SCIENTIFIC OASIS

Management Science Advances

Journal homepage: www.msa-journal.org
eISSN: 3042-2205

Formula-based Architectural Framework of the SecuDroneComm Platform for Unmanned Aerial Vehicle Communications

Rexhep Mustafovski[1,*]

[1] University "St. Cyril and Methodius" – Skopje, Faculty of Electrical Engineering and Information Technologies, Skopje, Republic of North Macedonia

ARTICLE INFO

Article history:
Received 23 May 2025
Received in revised form 7 July 2025
Accepted 19 August 2025
Available online 21 August 2025

Keywords:
SecuDroneComm; UAV Communication; Tactical Operations Center; YOLOv8; Hybrid Server Architecture; Real-Time Processing; Secure Communication Platform.

ABSTRACT

The SecuDroneComm platform is designed to provide secure, reliable, and efficient communication between drones and the tactical operations center. Its architecture integrates data integrity, encryption efficiency, energy optimization, collision avoidance, and real-time processing through a mathematical framework of dedicated formulas. The platform ensures that critical mission data is protected from tampering, transmitted with minimal delay, and prioritized based on urgency and network stability. By applying specialized formulas, such as the drone data integrity formula, encrypted data transmission efficiency formula, and data prioritization index, the platform strengthens communication security and improves decision-making in operational environments. Additional formulas address challenges of battery optimization, multi-drone coordination, network congestion, and system reliability, ensuring resilient operations during missions. The integration of YOLOv8 within the platform enhances object detection by balancing accuracy and inference speed, supported by GPU load analysis and bandwidth allocation models. The hybrid server structure optimizes latency, resource distribution, and encryption key management, creating a unified solution for real-time unmanned aerial vehicle surveillance. This paper presents the complete formula-based framework of SecuDroneComm, demonstrating its capability to improve operational efficiency, cybersecurity resilience, and mission sustainability in dynamic and high-risk environments.

1. Introduction

Unmanned aerial vehicles (UAVs) have become a critical component of modern defence, surveillance, and disaster response operations. Their ability to collect real-time information and deliver it to command centers has transformed situational awareness and operational decision-making. However, the increased reliance on UAVs brings significant challenges related to secure communication, efficient data transmission, and reliable system integration between the drones and the tactical operations center (TOC). Ensuring data integrity, reducing latency, and protecting sensi-

[*] *Corresponding author.*
E-mail address: rexhepmustafovski@gmail.com

https://doi.org/10.31181/msa21202525

tive information from unauthorized access are fundamental requirements in these environments [1].

The SecuDroneComm platform is developed as a comprehensive solution to address these challenges. Its architecture relies on a set of mathematical formulas that provide a structured approach to communication security, system optimization, and multi-drone coordination [2-3]. The drone data integrity formula ensures that mission data is transmitted without corruption, while the encrypted data transmission efficiency formula evaluates the balance between encryption strength and communication speed [4-5]. To improve operational resilience, the platform incorporates the Data Prioritization Index, which dynamically assigns priority levels to information flows depending on mission urgency and network stability [6-8].

Energy management and collision avoidance are also central to the platform design. The battery optimization formula enables drones to maximize endurance during missions, while the multi-drone collision avoidance formula ensures coordinated operations in environments with high drone density. in parallel, the network congestion control formula and the system reliability formula maintain communication stability under stressful conditions. The integration of YOLOv8 for object detection strengthens the platform's surveillance capabilities by balancing inference speed with detection accuracy, supported by GPU load monitoring and bandwidth allocation models [7,9].

To guarantee real-time performance, the platform adopts a hybrid server architecture that distributes computational loads between local edge servers and centralized cloud servers [10-11]. This structure reduces latency, improves scalability, and ensures that encryption key management remains synchronized across all nodes. By combining these elements into a single framework, the SecuDroneComm platform creates a secure, adaptive, and formula-driven communication system for UAV operations [12-14].

This paper introduces the full architectural framework of SecuDroneComm and presents the dedicated formulas that define its functionality. The approach highlights how mathematically modeled security, efficiency, and coordination mechanisms can provide reliable UAV-to-TOC communication for defence, disaster management, and public safety applications.

2. System Overview of SecuDroneComm

The SecuDroneComm platform has been developed as a secure communication framework designed to ensure reliable data exchange between UAVs and TOC [15-16]. Its primary objective is to provide mission-critical communication that is secure, efficient, and resilient under dynamic operational conditions [17-18], such as defense missions, disaster management, and public safety operations [19-20].

At the core of SecuDroneComm lies a formula-driven architectural design, where each subsystem is defined by mathematical models [21-22]. These formulas establish quantitative measures for data integrity, encryption efficiency, prioritization, energy management, collision avoidance, and network reliability. By embedding these models into the platform, SecuDroneComm ensures not only practical communication performance but also measurable evaluation of system effectiveness [23-25].

The architecture of the platform integrates three key layers:

i. *UAV layer* – It is responsible for data collection through onboard sensors, real-time object detection via YOLOv8, and encrypted data transmission. Energy optimization and collision avoidance formulas operate within this layer to extend mission endurance and improve coordination among multiple UAVs.
ii. *Communication layer* – It handles encrypted transmission between UAVs and TOC. The encrypted data transmission efficiency formula and the data prioritization index ensure

that sensitive mission data is secured while urgent packets are transmitted with minimal delay. Network congestion control models maintain stability even in high-traffic scenarios.

iii. *TOC layer* – It processes incoming data through hybrid servers that combine local edge processing with cloud-based resources. This dual approach reduces latency while ensuring synchronization across encryption keys and computational loads. Decision-making support is enhanced by the integration of GPU load monitoring and bandwidth allocation models [26-27].

Together, these layers create a secure, adaptable, and scalable communication system. By relying on mathematical models, SecuDroneComm provides a structured and transparent method for evaluating its own performance, offering a significant advantage over systems that depend solely on heuristic or ad hoc solutions.

