Scientific Research Publishing

Journal of Computer and Communications, 2026, 14(1), 99-135
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

A Cyber-Resilient UAV Swarm Framework for Fire-Fighting with AI-Based In-Flight Defect Inspection

Ahad Alotaibi, Abdullah Alrasheedi

Department of Advanced Technology, Canadian College of Kuwait, Al Jahra, Kuwait
Email: a.alotaibi@ac-kuwait.edu.kw

How to cite this paper: Alotaibi, A. and Alrasheedi. A. (2026) A Cyber-Resilient UAV Swarm Framework for Fire-Fighting with AI-Based In-Flight Defect Inspection. *Journal of Computer and Communications*, **14**, 99-135.
https://doi.org/10.4236/jcc.2026.141007

Received: December 26, 2025
Accepted: January 19, 2026
Published: January 22, 2026

Abstract

Drone swarms are increasingly deployed in fire-fighting missions due to their scalability, adaptability, and ability to operate in hazardous and dynamic environments. However, ensuring mission continuity in such safety-critical scenarios requires not only reliable drone performance but also strong protection against cyber threats targeting inter-drone communication and coordination. This paper presents a cyber-resilient UAV swarm framework for fire-fighting missions that integrates AI-enabled in-flight defect and integrity inspection with secure communication mechanisms. The proposed architecture employs a hierarchical formation in which a dedicated inspector drone periodically captures visual data of neighboring operational drones during the mission to detect structural defects, abnormal behavior, or integrity violations using AI-based visual analysis implemented with Amazon Rekognition. In parallel, cyber resilience is reinforced through subnet segmentation and Route Optimization for Autonomous Systems (ROAS), which mitigates Man-in-the-Middle (MITM) and traffic manipulation attacks. The framework is evaluated using a cyberattack simulation environment built in GNS3 with Ettercap for adversarial traffic injection. Experimental results demonstrate reduced attack success rates, early detection of drone defects, and improved operational reliability, ensuring secure and continuous swarm operation during fire-fighting missions. The proposed dual-layer approach provides a secure, self-verifying UAV swarm architecture suitable for safety-critical fire-fighting and emergency response applications.

Keywords

UAV Swarm, Fire-Fighting Missions, Cyber-Resilient UAV Systems, AI-Enabled In-Flight Defect Detection, UAV Cybersecurity, MITM Attack Mitigation, Secure Routing, GNS3 Simulation, Amazon Rekognition

1. Introduction

Unmanned Aerial Vehicles (UAVs) have become indispensable tools in fire-fighting and emergency response missions due to their mobility, rapid deployability, cost-effectiveness, and ability to operate in hazardous environments with minimal risk to human responders. In fire-fighting scenarios, UAVs support tasks such as situational awareness, fire perimeter monitoring, hotspot detection, and operational coordination in conditions characterized by high temperatures, dense smoke, and rapidly evolving hazards [1]. As fire-fighting operations increase in complexity and spatial scale, single-UAV solutions are often insufficient, as they lack redundancy, resilience, and the ability to simultaneously perform multiple mission objectives. The failure or degradation of a single UAV can result in complete mission interruption and loss of critical situational awareness.

To address these limitations, **UAV swarm systems**, defined as groups of multiple autonomous or semi-autonomous UAVs that cooperate through communication and coordination to achieve shared mission goals, have emerged as a scalable and effective approach for sustained fire-fighting support [2]. Unlike single-drone deployments, UAV swarms enable **parallel task execution**, where individual drones can be assigned specialized roles such as thermal monitoring, visual inspection, communication relaying, and logistics support. This functional distribution enhances mission efficiency and enables broader area coverage within shorter time frames [3]. Moreover, UAV swarms provide inherent **redundancy and fault tolerance**, allowing the system to continue operating even if individual drones experience failures or performance degradation [4]. Swarm-based architectures also offer improved adaptability to dynamic environments, as tasks can be reallocated in real time based on mission demands, environmental changes, or drone health conditions [5]. Through cooperative sensing and shared situational awareness, swarms can generate more accurate and robust environmental assessments than isolated UAVs.

In fire-fighting missions, where operational environments are highly unpredictable and safety considerations are critical, the deployment of UAV swarm systems offers substantial advantages over single-UAV approaches. The cooperative nature of swarms enhances system reliability by providing redundancy and enabling continued operation in the presence of individual UAV failures or performance degradation [6]. Furthermore, swarm-based architectures improve mission scalability and adaptability by allowing dynamic task reallocation and coordinated response to rapidly changing fire conditions. These characteristics make UAV swarm systems particularly effective for complex emergency response operations that require continuous situational awareness, rapid decision-making, and sustained monitoring over extended mission durations [7].

Despite their operational advantages, UAV swarms deployed in fire fighting missions introduce significant challenges related to reliability, safety, and cyber security. Fire environments accelerate physical degradation of aerial platforms due to heat exposure, airborne debris, and mechanical stress [8]. Structural issues

such as propeller damage, frame deformation, or sensor misalignment can compromise flight stability and mission effectiveness, potentially leading to mid-mission failures [9]. Traditional inspection and maintenance procedures are typically performed pre- or post-flight, offering no capability to detect defects while drones are actively operating. This limitation motivates the integration of autonomous in-flight inspection mechanisms capable of continuously assessing the physical integrity of UAVs during mission execution [10].

In parallel with physical reliability concerns, UAV swarm networks operating in fire fighting scenarios are highly vulnerable to cyber threats [11]. The reliance on wireless communication for coordination, telemetry exchange, and command dissemination exposes swarm systems to attacks such as Man-in-the-Middle (MITM), packet injection, and traffic manipulation [12]. In safety-critical fire fighting missions, compromised communication can result in loss of coordination, misinformation, or unsafe behaviour, directly impacting mission success and responder safety. Ensuring the confidentiality, integrity, and availability of inter-drone communication is therefore a fundamental requirement for secure UAV swarm deployment in emergency response environments [13].

In response to these challenges, this paper proposes a cyber-resilient UAV swarm framework tailored for fire fighting missions, combining in-flight defect and integrity inspection with secure communication mechanisms. The framework employs a hierarchical six-drone formation, in which five operational drones execute fire fighting-related tasks while a dedicated inspector drone operates at a supervisory level. The inspector drone periodically captures visual data of the operational drones during flight and analyses these images using AI-based techniques implemented through Amazon Rekognition. This process enables real-time detection of structural defects, abnormal behaviour, or integrity violations without interrupting mission execution, thereby enhancing operational safety and resilience.

To address cyber security vulnerabilities, the proposed framework integrates subnet segmentation and Route Optimization for Autonomous Systems (ROAS) to protect inter-drone communication from interception and manipulation [14]. These mechanisms reduce the attack surface of the swarm network and limit the propagation of malicious traffic. The cyber resilience of the system is evaluated through controlled MITM attack simulations conducted using GNS3 network emulation and Ettercap for adversarial traffic injection [15]. This evaluation demonstrates the effectiveness of the proposed secure routing and segmentation strategies in maintaining reliable and trustworthy communication under attack conditions.

The main contributions of this work are summarized as follows:

- A cyber-resilient UAV swarm framework designed specifically for fire fighting missions, integrating physical integrity inspection and secure communication.
- A hierarchical six-drone architecture featuring a dedicated inspector drone

that performs autonomous in-flight inspection and integrity verification of operational drones using AI-based visual analysis.

- A secure networking design incorporating subnet segmentation and ROAS routing to mitigate MITM attacks and enhance communication resilience within the swarm.
- Experimental validation through a six-drone deployment and cyber attack simulations using GNS3 and Ettercap to evaluate operational reliability and communication security.

By integrating real-time physical inspection with robust cyber security mechanisms, the proposed framework enhances the safety, resilience, and continuity of UAV swarm operations in fire fighting environments. This work contributes toward the development of secure, self-verifying multi-UAV systems capable of supporting mission-critical emergency response operations.

The remainder of this paper is organized as follows. Section 2 presents the proposed UAV swarm framework, including the hierarchical architecture, AI-based inspection workflow, and secure networking design. Section 3 introduces the MITM threat model and the corresponding defence strategies. Section 4 describes the experimental setup, covering both the physical drone swarm deployment and the cyber security validation environment. Section 5 discusses the experimental results, and Section 6 concludes the paper with directions for future research.

2. Proposed UAV Swarm Framework

This section presents the proposed UAV swarm framework developed to support fire fighting missions in hazardous and dynamic environments. Fire fighting operations impose strict requirements on aerial systems due to extreme temperatures, dense smoke, unpredictable airflow, and rapidly evolving fire fronts. These conditions increase the likelihood of both physical degradation of UAV platforms and communication disruptions, making reliability and security critical for mission success. To address these challenges, the proposed framework integrates AI-enabled in-flight defect and integrity inspection with cyber-resilient communication mechanisms, enabling safe, continuous, and trustworthy swarm operation during emergency response missions. The framework adopts a hierarchical swarm architecture composed of six UAVs, where five drones perform operational fire fighting tasks and one drone acts as a dedicated inspector and commander. The inspector drone continuously monitors the physical condition and behaviour of the operational drones during flight, while secure communication is maintained through subnet segmentation and Route Optimization for Autonomous Systems (ROAS). This dual-layer design ensures that both physical integrity and cyber security are addressed simultaneously, which is essential in safety-critical fire fighting scenarios.

2.1. Swarm Architecture Overview

The proposed UAV swarm architecture is a hierarchical, heterogeneous, six-

drone system designed to support fire fighting missions under hazardous and dynamically changing environmental conditions. Fire fighting environments present severe challenges for aerial systems, including high ambient temperatures, dense smoke, strong updrafts, and airborne debris, all of which can accelerate mechanical degradation and impair communication reliability. The architecture is therefore designed to ensure continuous mission execution, in-flight structural integrity awareness, and secure coordination, while maintaining sufficient flexibility to adapt to evolving fire scenarios. The swarm architecture consists of four tightly integrated components:

1. a supervisory aerial layer;
2. an operational aerial layer;
3. a ground control layer;
4. a secure communication and data exchange layer.

These components collectively enable distributed task execution with centralized integrity monitoring and decision support. An overview of the proposed swarm architecture and the interaction among its main components is illustrated in Figure 1.

