitioning from direct links to remote control, known vulnerabilities in existing UAV communication protocols must be addressed.

2.1. Encryption and Authentication Deficiencies

Many widely used protocols employed in UAV systems lack robust encryption or authentication mechanisms, making them susceptible to interception or spoofing in operational environments [2].

- Hobbyist Protocols: Protocols such as FrSky, FlySky, Spektrum, and ExpressLRS often do not include native encryption. Upon detecting the signal, adversaries can predict frequency-hopping sequences (FHSS) and clone the transmitter.
- ExpressLRS: Research has demonstrated that this protocol can be compromised after capturing only a few packets, and it suffers from specific vulnerabilities such as UID leakage (CVE-2022-29969).
- MAVLink: MAVLink1, when used without message signing, is openly readable and vulnerable to command injection. While MAVLink2 supports signing, the risk of jamming persists, and unsigned packets remain easy to spoof.

2.2. Susceptibility to Electronic Warfare

Even when encryption is present, the physical layer remains vulnerable. For instance, DJI's OcuSync utilizes AES-256 encryption, which effectively protects commands and video from unauthorized reading. However, the system remains susceptible to frequency jamming [4]. It is critical to note that while frequency-hopping spread spectrum (FHSS) reduces interference, it does not provide cryptographic protection against Man-in-the-Middle (MITM) attacks, which remain feasible against unencrypted telemetry protocols [2].

3. Related work and theoretical foundations

The problem of robotic control under uncertainty and degraded communication conditions is an active area of scientific research. Recent studies have shifted focus toward decentralized architectures that maintain stable control despite severe hardware constraints.

3.1. Adaptive Control and Edge Computing

Recent advancements have focused on reducing latency and reliance on cloud infrastructure. Feng proposed an adaptive control system based on multimodal sensor fusion and edge computing, which achieved a 60% reduction in latency [5]. Similarly, Araujo et al. deployed ResNet-18 on edge hardware to facilitate local autonomous navigation. By removing the need for persistent cloud access, this approach ensures autonomy even in isolation [6].

3.2. Operation Under Intermittent Connectivity

To address unstable communication, the ACHORD project demonstrated methods for coordinating groups of robots in environments with intermittent connectivity by employing multilayer network architectures and localized autonomy [7]. Furthermore, Kivrak developed a cyber-physical architecture for autonomous systems that employs digital twins to reduce transmitted data volumes, a concept critical for bandwidth-constrained environments [8].

3.3. Modularity in Robotic Software

The proposed architecture builds upon established principles of modularity. The CLARAty architecture and various cloud robotics models have utilized modular frameworks to isolate

autonomy logic from specific hardware platforms [9]. This separation ensures that software remains compatible across diverse robotic platforms. However, most existing solutions enforce a rigid dichotomy between complete manual control and full autonomy, which is particularly risky in unpredictable combat environments.

4. Proposed adaptive software architecture

To address the identified challenges of EW interference and bandwidth limitations, we propose a multilayer architecture [1] composed of three functional layers. This system is designed to ensure resilient control of robotic logistics platforms by dynamically adapting autonomy levels and optimizing data traffic. As shown in Figure 1, the proposed architecture is organized into three functional layers that enable adaptive autonomy under degraded communication conditions.