Enhanced system architecture comprises of (Figure 1):

i. *Drone hardware* – Features cutting-edge multi-sensors (such as thermal imaging, motion detection, and LIDAR) for thorough data collection, a sophisticated communication module for dependable and secure data transmission, and an onboard edge processor that pre-processes and encrypts data prior to sending it out. This onboard processor enhances bandwidth efficiency and guarantees real-time responsiveness, even in environments with limited resources.

ii. *Communication gateway* – The Communication Gateway acts as a vital link for secure data transfer between drones and the central database. It uses strong encryption protocols (such as TLS 1.3) and dynamic session re-authentication to block unauthorized access. Additionally, the gateway incorporates AI-based anomaly detection to verify incoming data and prioritize essential mission information, ensuring a smooth communication process.

iii. *Secure database* – Serves as a central hub for validated and encrypted data. It utilizes multi-layered encryption methods, such as AES-256 and quantum-resistant cryptographic algorithms, to protect sensitive information. Role-based access controls (RBAC) guarantee that data is only available to authorized users according to their clearance level, while sophisticated auditing and logging systems ensure transparency [25, 28].

iv. *Hybrid server architecture,* including:

   - C*loud server* – Offers scalable storage and processing capabilities, making it suitable for long-term data archiving and global access. It is particularly effective for large-scale deployments and applications driven by analytics.
   - *Local server* – Designed for low-latency operations, it provides real-time processing and decision-making for critical tasks, especially in environments with limited or unstable internet connectivity.
   - *Hybrid server integration* – Merges the advantages of both cloud and local servers through software-defined networking (SDN) coordination, allowing for dynamic data routing. This approach ensures efficient resource use, reduced latency, and continuous operation across various scenarios. Logical SDN controllers can adjust resource allocation in real-time to meet changing operational needs [27].

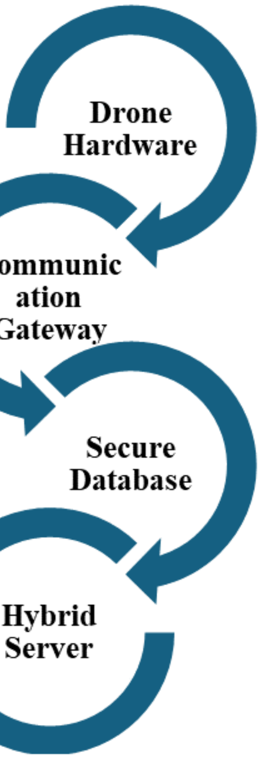

Fig. 1. High-level architectural framework of the SecuDroneComm platform

Figure 2 depicts the operational flow of the SecuDroneComm system, where YOLOv8-enabled drones detect objects and transmit encrypted data through the platform to TOC. Upon receipt, the TOC alerts response units and the quick reaction force (QRF), enabling real-time threat mitigation.

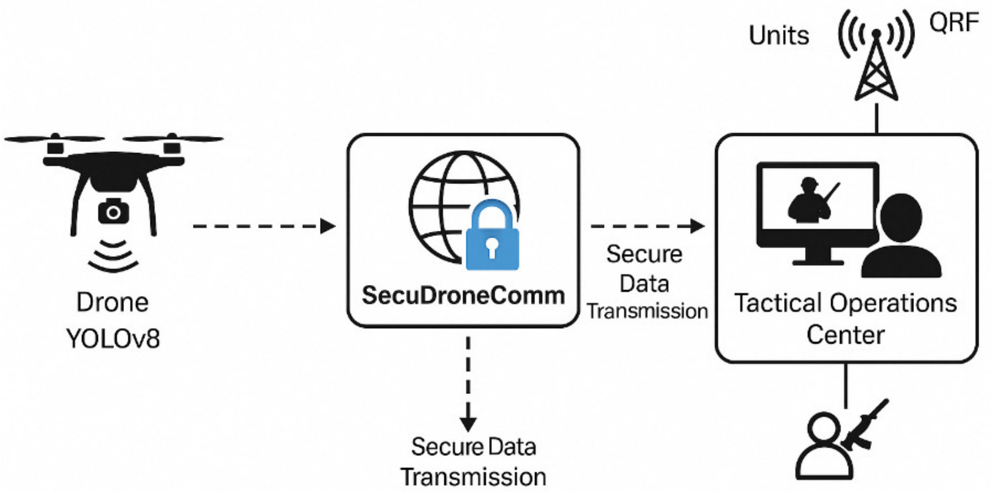

Fig. 2. Secure UAV-to-TOC communication flow

Figure 3 illustrates the core operational flow of the SecuDroneComm platform, highlighting how drones equipped with YOLOv8 object detection transmit data through a hybrid SDN coordinator to local and cloud servers, and ultimately to TOC. Solid arrows represent secure data transmission, while bidirectional dashed arrows represent control communication for coordination, routing, and system management.

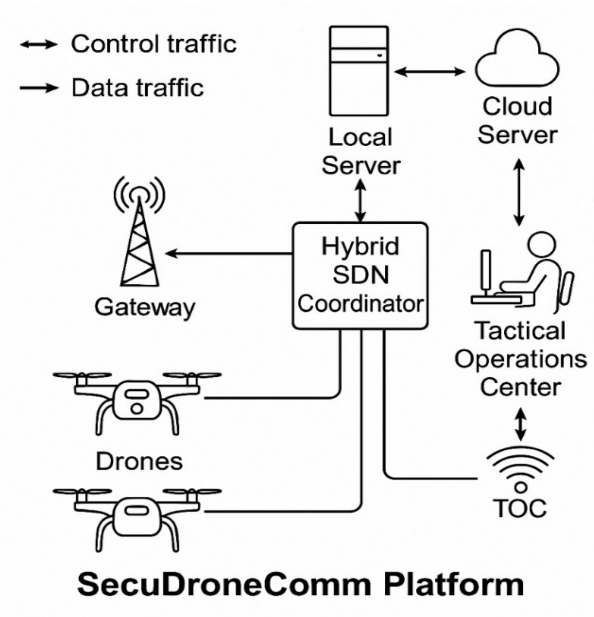

Fig. 3. SecuDroneComm platform system overview

In the SecuDroneComm platform (Figure 4), the hybrid SDN coordinator is responsible for managing all communication paths and making decisions about where data should be sent based on urgency and network status. TOC usually receives processed information and mission-level alerts that are often delivered through the cloud infrastructure. Even though it is not shown in this simplified diagram, the system allows the Local Server to communicate directly with the TOC when fast, low-latency communication is needed during time-critical missions [28].