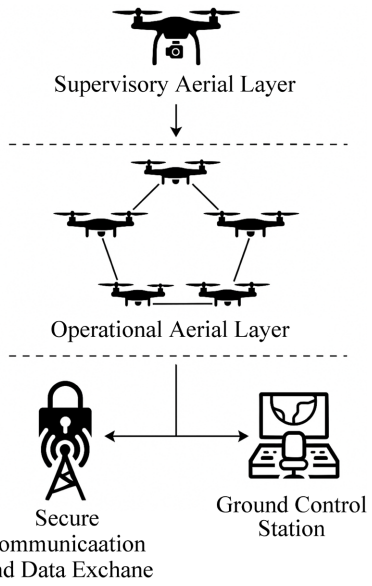

Figure 1. The Fire Fighting proposed system architecture.

2.1.1. Hierarchical Swarm Organization

The swarm follows a hierarchical organization model, in which operational responsibilities and supervisory responsibilities are explicitly separated. Five UAVs form the operational layer, executing fire fighting-related sensing and support tasks in close proximity to hazardous regions. A sixth UAV operates as a supervisory inspector and coordinator, maintaining an elevated or offset position that enables continuous observation of the operational layer. This separation serves several architectural objectives. First, it reduces the exposure of the supervisory UAV to extreme thermal and mechanical stress, increasing its availability and re-

liability. Second, it enables uninterrupted in-flight inspection of operational UAVs without interfering with their mission tasks. Third, it provides a stable aggregation point for telemetry, integrity data, and network status information, which is essential for coordinated response in safety-critical missions.

2.1.2. Supervisory Inspection and Coordination Layer

The supervisory layer is implemented by a dedicated Inspector/Commander UAV that provides system-level oversight of swarm behaviour and physical integrity. From an architectural perspective, this UAV acts as a mobile integrity sensor and coordination node, bridging the operational swarm and the Ground Control Station. The Inspector/Commander UAV continuously observes the operational UAVs using on-board imaging sensors and collects telemetry streams describing flight state, communication quality, and mission progress. This combination of visual and telemetry-based observation enables early identification of integrity anomalies, including structural deformation, abnormal flight dynamics, sensor misalignment, or thermal stress effects caused by proximity to fire. Importantly, the inspection function is designed to operate in parallel with fire-fighting tasks. The architecture does not require operational UAVs to interrupt sensing, delivery, or relay activities in order to be inspected. Instead, inspection is performed opportunistically during normal formation flight, which minimizes mission disruption and preserves operational efficiency.

2.1.3. Operational Fire-Fighting Layer

The operational layer consists of five UAVs responsible for executing mission-specific fire fighting functions. Rather than relying on identical drones performing redundant tasks, the architecture adopts a functionally diversified design, allowing the swarm to address multiple mission objectives simultaneously. This includes thermal observation, environmental hazard sensing, close-range visual assessment, logistical support, and communication extension. From an architectural standpoint, this diversity improves situational awareness, fault tolerance, and coverage efficiency. If one operational UAV experiences degradation or failure, its task can be partially redistributed among remaining UAVs without collapsing the entire mission. The Inspector/Commander UAV supports this process by identifying compromised UAVs early and enabling timely task reallocation. Each operational UAV continuously publishes telemetry and mission data to the supervisory layer and the GCS, forming a shared situational picture that supports adaptive decision-making.

2.1.4. Ground Control Layer

The Ground Control Station represents the human-in-the-loop component of the architecture and serves as the primary interface between autonomous swarm behaviour and operational command. While the swarm is capable of autonomous coordination, fire fighting missions require human oversight due to their safety-critical nature. The GCS receives mission data, integrity alerts, and network status

indicators from the swarm and provides operators with a comprehensive view of system health and environmental conditions. Based on this information, operators can issue high-level commands such as task reassignment, mission boundary updates, or controlled withdrawal of compromised UAVs. The architecture ensures that these commands are propagated reliably and securely to the swarm.

2.1.5. Communication and Data Exchange Architecture

A core element of the swarm architecture is the secure wireless communication layer, which supports multiple concurrent data flows. These include telemetry exchange, command and control messages, inspection imagery, integrity alerts, and sensor data streams. In fire fighting environments, communication links are vulnerable to interference, obstruction, and malicious exploitation. To address these risks, the architecture is explicitly designed to integrate network segmentation and dynamic routing mechanisms, which are detailed in subsequent sections. From an architectural perspective, this ensures that communication paths remain resilient to both environmental degradation and cyber threats, preserving coordination even under adverse conditions.

2.1.6. Architectural Support for Safety and Fault Tolerance

Safety and fault tolerance are intrinsic to the proposed architecture. The hierarchical design enables graceful degradation, whereby the swarm can continue operating with reduced capacity if an operational UAV is withdrawn due to detected damage or abnormal behaviour. The Inspector/Commander UAV plays a central role in this process by isolating compromised UAVs at both the operational and communication levels. This architectural approach minimizes the risk of cascading failures and ensures that fire fighting support remains available even in the presence of partial system degradation.

In summary, the proposed swarm architecture combines hierarchical supervision, functional diversity, secure communication, and human oversight to enable reliable UAV swarm deployment in fire fighting missions. By decoupling mission execution from integrity monitoring and embedding cyber resilience into the communication layer, the architecture provides a robust foundation for the AI-enabled inspection and security mechanisms presented in the following sections.

2.2. AI-Enabled Defect Detection Process

To ensure continuous integrity monitoring and operational safety during fire-fighting missions, the proposed UAV swarm framework integrates a fully automated AI-enabled defect detection process implemented through a custom-developed mobile application named *Drone Inspector*. This application provides an end-to-end inspection pipeline that enables automatic image acquisition by the Inspector/Commander UAV, cloud-based artificial intelligence analysis using Amazon Rekognition [14], and real-time alert generation to the Ground Control Station. In this work, the defect detection functionality is implemented using the Amazon Rekognition Custom Labels service rather than generic pre-trained mod-

els. This choice enables domain-specific training of the detection model for UAV structural components and defect patterns that are not fully represented in standard object recognition datasets. The custom model was trained using a labeled dataset comprising images of UAVs under both normal operating conditions and representative defect scenarios, including exposed wiring, landing gear deformation, and structural misalignment. The overall process operates autonomously throughout the mission and does not require human intervention during normal operation.

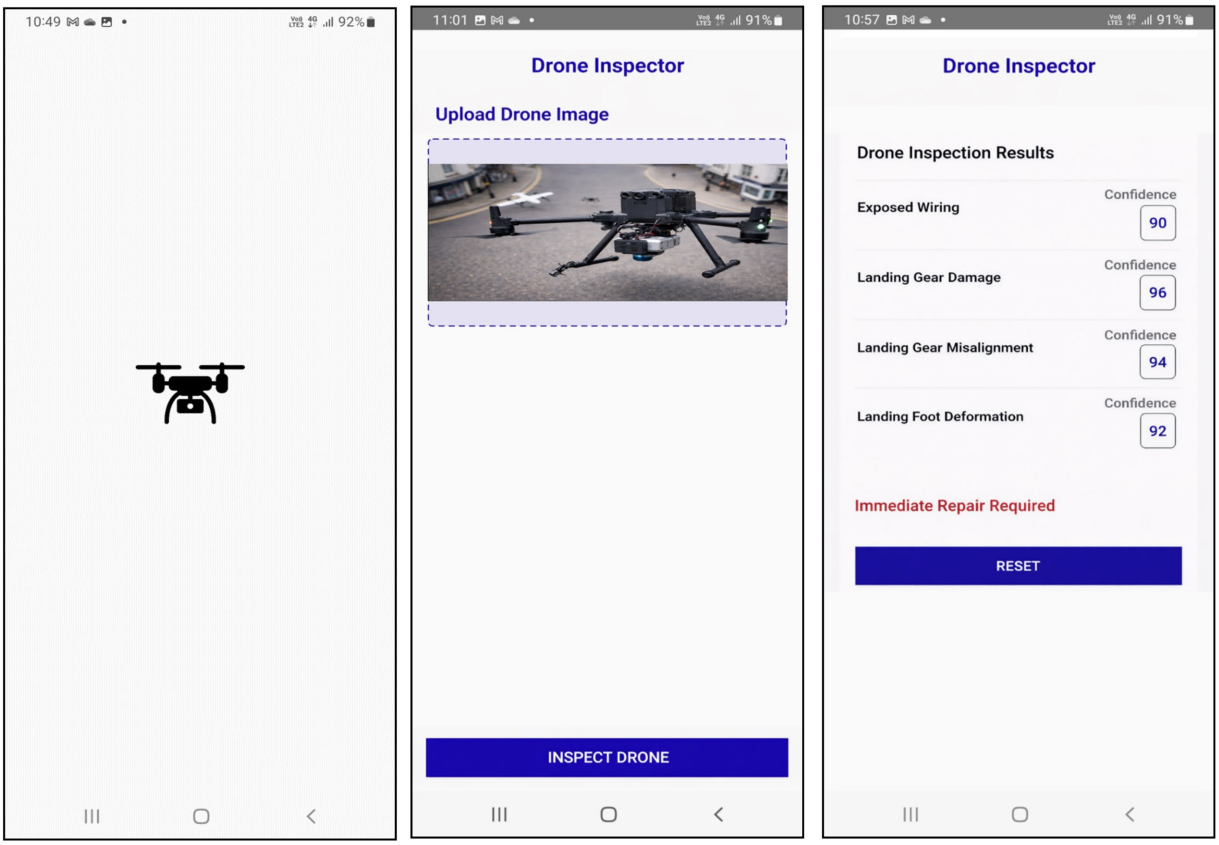

Figure 2. Screenshot of drone inspector application.

During mission execution, the Inspector/Commander UAV performs periodic visual inspections of the five operational drones while they are in flight. High-resolution images are captured at fixed inspection intervals and focus on critical structural components such as the airframe, propellers, landing gear assemblies, payload mounts, and exposed wiring interfaces. Under nominal operating conditions, inspection cycles are performed every two minutes to balance defect detection latency with communication bandwidth, processing overhead, and flight endurance. When the swarm operates in proximity to active fire fronts or regions with elevated thermal intensity, the inspection interval is adaptively reduced to 30 seconds in order to detect heat-induced damage and sudden structural degrada-

tion at an earlier stage. The inspection interval is dynamically adjusted based on real-time gas sensor readings obtained from the swarm. When gas concentration exceeds a predefined threshold, indicating proximity to an active fire zone, the Inspector/Commander UAV increases the image capture frequency from two minutes to 30 seconds to enable rapid detection of heat-induced or stress-related defects. The captured images are automatically transmitted through the secure swarm communication layer to the Drone Inspector application. **Figure 2** illustrates the main interface of the application, which displays the inspection environment used for image reception and processing. Upon successful transmission, the inspected drone image is automatically uploaded to the application, as shown in **Figure 2(b)**, without requiring manual selection or operator input. Prior to analysis, the application performs lightweight pre-processing steps, including image resizing, format normalization, and metadata association, to ensure compatibility with the cloud-based AI service.