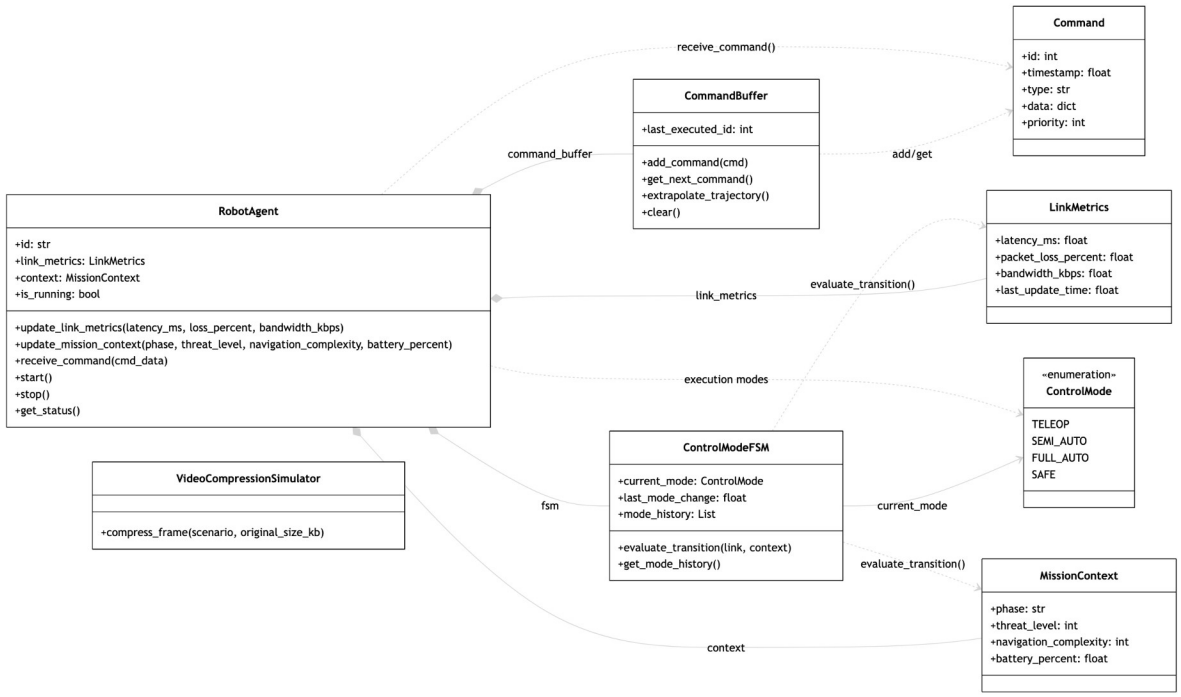

Figure 1: Adaptive software architecture of the proposed robotic logistics control system.

4.1. Adaptive Multimedia Communication Layer

In contested environments, video transmission often consumes the majority of available bandwidth [4]. To mitigate this, the proposed architecture moves away from transmitting full video frames. Instead, it employs semantic compression with region-of-interest (ROI) extraction.

By prioritizing the transmission of semantically relevant data—such as recognized obstacles or targets—over static background information, this layer significantly reduces bandwidth requirements. This approach is conceptually aligned with "Quality of Anything" (QoX) models utilized in 6G networks [10], ensuring that the operator maintains situational awareness even when data throughput is severely restricted.

4.2. Reliable Command Transmission Layer

Electronic warfare often induces jitter and packet loss, rendering standard remote control erratic. To address this, the architecture implements a distributed command buffering scheme with timestamping [2].

- Buffering: This mechanism buffers commands locally on the robot to smooth out motion execution during short-term communication disruptions, preventing the "stuttering" often seen in high-latency scenarios.
- Guaranteed Delivery: Critical control commands are transmitted with guaranteed delivery (Quality of Service Level 2) via an MQTT broker. This ensures that vital instructions are not lost, even if the link is unstable.

4.3. Dynamic Autonomy Control Layer (FSM)

The core logic of the system is governed by a Finite-State Machine (FSM). This module manages all transitions to autonomous modes whenever the connection fails.

The FSM monitors communication quality metrics and mission context in real-time. It switches the robotic platform between three distinct modes:

1. Teleoperation: Full manual control when the link is stable.
2. Semi-Autonomous: Shared control where the robot assists with stability and obstacle avoidance during minor signal degradation.
3. Fully Autonomous: The robot executes pre-planned paths or safe-stop procedures independently when the link is severed.

This dynamic switching ensures that the logistics platform does not stall in a vulnerable position but continues its mission or seeks cover based on local environmental data. The current control mode and link quality are continuously reflected at the operator side, enabling situational awareness and timely intervention, as illustrated in Figure 2.