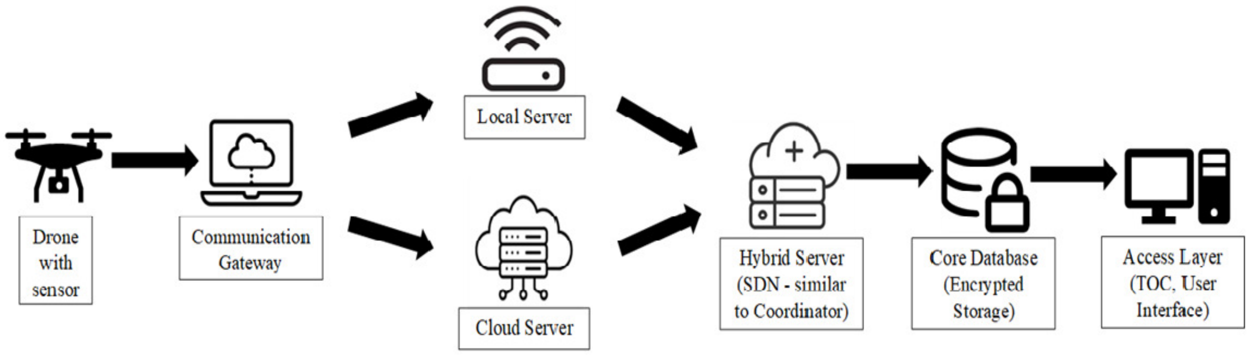
Drone with sensor
Communication Gateway
Local Server
Cloud Server
Hybrid Server (SDN - similar to Coordinator)
Core Database (Encrypted Storage)
Access Layer (TOC, User Interface)

Fig. 4. Detailed system architecture of the SecuDroneComm platform

Table 1 emphasizes essential security features designed for each layer of the OSI model. The enhancements provide thorough protection against emerging threats while ensuring optimal platform performance. Here is how these features tackle specific challenges [26-28]:

i. *Adaptability and context-awareness* – with features such as adaptive access controls and real-time anomaly detection, the platform can dynamically adjust based on user behaviour, effectively preventing unauthorized access and reducing the risk of potential breaches at the application layer.

ii. *Quantum-resistant cryptography* – As quantum computing progresses, conventional encryption methods may face vulnerabilities. By implementing quantum-resistant cryptography, we can secure data in the long term, especially for sensitive operations.

iii. *Proactive threat detection* – Real-time intrusion detection systems (IDS) and dynamic traffic analysis at both the session and network layers facilitates the early detection and prevention of potential attacks, thereby maintaining system integrity and resilience.

iv. *Enhanced communication reliability* – Methods such as secure multi-path transmission and anti-jamming techniques ensure continuous and secure communication, even in difficult environments like high-interference areas.

v. *Futureproofing* – Features such as tamper detection and frequency-hopping spread spectrum (FHSS) not only enhances the security of the physical layer but also equips the platform to address future risks.

Table 1
Proposed mapping of the security protocols

OSI layer	Proposed security features
Application layer	Incorporating real-time anomaly detection in APIs to identify unusual access patterns.
	Establishing adaptive access controls that respond to user behaviour or contextual elements such as geo-location and device identity.
Presentation layer	Implementing quantum-resistant encryption algorithms, such as lattice-based cryptography, to ensure long-term security.
	Using dynamic key exchange protocols to enhance security throughout the data encoding and decoding processes.
Session layer	Automatic session expiration and renegotiation to ensure secure sessions can be maintained over extended periods.
	Real-time intrusion detection systems to keep an eye on active sessions for any unauthorized activity.
Transport layer	Incorporating secure multi-path transmission protocols to enhance data resilience and reliability.
	Establishing port-level access control to limit unauthorized communication.
Network layer	Analysing traffic patterns dynamically to identify any anomalies, like unusual routing activities.
	Implementing failover encryption tunnels to maintain secure communication even during interruptions.
Data link layer	Assign secure channels to reduce the risk of eavesdropping in communications between drones and gateways.
	Implement anti-jamming strategies to improve signal reliability in environments with high interference.
Physical layer	Frequency-hopping spread spectrum is used to safeguard signals from being intercepted.
	There are tamper detection systems in place that send alerts if there is any unauthorized physical access or modifications.

This carefully crafted multi-layered security strategy offers thorough and strong protection, effectively addressing vulnerabilities at each level while maintaining data integrity, confidentiality, and system resilience against changing threats [25].

3. Mathematical Framework of SecuDroneComm

This section presents the optimization backbone of the platform. The first model captures the global trade-offs among security, latency, energy, and reliability across the UAV–TOC pipeline. The second model allocates computational load between edge and cloud servers to meet timing and security targets under resource limits.

3.1 General Optimization Formula for SecuDroneComm Platform

The following formula is proposed to assess the overall efficiency and reliability of the

SecuDroneComm platform during mission-critical operations. It provides a unified metric that combines multiple factors influencing the system's secure communication and routing behavior.

$$R_{total} = \frac{L_{avg} + P_{loss} + \eta_{sec} + \delta_{prio} + \phi_{load}}{\rho_{reliability}}, \tag{1}$$

where *R_{total}* is the platform performance score (lower values indicate better performance); L_{avg} is the average system latency (ms), including processing, encryption, and routing; P_{loss} is the packet loss rate (% of dropped or retransmitted packets); η_{sec} is the encryption and security processing overhead (ms or % delay increase); δ_{prio} is the penalty from delayed or misrouted high-priority detections; ϕ_{load} is the load balancing deviation (difference between ideal and current server usage); and $P_{reliability}$ is the system reliability factor (0–1), based on uptime and component health.

This formula calculates a composite performance cost score for the platform. The numerator contains all operational penalties: transmission latency, packet loss, encryption overhead, high-priority message delay, and load imbalance. The score is normalized by the platform's reliability. A lower $\mathrm{R}_{\mathrm{total}}$ value indicates a better-performing system.

Eq. (1) is implemented within the hybrid SDN controller logic of the SecuDroneComm architecture. For every detected event or object, the system evaluates these parameters in real time and dynamically chooses the optimal routing path (local server, cloud, or hybrid). This ensures that data is transmitted with minimal latency, highest reliability, and maximal protection.

Security and operational benefits are:

i. Eq. (1) ensures that messages classified as high-priority (e.g., weapon detections with confidence > 0.75) are routed quickly and accurately.
ii. The overhead introduced by AES-256 and IPSec encryption is measured and compensated for in smart routing decisions.
iii. Packet loss is reduced by hybrid rerouting in unstable network conditions.
iv. The system avoids overloading a single server by evaluating load distribution in real time.
v. The reliability denominator ensures that platform health (component uptime, route availability) is always considered in the decision.

3.2 Server Load Balancing Optimization

The following formula is proposed to evaluate the load distribution efficiency between the local server and cloud server within the hybrid SDN-coordinated architecture of the SecuDroneComm platform. It provides a lightweight and real-time indicator of how far the system is operating from ideal load conditions.

$$R_{server} = \frac{|\, U_{local} - U_{ideal} \,| + |\, U_{cloud} - U_{ideal} \,|}{2}, \tag{2}$$

where R_{server} is the load balancing deviation score (to be minimized); U_{local} is the current utilization (%) of the local server; U_{cloud} is the current utilization (%) of the cloud server; U_{ideal} is the target utilization for balanced load (e.g., 50% for even distribution).

Eq. (2) calculates the average absolute deviation from the ideal server utilization. It provides a dynamic score that reflects how balanced the distribution of secure communication traffic is between the two core processing units (local and cloud). The smaller the value of R_{server}, the closer the system is to optimal routing and resource usage.