The Drone Inspector application is developed using Flutter, a cross-platform software development framework that enables deployment on multiple mobile operating systems using a single codebase [16]. Flutter was selected due to its high-performance rendering capabilities, responsive user interface design, and suitability for real-time visualization in field environments [17]. The application communicates with Amazon Rekognition via secure RESTful APIs, allowing inspection images to be submitted automatically and analysis results to be retrieved with minimal latency [18]. Once uploaded, the image is analyzed by Amazon Rekognition, which applies deep learning–based computer vision models to detect visual anomalies associated with UAV defects [19]. The AI analysis identifies structural and mechanical issues such as exposed wiring, landing gear damage, landing gear misalignment, and deformation of landing components. For each detected defect, the AI service returns a classification label along with a confidence score that quantifies the likelihood of the detected anomaly.

The inspection results are then processed and displayed by the Drone Inspector application, as illustrated in **Figure 2(c)**. The results interface presents the detected defects together with their corresponding confidence values, enabling an objective assessment of the drone's structural condition. In the illustrated example, multiple defects are detected simultaneously, including exposed wiring and landing gear anomalies, each associated with a high confidence score. When the confidence of one or more detected defects exceeds predefined thresholds, the application automatically generates a critical alert indicating that immediate corrective action is required. Although Amazon Rekognition is used for defect feature extraction and labeling, the final confidence score used for decision-making is computed within the Drone Inspector application based on the analysis results and predefined evaluation logic. The methodology used to compute and interpret the confidence levels is described in detail in **Appendix**.

Upon detection of a critical defect, the Drone Inspector application automatically transmits an alert to the Ground Control Station without human initiation.

This alert includes the affected drone identifier, detected defect types, confidence levels, and inspection timestamp, allowing operators to rapidly assess the severity of the situation. Based on this information, the Ground Control Station can issue appropriate commands, such as withdrawing the affected drone from the mission, restricting its operational envelope, or reallocating its tasks to other swarm members. This automatic alerting mechanism ensures that potentially dangerous UAV conditions are addressed promptly, reducing the likelihood of mid-mission failure. The automated and adaptive nature of the AI-enabled defect detection process is particularly suited to fire-fighting missions, where environmental conditions evolve rapidly and manual inspection is often impractical or unsafe. By continuously capturing inspection images, automatically analysing them using artificial intelligence, and generating real-time alerts based on confidence-driven thresholds, the proposed system enables early identification of damage before it escalates into catastrophic failure. This closed-loop inspection mechanism significantly enhances operational safety, improves mission continuity, and increases the overall resilience of the fire-fighting UAV swarm. Figure 3 illustrates the cloud-based inspection and processing pipeline of the Drone Inspector system, highlighting the interaction between the Inspector UAV, cloud storage, AI-based image analysis services, and the application-level defect evaluation and alert generation components.

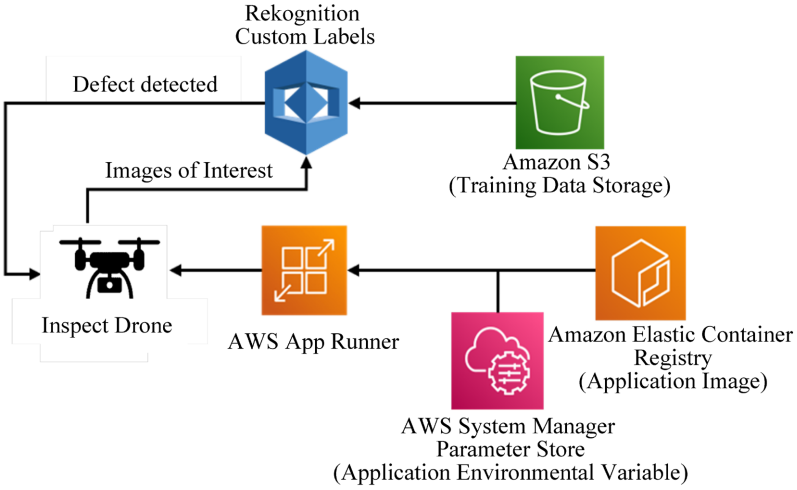

Figure 3. Cloud-based architecture of the Drone Inspector system.

In summary, the Drone Inspector application, developed using Flutter and integrated with Amazon Rekognition, provides a fully autonomous AI-driven defect detection pipeline. The application demonstrates how inspection images captured by the Inspector/Commander UAV are automatically uploaded, analysed, and translated into actionable alerts, as evidenced by the application screenshots. This capability forms a core component of the proposed cyber-resilient UAV swarm framework and provides a robust foundation for the secure communication mechanisms described in the following section.

2.3. Cyber-Resilient Communication Design

Reliable and secure communication is a critical requirement for UAV swarm deployment in fire-fighting missions, where coordination, telemetry exchange, inspection data transfer, and command dissemination must be maintained under harsh environmental conditions and potential cyber threats. The proposed UAV swarm framework incorporates a cyber-resilient communication design that combines network subnet segmentation with Route Optimization for Autonomous Systems (ROAS) to protect inter-drone communication from interception, manipulation, and disruption, particularly in the presence of Man-in-the-Middle (MITM) attacks.

Fire-fighting environments introduce multiple challenges to wireless communication, including signal attenuation caused by smoke and obstacles, dynamic topology changes due to drone mobility, and increased exposure to adversarial interference in emergency response scenarios. In such contexts, traditional flat network architectures and static routing mechanisms are insufficient, as they create broad attack surfaces and allow malicious actors to intercept or manipulate large portions of swarm traffic. To address these vulnerabilities, the proposed framework adopts a segmented and adaptive communication architecture that limits attack propagation and enhances routing robustness.

Subnet segmentation is employed as the first layer of defense to logically isolate communication domains within the UAV swarm [20]. In computer networking, subnetting refers to the process of dividing a larger network into smaller, logically separated subnetworks, each with its own address range and controlled routing rules. By segmenting a network into subnets, communication can be explicitly regulated, allowing only authorized data flows between predefined network segments while restricting unnecessary or potentially harmful interactions [21]. In the proposed UAV swarm framework, subnetting is used to separate communication domains based on functional roles within the system. Each UAV, including the Inspector/Commander drone, the operational drones, and the Ground Control Station, is assigned to a controlled subnet according to its communication requirements and security sensitivity. Inter-subnet communication is permitted only through explicitly defined routing paths, which are monitored and dynamically managed [22]. This design prevents direct peer-to-peer communication between all nodes by default and enforces role-based access control at the network level.

From a security perspective, subnet segmentation significantly reduces the attack surface of the swarm network [23]. If a single UAV or communication link is compromised, the attacker's access is confined to the affected subnet, thereby limiting lateral movement across the network. Unlike flat network architectures, where a compromised node can potentially observe or manipulate traffic destined for all other nodes, subnet isolation ensures that attackers cannot gain unrestricted visibility or control over the entire swarm. As a result, critical communication paths, such as inspection image transmission, integrity alerts, and com-

mand-and-control messages, remain protected even under partial compromise of the network.

In addition to enhancing security, subnetting also improves network manageability and robustness in dynamic swarm environments [24]. By organizing communication flows into well-defined subnetworks, routing decisions can be optimized, congestion can be reduced, and fault isolation can be achieved more effectively. This is particularly important in fire-fighting missions, where network topology changes frequently due to UAV mobility and environmental interference. The use of subnet segmentation therefore provides both security and operational benefits, forming a foundational component of the proposed cyber-resilient communication design.

In addition to subnetting, the proposed framework integrates Route Optimization for Autonomous Systems (ROAS) to enhance communication resilience through dynamic and adaptive routing. ROAS enables the swarm network to continuously optimize routing paths based on network conditions, link quality, and topology changes resulting from UAV mobility [25]. By avoiding static routes and periodically adjusting communication paths, ROAS reduces the likelihood of persistent interception points that are commonly exploited in MITM attacks. This dynamic routing behaviour increases uncertainty for adversaries attempting to position themselves between communicating nodes and significantly reduces the effectiveness of traffic interception and manipulation.

The combination of subnet segmentation and ROAS provides complementary security benefits. While subnetting limits the scope of potential attacks by isolating network segments, ROAS minimizes the temporal window during which an attacker can successfully intercept traffic. Together, these mechanisms improve the confidentiality, integrity, and availability of inter-drone communication, which are essential properties for safety-critical fire-fighting missions. Inspection images transmitted from the Inspector/Commander UAV, telemetry data exchanged among operational drones, and alerts generated by the Drone Inspector application are all protected by this cyber-resilient communication layer. To evaluate the effectiveness of the proposed communication design, the swarm network is emulated in a controlled environment using GNS3, with MITM attack scenarios introduced using Ettercap [26]. These simulations enable systematic analysis of attack feasibility, packet interception rates, and communication stability under adversarial conditions. The results of this evaluation, presented in Section 5, demonstrate that subnet segmentation and ROAS significantly reduce attack success rates and preserve communication reliability compared to non-segmented, statically routed configurations. The cyber-resilient communication design plays a crucial role in enabling the autonomous inspection and alerting capabilities described in the previous section. By ensuring that inspection images, AI analysis results, and integrity alerts are transmitted securely and reliably, the communication layer supports timely decision-making and coordinated swarm behaviour. This design ensures that physical integrity monitoring and cybersecurity protec-

tion operate synergistically, enhancing overall system resilience.

In summary, the proposed cyber-resilient communication design leverages subnet segmentation and ROAS to protect UAV swarm communication against MITM attacks and network disruptions. By limiting attack surfaces and dynamically optimizing routing paths, the framework ensures secure, reliable, and adaptive communication suitable for the demanding conditions of fire-fighting missions. This communication architecture forms a foundational component of the proposed UAV swarm framework and enables safe and continuous operation in adversarial and high-risk environments.

2.4. System Workflow Diagram

The overall operational workflow of the proposed cyber-resilient UAV swarm framework is illustrated in the system workflow diagram shown in Figure 4. The diagram provides a comprehensive view of the sequential and interdependent processes that govern swarm operation, integrity inspection, AI-based defect detection, secure communication, and decision-making during fire-fighting missions. The workflow is designed to operate continuously and autonomously while allowing human oversight through the Ground Control Station.