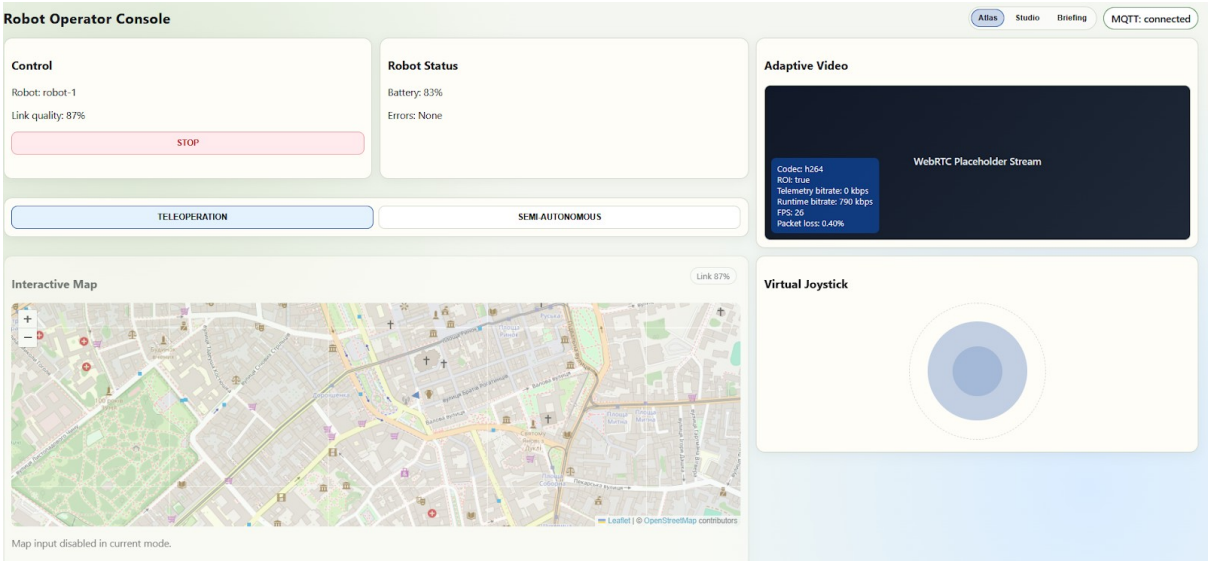

Figure 2: Operator interface for teleoperation and autonomy mode monitoring.

5. Experimental methodology and validation

The experimental evaluation was conducted in a simulated environment to ensure controlled simulated testing conditions. The prototype system was implemented using ROS 2 as the middleware layer, with Gazebo employed for physics-based simulation of robotic motion and sensor feedback. To emulate contested communication conditions, the network layer was configured to introduce variable latency, packet loss, and jitter patterns representative of satellite and long-range radio links typically observed in electronic warfare environments. This setup enabled systematic assessment of control stability and autonomy transitions under progressively degraded connectivity.

Several representative communication conditions were evaluated during the experiments. Four link-condition classes were considered: a stable channel (100 ms latency, 10 Mbit/s throughput), a degraded channel (2 s latency, 500 ms jitter, 1 Mbit/s throughput), an intermittent channel (periodic

disruptions lasting 5–10 s), and EW-like conditions with random packet loss of up to 30%. For architecture-level interpretation, these test conditions were grouped into three representative operating modes: M=0 (standard), M=1 (degraded), and M=2 (critical intermittent or EW-like conditions). In each scenario, the following metrics were measured: Lcmd, the average delay between operator command issuance and its execution in the simulator; B_{usage}, the actual network bandwidth consumption; P_{loss}, the share of lost or expired commands; and $T_{recovery}$, the time required to fully restore control after a link interruption. QoE was assessed on a predefined 5-point ordinal usability scale, ranging from artifact-free visualization to complete image loss, to characterize the practical usability of the video stream under simulated conditions. This setup enabled quantitative comparison between the baseline non-adaptive architecture and the proposed adaptive architecture under progressively degraded communication conditions.

5.1. Experimental Validation and Results

The experimental validation of the proposed adaptive software architecture for remote control systems confirmed its effectiveness in providing resilient control of robotic logistics platforms under unstable communication conditions. The proposed architecture was evaluated in simulated degraded communication conditions and compared against a non-adaptive baseline architecture (full-frame transmission with constant bitrate and constant frame rate). The objective of this evaluation was to compare control behavior at the architecture level, rather than to perform ablation studies of individual subsystems or a full comparison against all alternative transmission methods. The results are summarized in Table 1.