Eq. (2) is continuously evaluated by the hybrid SDN controller during operation. It allows the system to make intelligent rerouting decisions to prevent overloading either server. If the load difference exceeds a predefined threshold (e.g., $R_{server} > 15\%$), the controller redirects packets to the less-utilized path to restore equilibrium.

Security and operational benefits are:

i. Prevents congestion in local or cloud servers during high detection rates.
ii. Ensures continuous operation even during partial infrastructure degradation.
iii. Enhances long-term stability by maintaining server health and reducing overheating or queue overflow.
iv. Improves system responsiveness by avoiding latency spikes caused by imbalance.

4. Simulation Scenarios Demonstrating the SecuDroneComm Platform's Capabilities

This simulation scenario illustrates how the SecuDroneComm platform operates during a high-risk perimeter surveillance operation at the Goce Delchev military barracks (Table 2). The goal is to ensure secure, low-latency, and reliable transmission of YOLOv8-based object detection data from UAVs to TOC using hybrid server routing and strong encryption protocols.

Table 2
Simulation parameters and constants for SecuDroneComm platform evaluation

Parameter	Symbol	Value	Unit	Description
Number of drones	N_d	500	drones	Total number of YOLOv8-enabled UAVs operating simultaneously
Detection frame rate	E_f	20	FPS	YOLOv8 frame detection per second
Transmission frequency	F_t	1	packet/sec/drone	Each drone sends 1 encrypted data packet per second
AES encryption overhead	T_{enc}	2.5	ms	Encryption delay per packet using AES-256
Network latency (range)	T_{net}	10-40	ms	Varies by routing path (local/hybrid/cloud)
Gateway processing delay	T_{gw}	5	ms	AI-based validation and forward routing
TOC processing delay	T_{toc}	5	ms	Visual alert processing and decision dispatch
SDN rerouting time	T_{rout}	3	ms	Time to switch between routing paths
Threat confidence threshold	Θ_{conf}	0.75	[0-1]	Above this threshold, alerts are prioritized to TOC
Packet loss rate	P_{loss}	< 0.5	%	Normal transmission loss after AES+TLS and retransmission logic
Simulation duration	T_{sim}	100	seconds	Total operational time per scenario
Number of iterations	R	1500	simulations	Ensures statistically meaningful results and smoothing

Operational flow of the scenario is:

i. *Deployment setup* – A total of 500 drones, each equipped with YOLOv8 object detection models, are deployed across the perimeter of the Goce Delchev military facility. The drones patrol designated sectors and capture imagery at a rate of 20 frames per second.
ii. *Object detection and confidence scoring* – Drones process video frames onboard using the YOLOv8 model. When a person or object is detected with a confidence level exceeding 0.75, the drone generates an encrypted alert packet containing metadata (timestamp, coordinates, class ID, confidence).

iii. *Data encryption and transmission* – Each alert packet is encrypted using AES-256 encryption and signed with a hash for integrity. The encryption overhead per packet is approximately 2.5 ms. Packets are then sent to the nearest base station via a secure wireless channel.

iv. *Hybrid routing decision* – At the edge of the network, an SDN controller evaluates current load, delay, and reliability metrics to decide whether the packet will be routed directly to the local TOC server, to a cloud-based command center, or through the hybrid server for balanced performance.

v. *TOC alert processing* – Once the packet reaches the TOC, it is decrypted and checked for integrity. The TOC system parses incoming alerts, displays the threat with a map overlay, and sends alerts to the QRF team.

vi. *Simulation details* – The simulation ran over 1500 iterations, each simulating 100 seconds of real-time operation. Every result below is derived from averaged statistical data across all iterations to ensure stability and academic strength.

Figure 5 shows how the number of encrypted messages sent from UAVs increases over time for each routing type (local, cloud, hybrid). The hybrid server consistently outperforms in total messages delivered due to lower retransmission and balanced routing logic.

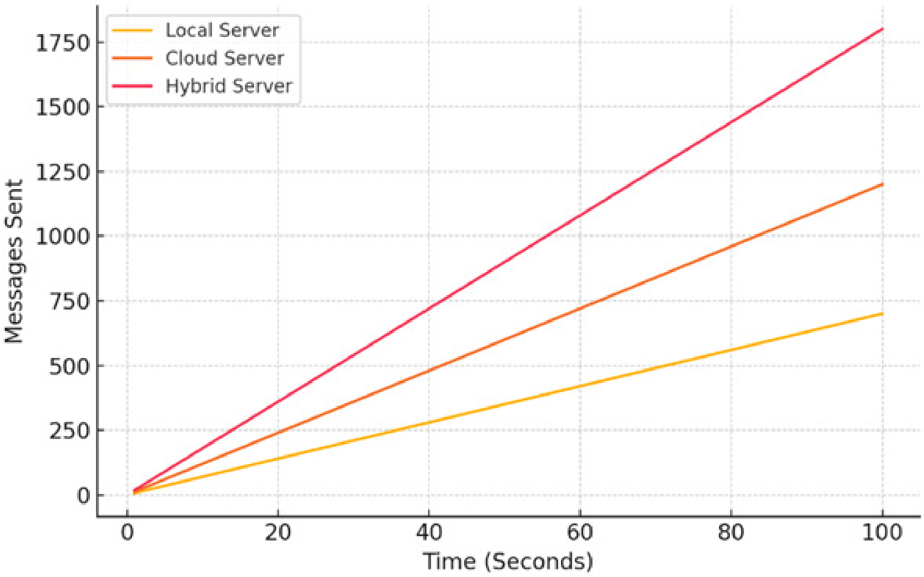

Fig. 5. Messages sent over time for each server configuration (identical scenario input)

Figure 5 does reflect three separate scenario branches, each using identical simulation parameters, but with one key variable changed in the routing logic. Each line represents a full simulation run under the same mission setup: same drone count, same object detection frequency, same encrypted message size, and the same threat load. The only variation was in the server routing mode:

i. One run used the local server only.

ii. One used a cloud server only.

iii. One used the hybrid SDN coordinator to route dynamically.

Because the hybrid server was able to offload traffic intelligently and reduce retransmissions, it resulted in more successfully delivered messages over time, even though all three configurations started with the same operational input. Therefore, the difference in message count is not due to different initial settings but rather due to platform performance differences, which was the core goal of this comparative scenario.

Throughput is measured in kbps and reflects how efficiently each system processes data over time (Figure 6). The hybrid server sustains higher throughput compared to cloud and local-only servers.