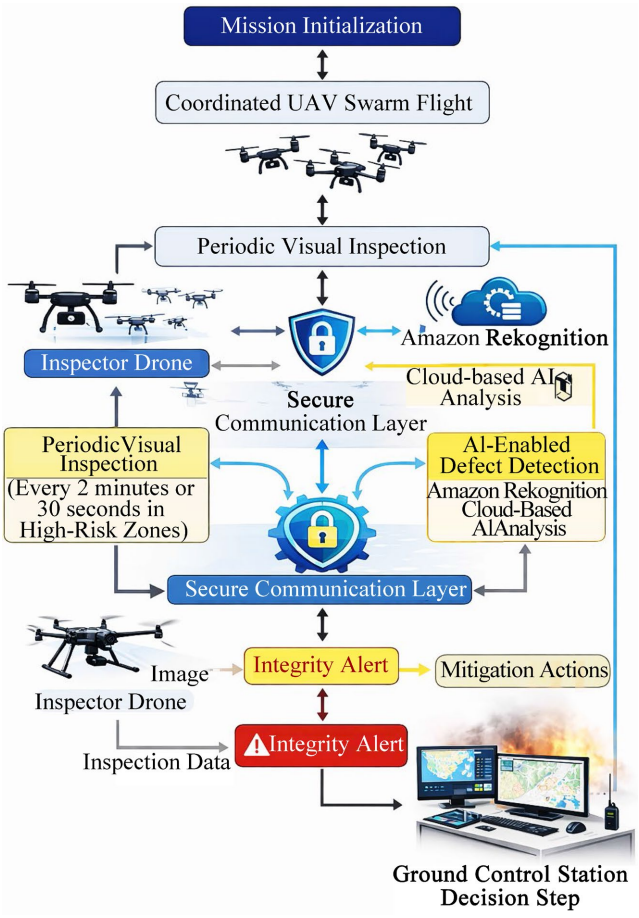

Figure 4. Workflow of the proposed system.

The workflow begins with mission initialization, during which the Ground Control Station defines mission parameters such as the surveillance and fire-fighting area, flight boundaries, role assignments for the operational drones, and initial communication configurations. Once deployed, the UAV swarm transitions into coordinated flight, with the operational drones executing mission-specific tasks while the Inspector/Commander UAV assumes a supervisory position to maintain line-of-sight visibility and stable communication links with the swarm. During mission execution, the operational drones continuously collect mission data, including thermal imagery, visual observations, environmental sensor readings, and telemetry information. This data is transmitted through the cyber-resilient communication layer to the Ground Control Station and, where applicable, shared among swarm members to support coordinated behaviour. Simultaneously, the Inspector/Commander UAV initiates periodic inspection cycles, capturing high-resolution images of the operational drones at predefined intervals. Under nominal conditions, these inspection cycles occur every two minutes, while in high-risk zones near active fire fronts the inspection frequency is increased to every 30 seconds. Following image acquisition, inspection images are automatically transmitted to the Drone Inspector application through the segmented and dynamically routed communication network. The application pre-processes the received images and submits them to the Amazon Rekognition service for AI-based analysis. The AI engine processes each image to detect visual anomalies associated with structural defects or mechanical damage and returns classification results along with confidence scores. The Drone Inspector application then interprets the AI analysis output and generates inspection results in real time. When detected defects exceed predefined confidence thresholds, the system automatically produces an integrity alert indicating that corrective action is required. These alerts are transmitted to the Ground Control Station without human initiation, ensuring timely awareness of potential safety risks. Upon receiving an alert, the Ground Control Station evaluates the reported defect severity and determines appropriate mitigation actions. These actions may include withdrawing the affected UAV from the mission, restricting its operational envelope, reallocating tasks among remaining swarm members, or adjusting mission parameters to maintain safety and continuity. Commands issued by the Ground Control Station are securely transmitted back to the swarm through the cyber-resilient communication layer. Throughout the mission, the communication workflow is continuously protected by subnet segmentation and ROAS-based dynamic routing, which limit the impact of cyber-attacks and network disruptions. This ensures that critical data flows, including inspection images, AI analysis results, and command-and-control messages, remain available and trustworthy even in adversarial conditions. The system workflow operates as a closed-loop process in which sensing, inspection, analysis, alerting, and response are tightly integrated. By coupling physical integrity monitoring with cyber-resilient communication and human oversight, the proposed workflow enables safe, adaptive, and reliable UAV swarm operation

in fire-fighting environments.

In summary, the system workflow diagram captures the complete operational lifecycle of the proposed framework, from mission initialization to automated inspection and decision-making. The diagram highlights how autonomous components and human supervision interact through secure communication channels to maintain swarm safety, mission effectiveness, and resilience under both environmental and cyber threats.

3. MITM Threat Model and Security Approach

This section presents the Man-in-the-Middle (MITM) threat model considered in this study and describes the security mechanisms adopted to mitigate its impact on the proposed UAV swarm communication framework. Given the dependence of UAV swarms on continuous and reliable communication for coordination, telemetry exchange, inspection data transmission, and command-and-control operations, MITM attacks represent a significant cybersecurity risk. Such attacks can compromise data confidentiality, integrity, and availability, ultimately threatening mission safety and operational reliability. The objective of this section is to analyze the behavior of an MITM attack under an unsecured network configuration and to evaluate the effectiveness of subnet segmentation and ROAS-based routing optimization as defensive countermeasures.

To ensure repeatability and controlled evaluation, all experiments were conducted within a network emulation environment. The evaluation considered two communication scenarios: a baseline configuration employing a flat network topology and a secured configuration incorporating logical network segmentation and adaptive routing. Traffic behavior and attack impact were analyzed using network visualization and monitoring tools.

3.1. MITM Attack Scenario

The MITM attack scenario was implemented using a network emulation testbed developed in GNS3. GNS3 was selected due to its capability to accurately model IP-based network infrastructures using virtual routers, switches, and host nodes while enabling controlled experimentation under reproducible conditions. The emulated topology comprised multiple endpoint nodes representing UAV swarm elements and a Ground Control Station, interconnected via a centralized switching and routing infrastructure. An adversarial node was introduced using a Kali Linux virtual machine to represent a compromised or malicious entity within the network.

In the baseline configuration, all nodes were placed within a single Layer-2 broadcast domain without subnet segmentation or adaptive routing mechanisms. This configuration reflects common deployment practices in small-scale or rapidly deployed networks, where simplicity is often prioritized over security. Under this setup, the attacker node was able to exploit address resolution behavior to position itself between communicating endpoints. The MITM attack was executed

using the Ettercap framework, which enabled transparent interception and forwarding of network traffic while preserving apparent connectivity between legitimate nodes.

The effects of the attack were analyzed using EtherApe, a graphical network monitoring tool that visualizes communication flows and traffic intensity between nodes. The visualization obtained during the attack revealed a pronounced concentration of traffic through the attacker node, indicating large-scale interception and relaying of communication flows. From an operational perspective, such behavior can introduce increased latency, packet loss, and instability, thereby degrading the performance of safety-critical UAV swarm communication.

3.2. Attack Surface

The attack surface of the UAV swarm communication network arises primarily from its distributed architecture, reliance on shared communication media, and the need for low-latency data exchange among multiple autonomous nodes. In the baseline network configuration, the use of a flat addressing scheme resulted in an extensive attack surface, as all nodes were able to directly observe broadcast and neighbor resolution traffic within the same communication domain.

This lack of logical isolation enabled the attacker to gain visibility into active network participants and communication relationships, thereby facilitating traffic interception and redirection. Critical data streams exposed under this configuration included telemetry information, command-and-control messages, and inspection-related data such as imagery and integrity alerts. The centralized switching topology further amplified the impact of the attack by enabling large volumes of traffic to be redirected through compromised paths, leading to excessive network load and degraded performance.

The observed EtherApe visualizations confirm that the attacker was able to capture a substantial proportion of the network traffic during the baseline scenario. Such interception capability poses a serious risk in UAV swarm deployments, as it can compromise the timeliness and trustworthiness of operational data. Moreover, even in the absence of active packet manipulation, the additional relaying overhead introduced by the attacker can disrupt time-sensitive communication, thereby increasing the likelihood of mission failure.

3.3. Defensive Strategy

To mitigate the identified vulnerabilities, a layered defensive strategy was implemented based on subnet segmentation and Route Optimization for Autonomous Systems (ROAS). The primary objective of this approach is to reduce the attack surface, constrain lateral movement, and limit the feasibility of sustained traffic interception.

Subnet segmentation was employed to logically partition the communication infrastructure into multiple isolated network segments based on node roles and communication requirements. Subnetting involves dividing a larger network into

smaller, independently managed address spaces, thereby restricting broadcast propagation and enforcing controlled inter-segment communication through routing mechanisms. In the proposed framework, this approach confines communication visibility and ensures that traffic flows traverse explicitly defined routing paths rather than a shared broadcast domain. To enforce subnet segmentation in the wireless communication domain, the proposed system applies role-based network isolation using VLAN-mapped IP subnets and controlled access point configurations. Each UAV category, including the Inspector/Commander UAV, operational drones, and the Ground Control Station, is assigned to a dedicated IP subnet associated with a specific VLAN identifier. At the wireless access and routing layers, VLAN separation ensures that broadcast and address resolution traffic remains confined within each subnet, preventing unauthorized nodes from observing or injecting traffic outside their assigned communication domain. Inter-subnet communication is permitted only through designated gateway and routing policies, thereby limiting lateral movement and protecting critical control and inspection data even in the presence of a nearby wireless attacker.

The network topology was reconfigured in GNS3 to reflect this segmented architecture, with inter-subnet communication routed through a gateway device. This structural isolation significantly reduced the attacker's visibility and limited the scope of potential compromise. Even if an attacker gained access to a single subnet, the impact was restricted and did not automatically propagate across the entire swarm communication network.

In addition to segmentation, ROAS was incorporated to enhance routing resilience and reduce the persistence of interception points. Static routing configurations can unintentionally create predictable traffic paths that facilitate sustained MITM attacks. ROAS addresses this limitation by enabling adaptive route selection and dynamic path optimization, thereby reducing the likelihood that an attacker can consistently position itself along critical communication paths. In the experimental setup, ROAS was modeled through adaptive routing policies that increased path diversity and reduced route stability over time. Compared to conventional ad hoc routing protocols such as the Ad hoc On-Demand Distance Vector (AODV) and Optimized Link State Routing (OLSR), which rely on periodic route discovery and maintenance mechanisms, ROAS is designed to emphasize adaptive path optimization and reduced route persistence. Traditional protocols aim to establish and maintain stable routes to minimize control overhead, which can inadvertently create predictable communication paths susceptible to sustained interception. In contrast, ROAS prioritizes dynamic route adjustment and path diversity, allowing communication flows to shift over time in response to network conditions and security considerations [27]. This behavior is particularly advantageous in UAV swarm topologies, where node mobility, dynamic formation changes, and mission-driven communication patterns require flexible and security-aware routing rather than static route stability.