Table 1
Efficiency comparison of the proposed architecture

Scenario	Metric	Baseline Architecture (Non-adaptive)	Proposed Adaptive Architecture
1. Stable channel	Command latency L_{cmd}, ms	120	150 (slight increase due to processing)
M=0 (Standard)	Quality of Experience (QoE)	5.0	4.8
	Current system state (S)	Teleoperation	S_1 (Teleoperation)
	Link status	Stable	Stable
2. Degraded channel	Command latency L_{cmd}, ms	> 2000	800 (Buffered commands, semi-auto mode)
(M=1, Degraded)	Bandwidth usage (B_{usage}), Mbit/s	8.0	0.4 (ROI compression)
	Quality of Experience (QoE)	1.0 (Freezes, artifacts)	3.5 (Acceptable ROI clarity)
	Current system state	Teleoperation (non-adaptive)	S_2 (Semi-autonomous)

	Link status	Communication error	Degraded
3. Intermittent channel / EW	Command loss rate (P_{loss}), %	45	8 (Due to buffering and fallback)
(M=2, Critical)	Recovery time ($T_{recovery}$), s	3–5 (Full reconnection)	< 1 (Smooth mode transition)
	Current system state	Teleoperation (non-adaptive)	S_3 (Full autonomy) / Ssafe
	Link status	Loss of control	Intermittent

The main findings can be summarized across the following key metrics:

- Bandwidth Efficiency: Adaptive multimedia communication based on semantic compression ensured a significant reduction in channel load. In the degraded-channel scenario, average bandwidth demand decreased from 8.0 Mbit/s (baseline) to 0.4 Mbit/s (proposed ROI-based transmission). The relative reduction is computed as:

$$\Delta B = \frac{\left(B_{baseline} - B_{proposed}\right)}{B_{baseline}} * 100, \quad (1)$$

  This allowed the operator to maintain situational awareness even when data throughput was severely restricted.
- Command-Delivery Robustness: In scenarios with high jitter or intermittent disruptions, the share of lost or expired commands (Ploss) decreased from 45% in the baseline version to 8% with the proposed architecture. This improvement is attributed to the distributed command buffering scheme and fallback control logic, which prevent total loss of control during link instability.
- Control Continuity: In the evaluated EW-like scenario, the adaptive system maintained control more consistently than the baseline architecture, which exhibited frequent control losses. This indicates improved operational stability of the proposed architecture within the evaluated scenarios.
- Dynamic Autonomy: The deterministic mode switching based on a Finite-State Machine (FSM) ensured predictable behavior. The system enables smooth transitions from teleoperation to semi-autonomous and fully autonomous modes, eliminating abrupt jumps in robot behavior that could lead to collisions.

5.2. Limitations and Discussion

While the current results are promising, several limitations must be acknowledged. The use of the Gazebo simulation environment does not fully capture the complex effects of physical radio propagation, such as bursty correlated losses, interference, and mobility-dependent channel variation in real combat conditions. Furthermore, the prototype ROI extraction module relies on a simplified segmentation approach, and the experimental network setup does not yet reflect the full heterogeneity of battlefield communication environments. Therefore, the reported results should be interpreted as a limited validation of the proposed concept under controlled simulated input conditions. The present study was designed as an architecture-level comparison between the

proposed adaptive control architecture and a baseline non-adaptive architecture, rather than as a full comparative analysis against all alternative communication or control methods. At the same time, the observed behavior across the evaluated cases indicates the practical promise of the proposed approach. Further development of the model may enable validation across a broader range of scenarios and operating conditions.

6. Conclusions

The reliance on centralized, GPS-dependent control architectures is increasingly inadequate for modern military operations [2]. The analysis of current protocols demonstrates that unencrypted and non-adaptive systems are highly vulnerable to interception and jamming.