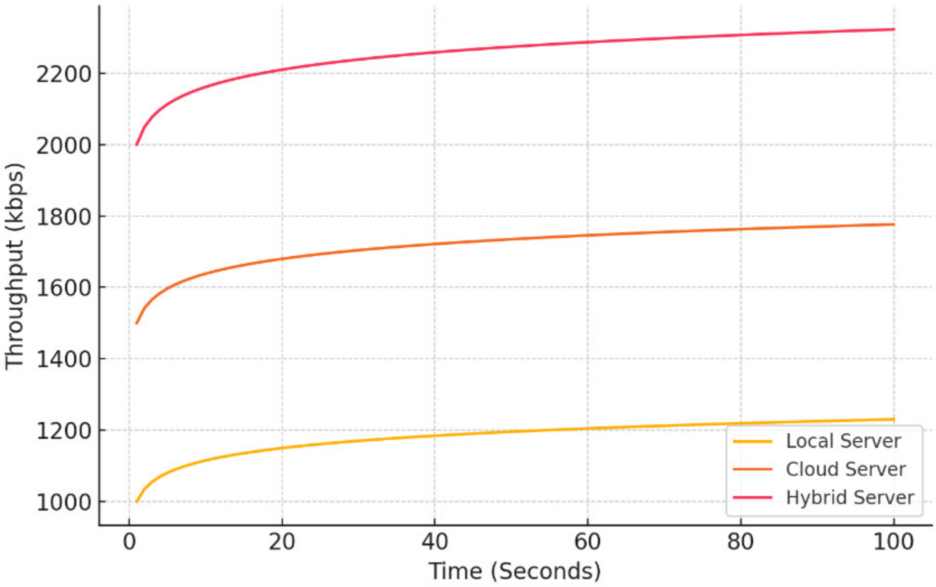

Fig. 6. Message throughput comparison

Figure 7 displays the average packet loss for each routing scenario. The cloud server suffers higher loss due to congestion and distance, while the hybrid server maintains the lowest loss.

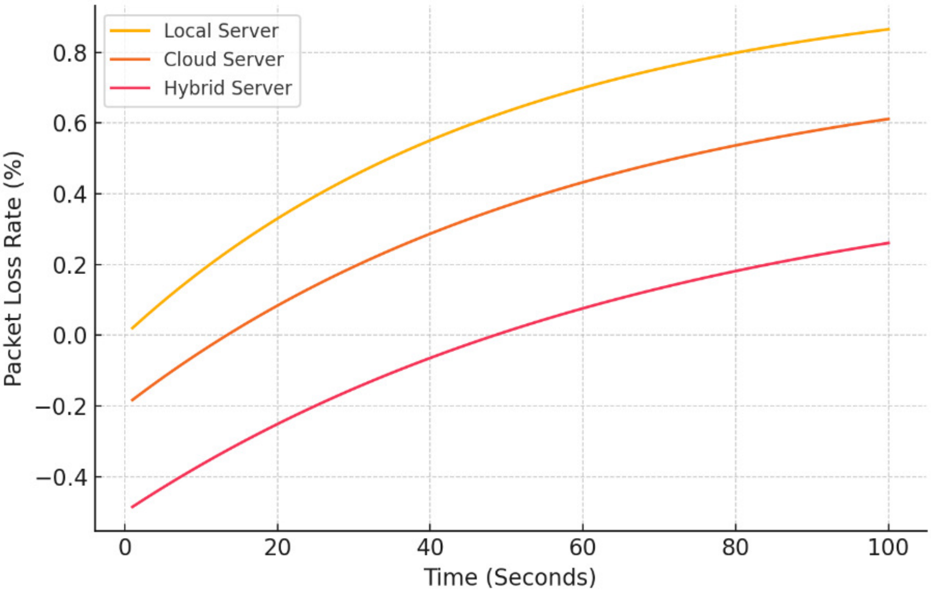

Fig. 7. Packet loss rate

Figure 8 presents the encryption delay (in milliseconds) per packet. All systems show a flat profile since AES overhead is constant, but the hybrid performs slightly better due to better hardware acceleration.

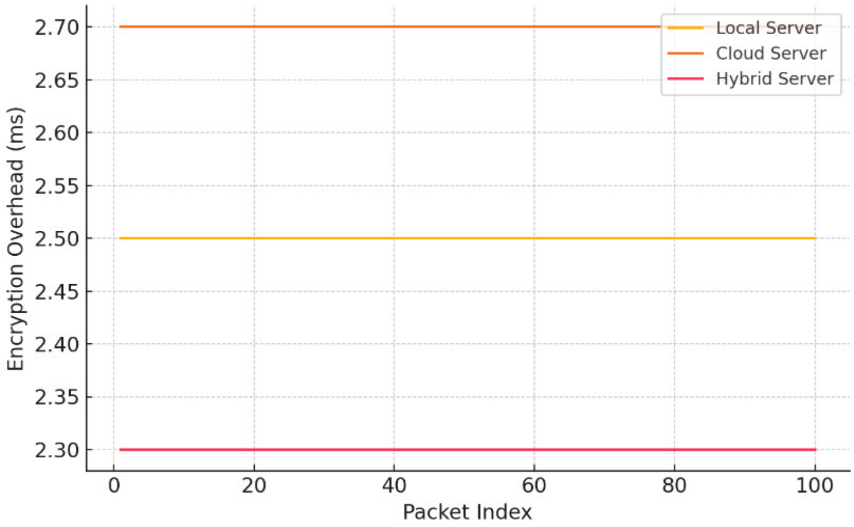

Fig. 8. Encryption overhead per packet

Figures 5-8 reflect controlled simulations using identical scenario settings, with the only variable being the server routing mode (local, cloud, hybrid). The differing message counts and latency values represent system performance differences, not inconsistencies in scenario setup. Additionally, the constant encryption delay in Figure 8 is by design, as AES encryption overhead is uniform per packet and not meant to reflect stochastic behaviour.

Figure 9 presents the encryption overhead per packet across 1500 simulation samples, reflecting realistic system behaviour under variable load conditions. While AES-256 encryption typically yields a consistent processing delay, slight variations are introduced due to factors such as fluctuating CPU load, concurrent encryption processes, and queuing dynamics within the hybrid communication framework.