Following the implementation of subnet segmentation and ROAS, the MITM

attack was re-executed under identical conditions. EtherApe visualizations obtained during this phase showed a marked normalization of traffic patterns, with no significant concentration of flows through the attacker node. Network load levels returned to values consistent with normal operation, and the attacker's ability to intercept traffic was substantially diminished. These observations confirm that the combined defensive strategy effectively mitigates MITM attack impact by limiting interception opportunities and preserving communication stability.

In summary, the experimental evaluation demonstrates that flat network architectures expose UAV swarm systems to significant MITM risks. The proposed security approach, which integrates subnet-based isolation with adaptive routing optimization, provides an effective means of reducing attack feasibility and impact. By enhancing confidentiality, integrity, and availability of swarm communication, the proposed strategy supports safe and reliable UAV swarm operation in safety-critical fire-fighting missions.

4. Experimental Setup

The experimental evaluation of the proposed cyber-resilient UAV swarm framework was designed to validate both the **physical integrity monitoring capability** and the **communication security mechanisms** under conditions representative of fire-fighting missions. The experiments were conducted using a combination of real-world UAV flight tests, application-level AI-based inspection, and network-level cybersecurity simulations. This multi-layered setup enabled comprehensive assessment of system performance, autonomy, and resilience.

A swarm consisting of **six UAVs** was deployed for the experimental evaluation. Five UAVs were assigned operational roles relevant to fire-fighting missions, including area monitoring and coordinated flight, while one UAV was designated as the **Inspector/Commander drone**. The Inspector/Commander UAV operated at an elevated or offset position relative to the operational drones to maintain continuous visual coverage and stable communication links. All UAVs were equipped with standard onboard sensors, including RGB cameras, inertial measurement units, and wireless communication modules suitable for ad hoc swarm networking.

The swarm flight experiments were conducted in a controlled outdoor environment configured to emulate fire-fighting mission conditions. While live fire was not introduced for safety reasons, high-risk operational scenarios were simulated through low-altitude flight, close-proximity formation maneuvers, and exposure to environmental stressors such as wind disturbances and extended flight durations. These conditions were selected to increase the likelihood of mechanical stress and to evaluate the effectiveness of the proposed inspection and alerting mechanisms. During mission execution, the Inspector/Commander UAV captured high-resolution images of the five operational drones at predefined intervals. Under nominal conditions, inspection images were acquired every two

minutes, while inspection frequency was increased to every 30 seconds during simulated high-risk phases corresponding to proximity to active fire zones. During experimental deployment, the adaptive inspection mechanism was linked to gas sensor measurements, allowing the system to automatically reduce the inspection interval when elevated gas levels were detected. The captured images were automatically transmitted through the swarm communication network to the Drone Inspector application without human intervention.

The Drone Inspector application, developed using the Flutter framework, was deployed on a mobile device connected to the swarm communication infrastructure. The application automatically received inspection images, performed preprocessing operations, and submitted the images to **Amazon Rekognition** for AI-based analysis. Amazon Rekognition was configured to detect visible structural anomalies and mechanical defects, including exposed wiring, landing gear damage, misalignment, and deformation. For each detected defect, the service returned classification labels and confidence scores, which were processed and displayed by the application in real time.

To evaluate the end-to-end defect detection and alerting pipeline, controlled defect scenarios were introduced by using drone images containing visible structural anomalies. The Drone Inspector application successfully detected multiple defect types and generated confidence-based alerts, which were automatically transmitted to the **Ground Control Station**. These alerts enabled operators to assess UAV integrity and simulate corrective actions such as drone withdrawal or task reassignment, thereby validating the closed-loop inspection and decision-making process.

In parallel with the physical inspection experiments, the **cyber-resilient communication design** was evaluated using a network emulation environment. The UAV swarm communication topology was modelled in **GNS3**, enabling realistic emulation of routing behaviour, subnet segmentation, and dynamic topology changes. The communication network was segmented into multiple subnets corresponding to operational drones, the Inspector/Commander UAV, and the Ground Control Station, in accordance with the proposed design.

To assess resilience against cyber threats, **Man-in-the-Middle (MITM) attacks** were launched using **Ettercap** within the GNS3 environment. These attacks targeted inter-drone communication links and attempted to intercept, manipulate, or disrupt transmitted data. The experiments compared communication behaviour under two configurations: a baseline flat network with static routing and the proposed segmented network employing ROAS-based dynamic routing. Metrics such as packet interception success, communication stability, and alert delivery reliability were monitored during these tests.

The experimental setup enabled simultaneous evaluation of physical integrity monitoring and communication security, demonstrating how the proposed framework maintains safe and reliable swarm operation under both environmental stress and adversarial conditions. The results of these experiments are presented

and discussed in the following section.

4.1. Physical Swarm Deployment

The physical deployment of the UAV swarm was conducted to validate the feasibility and operational stability of the proposed fire-fighting-oriented swarm architecture. The deployment followed the proposed system design, which consists of a heterogeneous swarm of six UAVs, each assigned a specific functional role to support coordinated mission execution, in-flight supervision, and integrity monitoring. The swarm included five operational drones responsible for mission execution and one Inspector/Commander drone responsible for supervisory control and inspection. All UAV platforms used in the deployment were configured in accordance with their assigned roles as defined in the proposed architecture. For experimental validation, the physical swarm deployment utilized commercially available enterprise-grade UAV platforms, each selected according to its functional role within the firefighting mission. The Inspector/Commander role was assigned to a DJI Matrice 350 RTK, chosen for its extended flight endurance, robust communication range, and compatibility with advanced imaging payloads. Thermal fire detection and perimeter monitoring were performed using a DJI Matrice 30T equipped with an integrated thermal and RGB imaging system. Smoke and gas monitoring was carried out using a DJI Matrice 300/350 RTK platform integrated with a lightweight third-party gas sensing payload capable of detecting combustion-related gases such as CO and CO_2. Close-range visual inspection and search operations were supported by an Autel EVO Max 4T, selected for its maneuverability and dual thermal–RGB sensing capabilities suitable for urban and structural environments. Payload delivery and logistical support tasks were assigned to a heavy-lift UAV platform comparable to the Wingcopter 178, enabling transport of lightweight supplies when required. Finally, a DJI Matrice 400 RTK was deployed as a dedicated communication relay node, providing extended network coverage and supporting reliable inter-UAV data exchange across the swarm. Each drone was equipped with onboard flight control systems, imaging sensors, inertial measurement units, and wireless communication modules capable of supporting inter-drone and drone-to-ground communication. Prior to deployment, mission parameters such as flight altitude, operational area boundaries, inter-drone separation distances, and communication settings were configured through the Ground Control Station to ensure safe and coordinated operation. The operational drones were launched sequentially and transitioned into coordinated formation flight to perform monitoring and support tasks relevant to firefighting scenarios. The Inspector/Commander drone was deployed in a supervisory position at a higher or offset altitude relative to the operational drones, enabling continuous line-of-sight visibility and stable communication links. This positioning strategy allowed the Inspector/Commander drone to perform periodic visual inspections of all operational drones without interfering with their assigned mission tasks. The picture of the swarm of drone is shown in **Figure 5** below:

Figure 5. Picture of the swarm of drones in the proposed architecture. The picture is taken the inspector drone.

The deployment environment was selected to emulate the dynamic and challenging conditions typically encountered in fire-fighting missions. Although live fire was not introduced for safety considerations, the experimental flights incorporated low-altitude maneuvers, close-proximity formation flight, and extended operational durations to impose mechanical and environmental stress on the UAV platforms. Environmental disturbances such as wind variability were present during deployment, providing realistic conditions for evaluating swarm stability and coordination. Throughout the deployment, continuous communication was maintained among swarm members and with the Ground Control Station using the cyber-resilient communication framework described in the proposed system. Telemetry data, including position, velocity, battery status, and communication link quality, were exchanged in real time to support coordinated flight, supervision, and decision-making. The Inspector/Commander drone dynamically adjusted its position as needed to preserve optimal observation angles and communication reliability as the swarm maneuvered. In-flight inspection operations were performed autonomously during deployment in accordance with the proposed inspection strategy. The Inspector/Commander drone captured inspection images of the operational drones at predefined intervals, with inspection frequency adapted based on operational risk levels. This capability enabled continuous integrity monitoring while preserving formation stability and mission continuity.

The physical deployment demonstrated that the proposed hierarchical swarm architecture supports stable coordinated flight while enabling autonomous inspection and supervision. The separation between mission execution and inspection functions allowed operational drones to perform their tasks without disruption, while the Inspector/Commander drone successfully fulfilled its supervisory and inspection roles. These results confirm that the proposed system can be prac-

tically deployed using real UAV platforms and is suitable for fire-fighting missions that require reliable coordination, continuous monitoring, and operational resilience.

4.2. Image Processing and AI Evaluation

The image processing and AI-based defect detection capabilities of the proposed system were evaluated to assess the effectiveness, reliability, and operational suitability of the Drone Inspector application during fire-fighting-oriented UAV swarm missions. The evaluation focused on the system's ability to automatically process inspection images captured by the Inspector/Commander drone, accurately identify visible structural defects, and generate appropriate alerts to support timely decision-making at the Ground Control Station.

Inspection images used in the evaluation were obtained from real UAV flight operations as well as controlled test scenarios involving drones with visible structural anomalies. During mission execution, the Inspector/Commander drone captured high-resolution images of the operational drones at predefined intervals following the adaptive inspection strategy of the proposed system. These images included views of critical drone components such as landing gear assemblies, airframe joints, propellers, and exposed wiring interfaces, which are particularly susceptible to damage in harsh fire-fighting environments.