The adaptive software architecture presented in this paper offers a robust solution to these challenges. By integrating semantic compression, smart buffering, and fail-safe autonomous switching, the system effectively counters the disruptions caused by electronic warfare and narrow bandwidth. The shift toward decentralized hybrid models, leveraging edge computing and AI, creates the basis for greater autonomy and responsiveness. This approach ensures that autonomous and semi-autonomous robotic logistics devices can operate reliably in distrustful and compromised environments, significantly reducing risks to operators while ensuring mission success [1].

Declaration on Generative AI

During the preparation of this work, the author(s) used Grammarly for grammar and spelling checking. Further, the author(s) used Codex to generate Figure 1, and Nano Bananas to generate Figures 2 in order to create illustrative images. After using these tools/services, the author(s) reviewed, edited, and validated the content as necessary and take(s) full responsibility for the accuracy, originality, and integrity of the publication's content.

References

[1] O. Romaniak, Y. Levus, Methods and tools for managing autonomous and semi-autonomous robotic logistics devices on the battlefield, in: Proceedings of the 2nd International Scientific and Practical Conference "Science and Information Technologies in the Modern World", International Scientific Unity, Athens, Greece, 2025, pp. 300-303. doi:10.70286/ISU-21.05.2025.

[2] C. Liu, Adaptive control of teleoperation systems with uncertainties: A survey, in: Proceedings of the 2021 3rd International Conference on Robotics Systems and Automation Engineering (RSAE '21), ACM, New York, NY, 2021, pp. 5-9. doi:10.1145/3475851.3475856.

[3] P. M. Wensing, J.-J. Slotine, Cooperative adaptive control for cloud-based robotics, in: Proceedings of the IEEE International Conference on Robotics and Automation (ICRA), IEEE, 2018, pp. 6401-6408. doi:10.1109/ICRA.2018.8460856.

[4] S. Krywult, Real-time Communication Systems for Small Autonomous Robots, thesis, Technische Universität Wien, Vienna, 2006. URL: http://hdl.handle.net/20.500.12708/22809.

[5] Y. Feng, Adaptive control system for collaborative sorting robotic arms based on multimodal sensor fusion and edge computing, Scientific Reports 15 (2025) Article 33383. doi:10.1038/s41598-025-18344-9.

[6] S. D. C. Silva Araujo, G. K. Ong Michael, U. U. Deshpande, S. Deshpande, M. G. Avalappa, Y. Amasi, S. Patil, S. Bhat, S. Karigoudar, ResNet-18 based multi-task visual inference and adaptive control for an edge-deployed autonomous robot, Frontiers in Robotics and AI 12 (2025) Article 1680285. doi:10.3389/frobt.2025.1680285.

[7] M. Saboia, L. Clark, V. Thangavelu, J. A. Edlund, K. Otsu, G. J. Correa, V. S. Varadharajan, A. Santamaria-Navarro, T. Touma, A. Bouman, H. Melikyan, T. Pailevanian, S.-K. Kim, A. Archanian, T. S. Vaquero, G. Beltrame, N. Napp, G. Pessin, A. Agha-mohammadi, ACHORD: Communication-aware multi-robot coordination with intermittent connectivity, in:

Proceedings of Robotics: Science and Systems (RSS 2022), 2022. doi:10.15607/RSS.2022.XVIII.058.

[8] H. Kivrak, M. Z. Karakusak, S. Watson, B. Lennox, Cyber-physical system architecture of autonomous robot ecosystem for industrial asset monitoring, Computer Communications 218 (2024) 72-84. doi:10.1016/j.comcom.2024.02.013.

[9] I. A. Nesnas, A. Wright, M. Bajracharya, R. Simmons, T. Estlin, W. S. Kim, CLARAty: An architecture for reusable robotic software, in: G. R. Gerhart, C. M. Shoemaker, D. W. Gage (Eds.), Unmanned Ground Vehicle Technology V, Proceedings of SPIE, volume 5083, SPIE, 2003, pp. 253-264. doi:10.1117/12.497223.

[10] V. Mineeva, A. A. Ateya, A. Volkov, A. Muthanna, A. Koucheryavy, S. A. Chelloug, A. A. Abd El-Latif, A novel feature-oriented quality of anything (QoX) framework for end-to-end robotic services in 6G networks, Scientific Reports 15 (2025) Article 24945. doi:10.1038/s41598-025-09677-6.