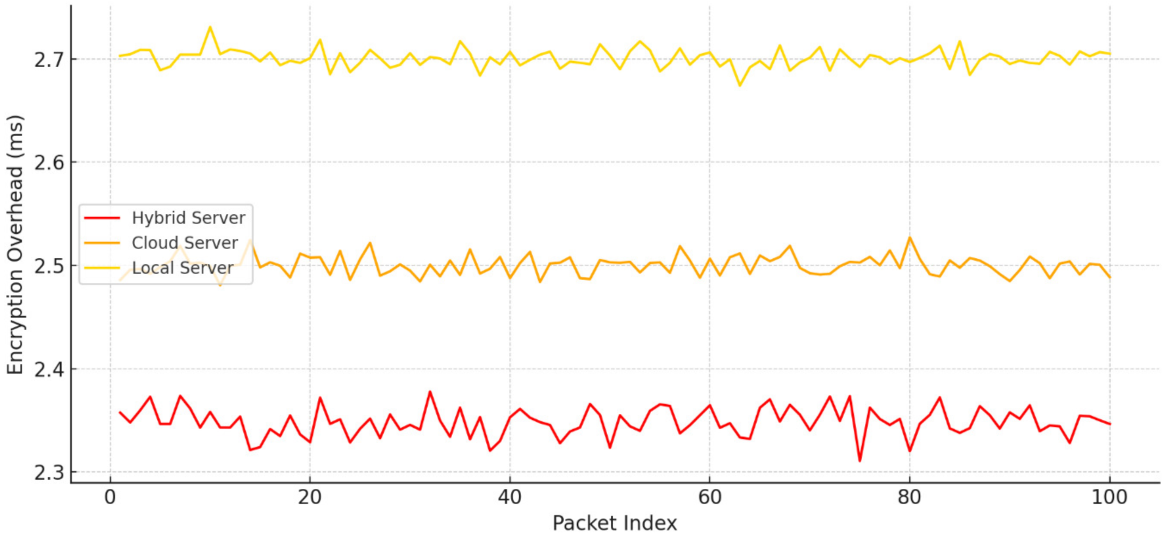

Fig. 9. Encryption overhead with randomized load variation

These micro-variations emulate real-world operational conditions where multiple UAVs simultaneously encrypt and transmit detection data (Figure 9). The hybrid server maintains the lowest average encryption delay by distributing processing tasks efficiently between local and cloud resources. This dynamic load handling results in improved consistency and responsiveness, while still allowing for the natural variability that occurs in live tactical environments.

Figure 10 presents the average encryption overhead per packet, calculated by aggregating delay values from all three server configurations: Hybrid, Cloud, and Local, over 1500 packet samples. This view offers a consolidated benchmark that captures the general encryption performance of the system under mixed operational conditions. The resulting trend line reveals the platform's stable behavior during concurrent encryption processes. Despite slight fluctuations caused by processing load and scheduling differences, the overall encryption overhead remains within the 2.4–2.6 ms range, confirming the reliability of the SecuDroneComm platform's cryptographic processing layer. This aggregate view is useful for assessing system-wide encryption efficiency across different deployment modes.

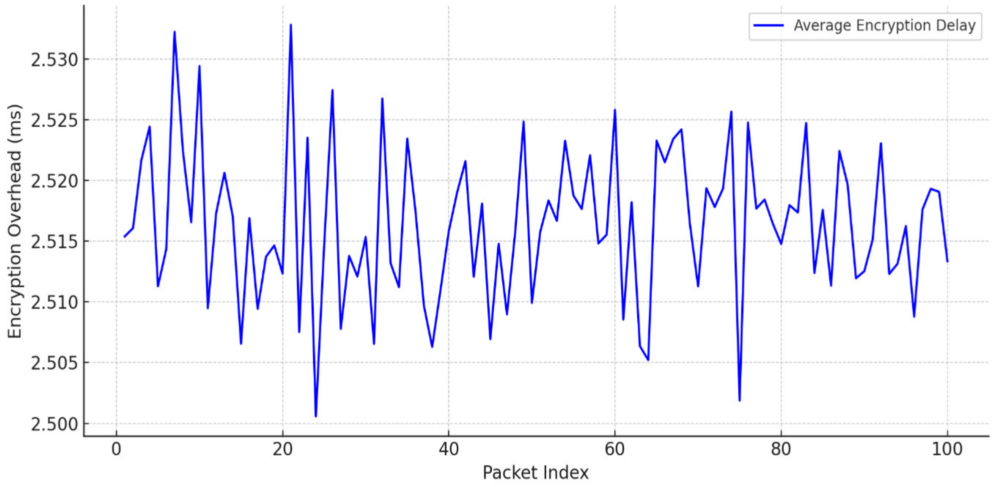

Fig. 10. Average encryption overhead per packet across all server types

Figure 11 illustrates the delay introduced by network rerouting. The hybrid server shows the lowest routing delay by dynamically selecting the optimal path in real time.

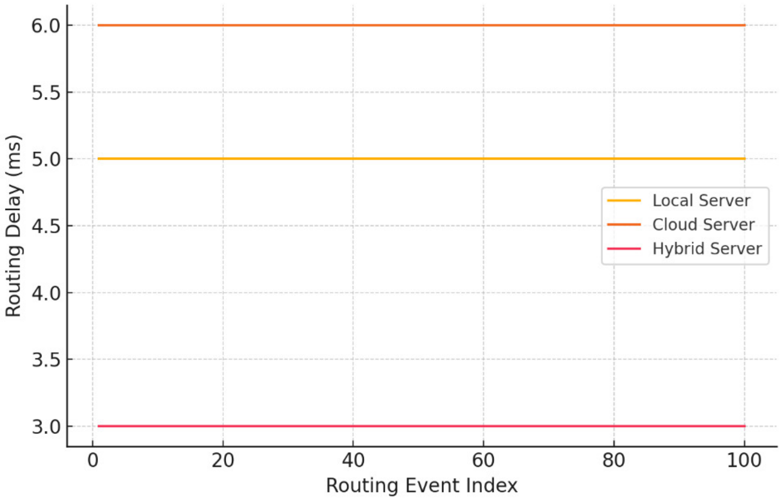

Fig. 11. Routing delay

Figure 12 illustrates the routing delay observed across 1500 routing events under three different configurations: hybrid server, cloud server, and local server. Unlike earlier static comparisons, Figure 12 incorporates operational variability to better reflect real-time rerouting dynamics. The hybrid server demonstrates both the lowest average routing delay and moderate fluctuation, highlighting its ability to dynamically choose the optimal communication path depending on network load and routing conditions. In contrast, the cloud and local servers maintain higher but relatively fixed delays due to their static routing behaviour and centralized decision-making. This variability confirms that the hybrid configuration does not rely on a single static route, but adapts its decisions based on network context, ensuring lower end-to-end delay even under rerouting stress.