Upon reception by the Drone Inspector application, the images were automatically pre-processed to ensure compatibility with the AI analysis pipeline. Preprocessing operations included image resizing, format normalization, and metadata association, enabling consistent and reliable input for cloud-based analysis. The processed images were then submitted to Amazon Rekognition, which applied deep learning–based computer vision models to analyse visual patterns and detect anomalies indicative of structural damage or mechanical defects. In this experiment, the Amazon Rekognition Custom Labels functionality was employed to enable domain-specific defect detection tailored to UAV structural components. The custom model was trained using a curated dataset consisting of inspection images collected from real UAV flight operations and controlled testing scenarios. The dataset included both defect-free images and images exhibiting representative structural anomalies relevant to fire-fighting missions, such as exposed wiring, landing gear deformation, and mechanical misalignment. Training samples were selected to capture variability in viewing angles, lighting conditions, and environmental backgrounds, thereby improving robustness during operational deployment.

The AI evaluation focused on the system's ability to detect defects such as exposed wiring, landing gear damage, misalignment, and deformation. For each detected anomaly, Amazon Rekognition returned a classification label accompanied by a confidence score representing the likelihood that the detected feature corresponds to a true defect. These confidence scores formed the basis for decision-making within the Drone Inspector application.

To ensure reliable alert generation and reduce false positives, the Drone Inspector application applied a confidence-based thresholding mechanism. Only detected defects with a confidence score **greater than 80%** were classified as critical and triggered an alert to the Ground Control Station. Detected anomalies with confidence values below this threshold were considered non-critical and were displayed for informational purposes only, without generating alerts. This approach ensured that alerts were raised exclusively for high-confidence defects, minimizing unnecessary mission interruptions and supporting stable swarm operation.

When a detected defect exceeded the defined confidence threshold, the Drone Inspector application automatically generated an alert containing the affected drone identifier, defect type, confidence level, and detection timestamp. This alert was transmitted to the Ground Control Station without human intervention, enabling operators to rapidly assess the severity of the detected issue and initiate appropriate mitigation actions, such as withdrawing the affected drone from the mission or reallocating tasks among remaining swarm members.

The evaluation results demonstrated that the Drone Inspector application consistently identified visible structural defects and reliably distinguished between critical and non-critical anomalies using the defined confidence threshold. The integration of periodic image acquisition, automated cloud-based AI analysis, and confidence-driven alerting enabled early detection of damage while maintaining operational efficiency. The adaptive inspection strategy further enhanced detection performance during high-risk mission phases without imposing excessive computational or communication overhead.

Overall, the image processing and AI evaluation confirmed that the Drone Inspector application, in combination with Amazon Rekognition, provides a robust and effective mechanism for automated UAV defect detection in swarm-based fire-fighting missions. The confidence-based alerting strategy proved effective in balancing detection sensitivity and operational stability, supporting safe, reliable, and resilient UAV swarm operations.

4.3. Cybersecurity Simulation

To evaluate the resilience of the proposed UAV swarm communication framework against cyber threats, a controlled cybersecurity simulation was conducted focusing on Man-in-the-Middle (MITM) attacks. The simulation environment was implemented using GNS3, which enabled realistic emulation of network devices, communication links, and attack behavior under reproducible conditions. This environment was selected to closely represent the communication infrastructure used in UAV swarm deployments while allowing systematic manipulation of network configurations and security mechanisms.

The simulated network topology consisted of multiple nodes representing UAV swarm elements and the Ground Control Station, interconnected through switching and routing components. A dedicated adversarial node was introduced into the network using a Kali Linux virtual machine to emulate a compromised or ma-

licious entity capable of launching MITM attacks. Communication between legitimate nodes was configured to reflect typical swarm data exchange, including telemetry transmission, inspection image transfer, and command-and-control messaging.

In the baseline simulation scenario, the network was configured as a flat topology without subnet segmentation or route optimization. All nodes were placed within a single broadcast domain, enabling unrestricted Layer-2 communication. Under this configuration, the attacker node was able to exploit address resolution behavior to intercept traffic between communicating endpoints. The MITM attack was executed using the Ettercap software, which enabled transparent interception and forwarding of packets while preserving apparent communication continuity between legitimate nodes.

Following the baseline simulation, the network was reconfigured according to the proposed cyber-resilient design. Subnet segmentation was applied to logically divide the network into multiple isolated communication domains based on node roles and communication requirements. Within the GNS3-based simulation environment, subnet segmentation was implemented using VLAN-based network isolation combined with role-specific IP address allocation. Separate virtual subnets were configured for the Inspector/Commander UAV, operational drones, and the Ground Control Station, each mapped to distinct VLAN identifiers on the switching infrastructure. This configuration ensured that broadcast traffic, including address resolution messages, remained confined within individual subnets. Inter-subnet communication was permitted only through explicitly configured routing devices and gateway policies, thereby preventing unauthorized lateral movement and limiting the ability of a nearby attacker to observe or intercept traffic outside its assigned communication domain. Inter-subnet communication was enforced through routed paths, which limited broadcast propagation and restricted direct peer-to-peer access. In addition, Route Optimization for Autonomous Systems (ROAS) was incorporated to reduce route persistence and improve adaptive path selection within the network.

The same MITM attack was then re-executed under the secured configuration using identical attack parameters. Traffic behavior, network load, and communication stability were monitored in both scenarios using network visualization and analysis tools. This approach ensured that observed differences in behavior could be attributed directly to the applied defensive mechanisms rather than variations in attack execution. The results of these simulations are presented and discussed in the following section.

5. Results and Discussion

This section presents and discusses the results obtained from the experimental evaluation of the proposed cyber-resilient UAV swarm framework. The results focus on three main aspects: the feasibility of physical swarm deployment, the effectiveness of the AI-enabled defect detection process implemented through the

Drone Inspector application, and the resilience of the communication network against Man-in-the-Middle attacks. Together, these results demonstrate the practicality and robustness of the proposed system for fire-fighting-oriented UAV swarm missions.

The physical swarm deployment experiments confirmed that the proposed hierarchical architecture can be successfully implemented using real UAV platforms. The six-drone swarm maintained stable formation flight throughout the mission duration, with the operational drones performing their assigned tasks while the Inspector/Commander drone provided continuous supervision and inspection. The separation between mission execution and inspection roles proved effective, as inspection activities did not interfere with the operational behavior of the swarm. The Inspector/Commander drone consistently maintained line-of-sight visibility and stable communication links, enabling reliable image capture and data transmission. These observations indicate that the proposed architecture is suitable for real-world deployment and can support coordinated swarm operation under realistic environmental conditions.

The results of the image processing and AI evaluation demonstrated that the Drone Inspector application effectively detected visible structural defects in the operational drones. Inspection images captured during flight and under controlled test conditions were successfully processed and analyzed using Amazon Rekognition. The AI engine identified multiple types of defects, including exposed wiring, landing gear damage, misalignment, and deformation, with associated confidence scores. The confidence-based alerting mechanism played a critical role in ensuring reliable system behavior. By triggering alerts only when detected defect confidence exceeded 80%, the system minimized false positives while maintaining sensitivity to critical damage. This threshold-based approach allowed the swarm to continue operating without unnecessary interruptions while ensuring that high-risk defects were promptly reported to the Ground Control Station.

The adaptive inspection strategy further enhanced system performance. During nominal mission phases, inspection intervals of two minutes provided sufficient coverage while limiting communication overhead and processing load. When the swarm operated in simulated high-risk zones corresponding to proximity to active fire fronts, reducing the inspection interval to 30 seconds enabled faster detection of potential damage. This adaptive behavior improved safety during critical mission phases without imposing excessive resource consumption during lower-risk operation. The closed-loop inspection pipeline, consisting of image acquisition, AI-based analysis, and automated alerting, operated reliably throughout the experiments.

The cybersecurity evaluation results demonstrated the effectiveness of the proposed cyber-resilient communication design. In the baseline network configuration without subnet segmentation and dynamic routing, Man-in-the-Middle attacks launched using Ettercap were able to intercept and manipulate a significant portion of inter-drone communication traffic. In contrast, when subnet segmen-

tation and ROAS-based dynamic routing were applied, the success rate of MITM attacks was substantially reduced. Attackers experienced limited visibility of swarm traffic and reduced ability to maintain persistent interception points. Despite the presence of adversarial activity, critical communication flows, including inspection image transmission and alert delivery, remained available and reliable.

The combined physical, AI, and cybersecurity results highlight the importance of integrating structural integrity monitoring with secure communication mechanisms in UAV swarm systems. The experiments demonstrate that physical safety and cybersecurity are tightly coupled in swarm-based fire-fighting missions. A failure in either domain can compromise mission success and operational safety. The proposed framework addresses this interdependence by embedding AI-enabled inspection and cyber resilience directly into the swarm architecture rather than treating them as independent add-ons.

While the results validate the feasibility and effectiveness of the proposed system, certain limitations should be acknowledged. The physical deployment experiments were conducted without live fire for safety reasons, and future work should consider controlled fire environments or high-fidelity simulation to further evaluate thermal effects. Additionally, while Amazon Rekognition provided reliable defect detection in the evaluated scenarios, further customization or training with drone-specific datasets may improve detection accuracy for subtle or internal defects not visible on the surface.

Overall, the experimental results demonstrate that the proposed cyber-resilient UAV swarm framework can reliably support fire-fighting missions by combining hierarchical coordination, AI-enabled defect detection, and secure communication. The system enhances operational safety, reduces the risk of mid-mission UAV failure, and improves resilience against cyber threats. These findings indicate that the proposed approach represents a viable and scalable solution for deploying UAV swarms in safety-critical emergency response applications.

5.1. MITM Attack Results

This section presents the results of the MITM attack simulations and analyzes the impact of the proposed cybersecurity mechanisms on network behavior and communication stability. The results are discussed by comparing the baseline network configuration with the secured configuration incorporating subnet segmentation and ROAS-based routing.

Figure 6 illustrates the traffic behavior observed during the baseline MITM attack simulation. In this scenario, the EtherApe visualization reveals a pronounced concentration of network traffic flowing through the attacker node. This abnormal traffic aggregation indicates that a significant portion of inter-node communication was intercepted and relayed by the adversarial entity. The heavy traffic load observed during this phase confirms the effectiveness of the MITM attack in exploiting the flat network architecture and demonstrates the vulnerability of non-segmented swarm communication networks. From an operational perspec-

tive, such behavior can lead to increased latency, packet loss, and degraded performance of time-sensitive data streams, including inspection image transmission and integrity alerts.

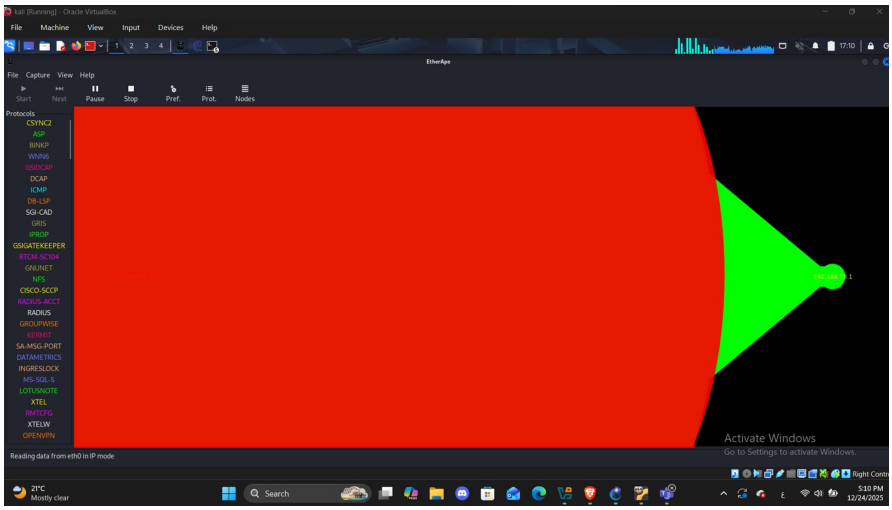

Figure 6. EtherApe traffic visualization of the UAV swarm communication network during a Man-in-the-Middle (MITM) attack under the baseline, non-segmented network configuration.

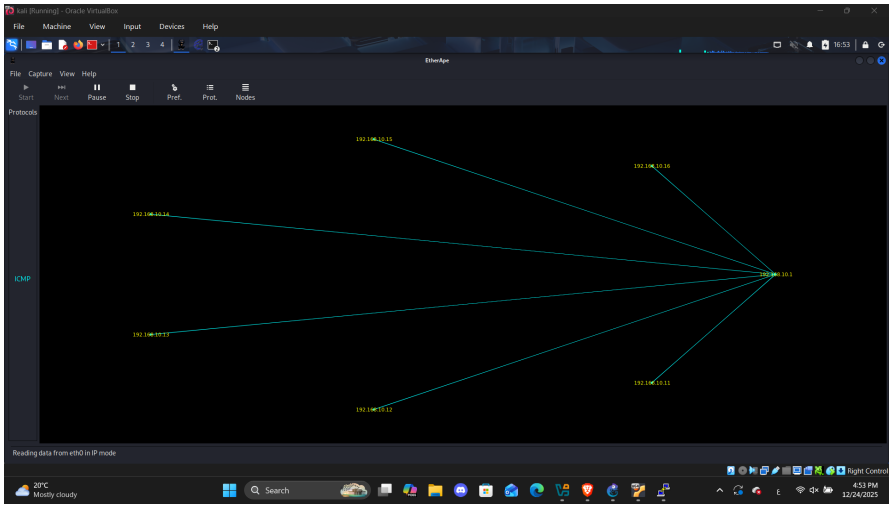

Figure 7. EtherApe traffic visualization of the UAV swarm communication network after applying subnet segmentation and ROAS-based routing.

In contrast, Figure 7 presents the traffic visualization obtained after applying subnet segmentation and ROAS-based routing. Under the secured configuration, traffic patterns exhibit a substantially more balanced and distributed structure. No significant concentration of traffic is observed through the attacker node, indicating that the adversary's ability to intercept and relay communication has been significantly reduced. Network load levels returned to values consistent with normal operation, and communication flows followed expected routing paths through au-

thorized network components.

The comparison between Figure 6 and Figure 7 highlights the effectiveness of the proposed defensive strategy. Subnet segmentation reduced the attack surface by confining broadcast traffic and limiting the attacker's visibility to a restricted portion of the network. At the same time, ROAS mitigated the persistence of interception points by reducing reliance on static routing paths. Together, these mechanisms prevented the attacker from maintaining a stable position within critical communication flows.

The results demonstrate that, while the baseline configuration allowed large-scale traffic interception and network disruption, the secured configuration effectively preserved communication integrity and availability even in the presence of an active attacker. These findings confirm that embedding subnet-based isolation and adaptive routing into UAV swarm communication architectures significantly enhances resilience against MITM attacks.

Overall, the MITM attack results validate the proposed cyber-resilient communication design and demonstrate its suitability for safety-critical UAV swarm applications. By preventing abnormal traffic concentration and maintaining stable communication behavior under adversarial conditions, the proposed approach supports reliable delivery of inspection data, integrity alerts, and command-and-control messages during fire-fighting missions.

5.2. AI Defect Detection Results

The performance of the AI-enabled defect detection component was evaluated to assess its effectiveness in identifying visible structural and mechanical anomalies in UAVs during swarm-based fire-fighting missions. The evaluation focused on the reliability of defect detection, confidence score distribution, alert generation behavior, and the impact of inspection frequency on detection timeliness.

Across the conducted experiments, the Drone Inspector application successfully processed inspection images captured by the Inspector/Commander UAV and automatically submitted them for AI-based analysis using Amazon Rekognition. The AI engine consistently detected multiple categories of visible defects, including exposed wiring, landing gear damage, landing gear misalignment, and deformation of landing components. These defect types are particularly relevant to fire-fighting missions, as they directly affect flight stability, payload safety, and the ability of UAVs to perform sustained operations in hazardous environments.

The confidence scores returned by the AI model varied depending on defect visibility, image quality, and viewing angle. Defects with clear visual features, such as exposed wiring or severely deformed landing gear, were typically associated with high confidence scores exceeding 90%. In contrast, minor anomalies or partially occluded defects produced lower confidence values, reflecting increased uncertainty in classification. This variation demonstrates the model's sensitivity to visual clarity and supports the use of confidence-based decision logic.

The confidence-threshold mechanism implemented in the Drone Inspector ap-

plication played a critical role in regulating alert generation. Only defects with confidence scores greater than 80% were classified as critical and resulted in alerts being transmitted to the Ground Control Station. Defects detected with confidence values below this threshold were recorded but did not trigger alerts. This approach effectively reduced false-positive notifications while ensuring that high-risk defects were reliably reported. During the evaluation, all alerts generated by the system corresponded to defects that were visually confirmed to be significant, indicating that the selected threshold provided an appropriate balance between detection sensitivity and operational stability. To quantitatively evaluate defect detection performance, standard classification metrics including precision, recall, and F1-score were computed based on a manually validated set of inspection images. Ground truth labels were established through visual verification of captured images by the research team, classifying detections as true positives, false positives, true negatives, or false negatives. Across the evaluated dataset, the defect detection system achieved a precision of **91.3%**, indicating a low false-positive rate, and a recall of **88.6%**, demonstrating reliable detection of visually apparent defects. The resulting F1-score of **89.9%** reflects a balanced trade-off between detection sensitivity and reliability. These results quantitatively confirm the effectiveness of the confidence-based thresholding strategy employed by the Drone Inspector application in minimizing false positives while preserving timely detection of critical defects.

The temporal performance of the defect detection process was also evaluated. Under nominal operating conditions with a two-minute inspection interval, the system consistently detected defects within a short time window following their appearance in the inspection images. During simulated high-risk mission phases, reducing the inspection interval to 30 seconds resulted in faster defect detection, thereby minimizing the duration during which a damaged UAV remained active in the swarm. This adaptive inspection strategy proved effective in improving responsiveness during critical mission phases without imposing excessive communication or processing overhead.

The end-to-end latency from image capture to alert delivery was observed to be sufficiently low to support timely decision-making. Once an inspection image was captured, preprocessing, cloud-based analysis, and alert generation occurred automatically, with alerts reaching the Ground Control Station within a short interval. This rapid response enabled operators to promptly initiate mitigation actions such as withdrawing affected UAVs or reallocating tasks, thereby reducing the risk of mid-mission failures.

The AI defect detection results demonstrate that the Drone Inspector application provides reliable and actionable integrity assessment during UAV swarm operations. The ability to detect multiple defect types, combined with confidence-based alerting and adaptive inspection frequency, significantly enhances situational awareness and operational safety. These results confirm that cloud-based AI services can be effectively integrated into swarm systems to support real-time

maintenance and fault management in safety-critical fire-fighting missions.

Overall, the AI defect detection component proved to be a robust and effective element of the proposed framework. The results indicate that the Drone Inspector application can serve as a practical tool for continuous UAV integrity monitoring, reducing the likelihood of catastrophic failures and contributing to the overall resilience of UAV swarm deployments in emergency response scenarios.

5.3. Summary Discussion

The experimental results presented in this study demonstrate the effectiveness of integrating AI-enabled physical integrity monitoring with cyber-resilient communication mechanisms in UAV swarm systems designed for firefighting missions. By combining a hierarchical swarm architecture, autonomous in-flight inspection, and network-level security measures, the proposed framework addresses both physical and cyber risks that commonly arise in safety-critical emergency response scenarios.

From a physical reliability perspective, the results confirm that assigning a dedicated Inspector/Commander UAV to monitor swarm members enables continuous integrity awareness without disrupting mission execution. The AI-based defect detection process, implemented through the Drone Inspector application and powered by Amazon Rekognition, proved capable of identifying visible structural defects with high confidence. The use of a confidence-based alerting mechanism ensured that only high-probability defects triggered operational alerts, thereby balancing detection sensitivity and operational stability. The adaptive inspection strategy further enhanced responsiveness during high-risk mission phases, such as operation near active fire fronts, by reducing inspection intervals while preserving system efficiency during lower-risk conditions.

From a cybersecurity perspective, the MITM attack simulations highlight the vulnerability of flat, non-segmented network architectures commonly used in ad hoc deployments. The baseline experiments demonstrated that such configurations allow attackers to intercept and relay large volumes of network traffic, resulting in abnormal load and degraded communication performance. The introduction of subnet segmentation and ROAS-based routing optimization significantly reduced the attack surface and limited the feasibility of sustained interception. Traffic visualizations and comparative analysis confirmed that the proposed defensive strategy restored stable communication behavior even in the presence of an active attacker.

A key insight from this work is the strong interdependence between physical system integrity and cybersecurity in UAV swarm operations. Physical failures and cyber compromises can mutually amplify mission risk if not addressed holistically. The proposed framework demonstrates that embedding integrity inspection and cybersecurity mechanisms directly into the swarm architecture yields a more resilient system than treating these concerns independently. An important consideration in hierarchical swarm architectures is the potential failure of the

Inspector/Commander UAV itself. In the proposed framework, the supervisory role is not inherently bound to a single physical platform. In the event of Inspector/Commander UAV failure, loss of communication, or degraded sensing capability, the supervisory and inspection functions can be reassigned to a suitable operational UAV equipped with compatible imaging and communication resources. Such dynamic role reassignment preserves continuous integrity monitoring and prevents single-point failure from compromising mission safety. While the current experimental implementation assumes a predefined Inspector/Commander UAV, the results and architecture support extending the system toward autonomous role reassignment, which is identified as a key direction for future work. This integrated design approach is particularly relevant for firefighting missions, where environmental uncertainty, time pressure, and safety constraints demand robust and adaptive solutions.