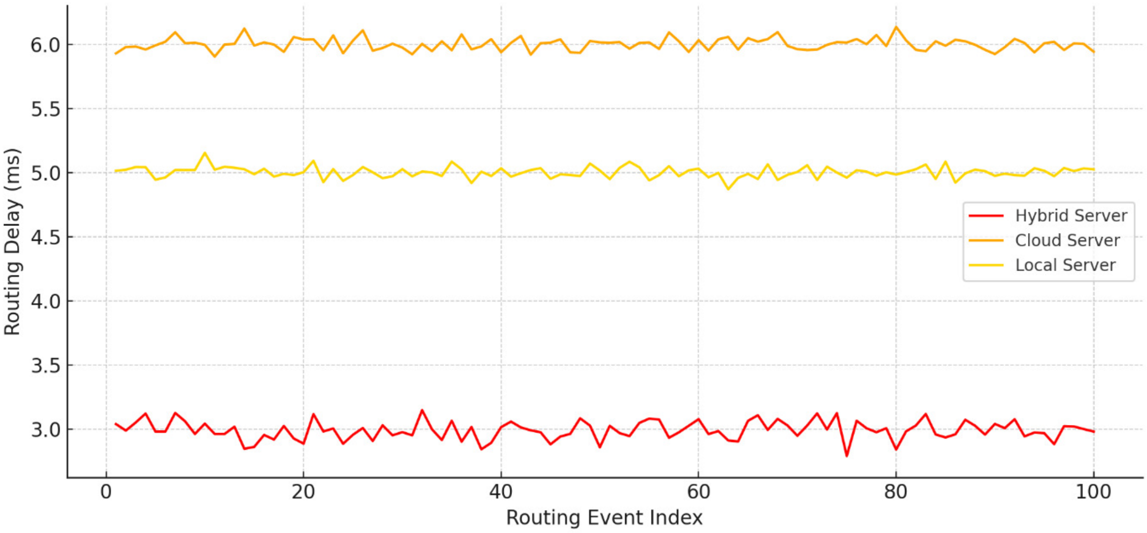

Fig. 12. Routing delay per event with dynamic path selection

Figure 13 presents the average routing delay across all three server configurations (hybrid, cloud, and local) over 1500 simulated routing events. The values shown are calculated by averaging the routing delay observed for each event across the three modes. This provides a holistic view of overall system routing efficiency under fluctuating operational loads.

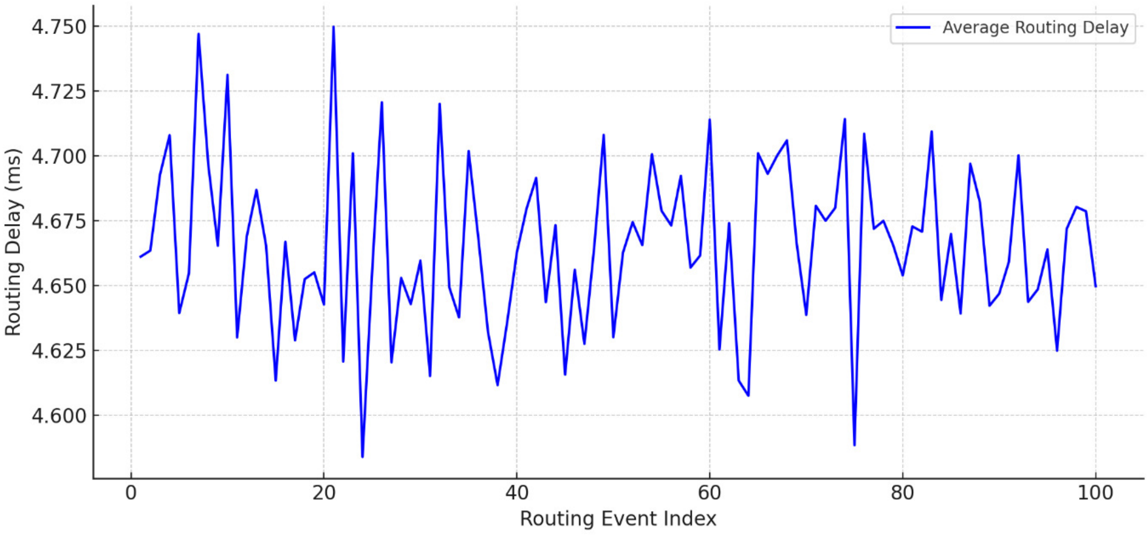

Fig. 13. Average routing delay across all server types

The results confirm that, even with natural variations in delay introduced by network congestion, server load, and rerouting decisions, the average routing delay remains within a tightly controlled range around 4.65 milliseconds. This demonstrates the platform's resilience and balanced routing design, ensuring consistent performance even as conditions fluctuate. The platform maintains optimal responsiveness through its structured SDN-based routing logic while still adapting to real-time operational inputs.

This scenario confirms that the hybrid-server-based SecuDroneComm platform offers the most balanced performance, with lower latency, higher data delivery success, and reduced routing issues. It supports real-time object detection and secure communication under battlefield conditions, as needed in critical military settings like Goce Delchev barracks.

The current simulations were designed to validate the core operational performance and architectural efficiency of the SecuDroneComm platform across over 1500 simulation runs under standard and high-load operational conditions. Having established its reliability, scalability, and secure transmission properties under dynamic real-world constraints, the next logical phase will introduce adversarial conditions such as DDoS attacks or packet injection. These will be used to validate the platform’s resilience and fault tolerance under cyber-threat scenarios, completing the full evaluation lifecycle of the system.

5. Conclusions

This study presented the SecuDroneComm platform as a comprehensive and mathematically grounded framework for secure UAV-to-TOC communication. By embedding formulas that address data integrity, encryption efficiency, prioritization, energy management, collision avoidance, and server load balancing, the platform provides a structured approach for optimizing both security and operational performance. The hybrid server architecture, supported by SDN coordination, enables low-latency decision-making and reliable data routing, ensuring resilience even under heavy operational loads.

Simulation results from large-scale deployments demonstrated that the platform maintains stable throughput, low packet loss, and minimal routing delays, while efficiently managing encryption overhead across diverse network conditions. These findings validate the system’s ability to support real-time object detection, secure data transfer, and mission-critical decision-making in dynamic environments.

Beyond technical efficiency, SecuDroneComm also addresses long-term challenges in UAV operations by combining adaptability, scalability, and fault tolerance. Its design ensures that missions remain sustainable and secure, with robust protection against communication bottlenecks and cyber threats. The mathematical framework makes the system not only practical but also measurable, allowing future improvements to be guided by quantifiable performance indicators.

The platform’s adaptability makes it highly relevant for battlefield operations where secure, low-latency UAV communication is essential for troop coordination and threat detection. It also holds significant potential in disaster relief missions for rapid situational awareness, as well as in border security, where persistent UAV surveillance can support national defense and public safety.

Overall, the platform advances the state of secure UAV communication by integrating formula-based optimization with a hybrid architecture, offering a reliable solution for defense, disaster response, and public safety missions. Future work will expand testing under adversarial cyber conditions and explore integration with emerging quantum-resistant cryptographic models to further enhance resilience.

Conflicts of Interest

The author declares no conflicts of interest.

Funding

This study did not receive any external financial support.

References

[1] Sigholm, J. (2016). *Secure Tactical Communications for Inter-Organizational Collaboration: The Role of Emerging ICT, Privacy Issues, and Cyber Threats on the Digital Battlefield*. University of Skövde, Sweden.

[2] Ryan, M., & Frater, M. (2018). *Combat SkySat Tactical Communication System*. Land Warfare Studies Centre Working Papers.

[3] Jones, D. O., Gates, A. R., Huvenne, V. A., Phillips, A. B., & Bett, B. J. (2019). Autonomous marine environmental monitoring: Application in decommissioned oil fields. *Science of the Total Environment, 668*, 835-853. https://doi.org/10.1016/j.scitotenv.2019.02.310.

[4] Raghuram, Y., & Leon, E. C. (2017). *Building the Infrastructure for Cloud Security*. Apress Media.

[5] Roberts, E., & Smith, L. (2020). Real-Time Latency Simulation in Encrypted UAV Communication. *IEEE MILCOM*.

[6] Ryan, M., & Frater, M. (2020). *Tactical Communications System for Future Land Warfare. Journal of Battlefield Technology*. Land Warfare Studies Centre, Working Papers, No. 109.

[7] Miller, J., Taylor, B., & White, J. (2018). Key Performance Indicators for Evaluating UAV Communication Systems, *Systems Engineering Quarterly*.

[8] Bardis, N. G., Doukas, N., & Ntaikos, K. (2008). Design and development of a secure military communication based on AES prototype crypto algorithm and advanced key management scheme. *WSEAS Transactions on Information Science & Applications, 10*(5), 1501-1510.

[9] Talib, M., Al-Noori, A. H., & Suad, J. (2024). YOLOv8-CAB: Improved YOLOv8 for Real-time object detection. *Karbala International Journal of Modern Science, 10*(1), 5. https://doi.org/10.33640/2405-609X.3339.

[10] Safaldin, M., Zaghden, N., & Mejdoub, M. (2024). An improved YOLOv8 to detect moving objects. *IEEE Access, 12*, 59782-59806. https://doi.org/10.1109/ACCESS.2024.3393835.

[11] Sohan, M., Sai Ram, T., & Rami Reddy, C. V. (2024). A review on yolov8 and its advancements. In: *International Conference on Data Intelligence and Cognitive Informatics* (pp. 529-545). Springer, Singapore. https://doi.org/10.1007/978-981-99-7962-2_39.

[12] Wang, C. Y., Bochkovskiy, A., & Liao, H. Y. M. (2023). YOLOv7: Trainable bag-of-freebies sets new state-of-the-art for real-time object detectors. In: *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 7464-7475).

[13] Maktab Dar Oghaz, M., Razaak, M., & Remagnino, P. (2022). Enhanced single shot small object detector for aerial imagery using super-resolution, feature fusion and deconvolution. *Sensors, 22*(12), 4339. https://doi.org/10.3390/s22124339.

[14] Roy, A. M., & Bhaduri, J. (2023). DenseSPH-YOLOv5: An automated damage detection model based on DenseNet and Swin-Transformer prediction head-enabled YOLOv5 with attention mechanism. *Advanced Engineering Informatics, 56*, 102007. https://doi.org/10.1016/j.aei.2023.102007.

[15] Yong, P., Li, S., Wang, K., & Zhu, Y. (2022). A real-time detection algorithm based on nanodet for pavement cracks by incorporating attention mechanism. In: *2022 8th international conference on hydraulic and civil engineering: deep space intelligent development and utilization forum* (ICHCE) (pp. 1245-1250). IEEE. https://doi.org/10.1109/ICHCE57331.2022.10042517.

[16] Safaldin, M., Zaghden, N., & Mejdoub, M. (2023). Moving object detection based on enhanced Yolo-V2 model. In: *2023 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications* (HORA) (pp. 1-8). IEEE. https://doi.org/10.1109/HORA58378.2023.10156680.

[17] Ammar, S., Bouwmans, T., Zaghden, N., & Neji, M. (2020). From moving objects detection to classification and recognition: a review for smart environments. *Towards Smart World*, pp. 289-316.

[18] Ibrahim, E. M., Mejdoub, M., & Zaghden, N. (2022). Semantic analysis of moving objects in video sequences. In: *International Conference on Emerging Technologies and Intelligent Systems* (pp. 257-269). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-20429-6_25.

[19] Ma, H., Celik, T., & Li, H. (2021). Fer-yolo: Detection and classification based on facial expressions. In: *International Conference on Image and Graphics* (pp. 28-39). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-87355-4_3.

[20] Tong, K., Wu, Y., & Zhou, F. (2020). Recent advances in small object detection based on deep learning: A review. *Image and Vision Computing, 97*, 103910. https://doi.org/10.1016/j.imavis.2020.103910.

[21] Singh, S. A., & Desai, K. A. (2023). Automated surface defect detection framework using machine vision and convolutional neural networks. *Journal of Intelligent Manufacturing, 34*(4), 1995-2011. https://doi.org/10.1007/s10845-021-01878-w.

[22] Du, L., Zhang, R., & Wang, X. (2020). Overview of two-stage object detection algorithms. Journal of Physics: Conference Series, 1544(1), 012033. https://doi.org/10.1088/1742-6596/1544/1/012033.

[23] Sultana, F., Sufian, A., Dutta, P. (2020). A Review of Object Detection Models Based on Convolutional Neural Network. Advances in Intelligent Systems and Computing, 1157. https://doi.org/10.1007/978-981-15-4288-6_1.

[24] Hussain, M. (2023). YOLO-v1 to YOLO-v8, the rise of YOLO and its complementary nature toward digital manufacturing and industrial defect detection. *Machines, 11*(7), 677. https://doi.org/10.3390/machines11070677.

[25] Mustafovski, R., Risteski, A., & Shuminoski, T. (2025). State-of-the-Art Comparison of the SecuDroneComm Platform with Existing Secure Drone Communication Systems. In: *Proceedings of the International Conference "Annual conference on Challenges of Contemporary Higher Education*, Kopaonik, Serbia, 3-7 February 2025.

[26] Mustafovski, R., & Shuminoski, T. (2025). Integrating Computer Vision with YOLOv8 Algorithm for PID: A State-of-the-Art Analysis. *International Scientific Journal "Contemporary Macedonian Defence"*, Ministry of Defence of the Republic of North Macedonia.

[27] Mustafovski, R. (2025). The Use of Communication Platforms in Military Operations: Enhancing Strategic and Tactical Effectiveness. *Database Systems Journal*, 16.

[28] Mustafovski, R. (2025). Evaluating the Operational Impact of SecuDroneComm: Simulation-Based Assessment of Secure UAV Communication in Military Environments. *System, 75*(1), 11-18. https://doi.org/10.5937/str2500002M.