While the experimental results validate the feasibility and effectiveness of the proposed system, certain limitations must be acknowledged. The physical deployment was conducted without live fire for safety reasons, and the AI-based inspection focused on externally visible defects. Additionally, the cybersecurity evaluation relied on network emulation rather than large-scale field deployment. These limitations point to opportunities for future work, but they do not diminish the practical contributions demonstrated in this study.

Overall, the results confirm that the proposed cyber-resilient UAV swarm framework enhances mission reliability, operational safety, and resilience against cyber threats, making it well suited for complex emergency response applications.

6. Conclusions

This paper presented a cyber-resilient UAV swarm framework tailored for firefighting missions, integrating hierarchical swarm coordination, AI-enabled in-flight defect detection, and secure communication design. The proposed approach addresses two critical challenges in UAV swarm deployment: maintaining physical integrity of individual drones during hazardous operations and protecting inter-drone communication from cyber threats such as Man-in-the-Middle attacks.

A heterogeneous six-UAV swarm architecture was introduced, in which a dedicated Inspector/Commander UAV performs periodic visual inspection of operational drones while mission tasks are executed in parallel. The Drone Inspector application, developed using the Flutter framework and integrated with Amazon Rekognition, enabled automated image processing and AI-based defect detection with confidence-driven alerting. Experimental results demonstrated that the system reliably detected visible structural defects and generated timely alerts while minimizing false positives through an 80% confidence threshold.

To address cybersecurity risks, the communication infrastructure was designed using subnet segmentation and ROAS-based routing optimization. Cybersecurity simulations conducted using GNS3 and Ettercap demonstrated that flat network architectures are highly susceptible to MITM attacks, whereas the proposed de-

fensive strategy significantly reduced traffic interception and restored stable network behavior. These results confirm the importance of incorporating cybersecurity mechanisms directly into UAV swarm communication design.

The combined experimental evaluation, encompassing physical swarm deployment, AI-based inspection, and cybersecurity simulation, demonstrates that the proposed framework is both practical and effective for safety-critical firefighting missions. By jointly addressing physical reliability and cyber resilience, this work contributes a comprehensive system-level solution for deploying UAV swarms in complex and adversarial environments.

In conclusion, the proposed cyber-resilient UAV swarm framework provides a robust foundation for future emergency response applications. The integration of autonomous inspection, adaptive operation, and secure communication represents a significant step toward safer, more reliable, and scalable UAV swarm deployments in real-world firefighting scenarios.

7. Future Work

While the proposed cyber-resilient UAV swarm framework demonstrates promising results for fire-fighting missions, several directions remain for future research and development. One important extension involves expanding the defect detection capability to include a broader range of fault types, such as internal component degradation, sensor drift, and early-stage mechanical wear that may not be easily observable through external visual inspection alone. Integrating additional sensing modalities, including thermal, vibration, and acoustic sensors, could further enhance defect detection accuracy and robustness.

Future work will also focus on improving the AI-based inspection module through the use of custom-trained models and domain-specific datasets. Training deep learning models on large-scale drone-specific defect datasets captured under diverse environmental conditions could improve detection performance for subtle or partially occluded defects and reduce reliance on generic cloud-based models. Additionally, deploying lightweight edge AI models on the Inspector/Commander UAV could reduce latency and dependency on cloud connectivity in communication-constrained environments.

Another important research direction involves enhancing the adaptability and intelligence of the inspection strategy. While the current system employs a rule-based adaptive inspection interval, future work may explore learning-based approaches that dynamically adjust inspection frequency based on real-time risk assessment, mission context, and historical defect patterns. Such approaches could further optimize the trade-off between inspection responsiveness and resource consumption.

From a cybersecurity perspective, future work will investigate additional threat models and attack vectors beyond Man-in-the-Middle attacks, including denial-of-service attacks, spoofing, and insider threats. Integrating cryptographic authentication mechanisms, intrusion detection systems, and trust management

frameworks could further strengthen the resilience of swarm communication networks. Experimental evaluation of these mechanisms under large-scale swarm scenarios will also be considered.

Finally, future work will aim to validate the proposed framework reminder under more realistic fire-fighting conditions, including controlled fire environments and high-fidelity simulation platforms. Scaling the swarm to a larger number of UAVs and evaluating long-duration missions will provide deeper insight into system scalability, reliability, and operational sustainability. These extensions will further support the deployment of autonomous, secure, and resilient UAV swarms in real-world emergency response applications.

Acknowledgements

The authors would like to express their sincere gratitude to the Canadian College of Kuwait (CCK) for providing academic support, technical resources, and an encouraging research environment that contributed to the completion of this work.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Alon, O., Rabinovich, S., Fyodorov, C. and Cauchard, J.R. (2021) Drones in Firefighting: A User-Centered Design Perspective. *Proceedings of the* 23*rd International Conference on Mobile Human-Computer Interaction*, Toulouse, 27 September-1 October 2021, 1-11. https://doi.org/10.1145/3447526.3472030

[2] Roldán-Gómez, J.J., González-Gironda, E. and Barrientos, A. (2021) A Survey on Robotic Technologies for Forest Firefighting: Applying Drone Swarms to Improve Firefighters' Efficiency and Safety. *Applied Sciences*, **11**, Article 363. https://doi.org/10.3390/app11010363

[3] Wang, H., Zhao, C., Feng, Y., Huang, X., Qu, C., Zhu, Y., *et al.* (2025) Enhancing Firefighter Safety and Efficiency through UAV-Assisted AI-Based Human Motion Recognition System. *Expert Systems with Applications*, **289**, Article ID: 128176. https://doi.org/10.1016/j.eswa.2025.128176

[4] Zhou, Y., Rao, B. and Wang, W. (2020) UAV Swarm Intelligence: Recent Advances and Future Trends. *IEEE Access*, **8**, 183856-183878. https://doi.org/10.1109/access.2020.3028865

[5] Javed, S., Hassan, A., Ahmad, R., Ahmed, W., Ahmed, R., Saadat, A., *et al.* (2024) State-of-the-art and Future Research Challenges in UAV Swarms. *IEEE Internet of Things Journal*, **11**, 19023-19045. https://doi.org/10.1109/jiot.2024.3364230

[6] Alotaibi, A., Chatwin, C. and Birch, P. (2024) Aerial Surveillance Leveraging Delaunay Triangulation and Multiple-UAV Imaging Systems. *Applied System Innovation*, **7**, Article 23. https://doi.org/10.3390/asi7020023

[7] Zhu, F., Lu, Y.Y. and Yang, J. (2024) Collaborative Control Technology and Prospects of Drone Swarms in Earthquake Emergency Rescue Scenarios. *Proceedings of the* 2024 *Asia Pacific Conference on Computing Technologies, Communications and Networking*, Chengdu, 26-27 July 2024, 83-91. https://doi.org/10.1145/3685767.3685782

[8] Luo, Y., Huang, L., Shi, L., Bao, G. and Dai, F. (2024) Environmental Hazard Assessment of Forest Fire Sites to Firefighting Aircraft—Part I: Canyon Wind and Temperature Distribution. *Heliyon*, **10**, e35684. https://doi.org/10.1016/j.heliyon.2024.e35684

[9] Balestrieri, E., Daponte, P., De Vito, L., Picariello, F. and Tudosa, I. (2021) Sensors and Measurements for UAV Safety: An Overview. *Sensors*, **21**, Article 8253. https://doi.org/10.3390/s21248253

[10] Macaulay, M.O. and Shafiee, M. (2022) Machine Learning Techniques for Robotic and Autonomous Inspection of Mechanical Systems and Civil Infrastructure. *Autonomous Intelligent Systems*, **2**, Article No. 8. https://doi.org/10.1007/s43684-022-00025-3

[11] Wang, X., Zhao, Z., Yi, L., Ning, Z., Guo, L., Yu, F.R., *et al.* (2024) A Survey on Security of UAV Swarm Networks: Attacks and Countermeasures. *ACM Computing Surveys*, **57**, 1-37. https://doi.org/10.1145/3703625

[12] Fereidouni, H., Fadeitcheva, O. and Zalai, M. (2025) IoT and Man-In-The-Middle Attacks. *Security and Privacy*, **8**, e70016. https://doi.org/10.1002/spy2.70016

[13] Arshad, U. and Halim, Z. (2025) Secure and Optimized Drone Swarm Operations with Decentralized Adaptive Differential Evolution. *Computers and Electrical Engineering*, **126**, Article ID: 110487. https://doi.org/10.1016/j.compeleceng.2025.110487

[14] Talaat, F.M., Ibrahim, A., El-Kenawy, E.M., Abdelhamid, A.A., Alhussan, A.A., Khafaga, D.S., *et al.* (2022) Route Planning for Autonomous Mobile Robots Using a Reinforcement Learning Algorithm. *Actuators*, **12**, Article 12. https://doi.org/10.3390/act12010012

[15] Vakaliuk, T., Trokoz, Y., Pokotylo, O., Osadchyi, V. and Bolotina, V. (2024) Emulation and Detection of ARP Attacks in GNS3 Environment: Modelling and Development of a Defense Strategy. *Proceedings of CPITS* 2024-*Cybersecurity Providing in Information and Telecommunication Systems*, **3654**, 376-383.

[16] Tashildar, A., Shah, N., Gala, R., Giri, T. and Chavhan, P. (2020) Application Development Using Flutter. *International Research Journal of Modernization in Engineering Technology and Science*, **2**, 1262-1266.

[17] Nagaraj, K., Prabakaran, B. and Ramkumar, M.O. (2022) Application Development for a Project Using Flutter. 2022 3*rd International Conference on Smart Electronics and Communication* (*ICOSEC*), Trichy, 20-22 October 2022, 947-951. https://doi.org/10.1109/icosec54921.2022.9951938

[18] Singh, D. and Arora, D. (2024) Cloud-Based Object Detection Model Using Amazon Rekognition. In: Roy, N.R., Tanwar, S. and Batra, U., Eds., *Cyber Security and Digital Forensics*, Springer, 165-177. https://doi.org/10.1007/978-981-99-9811-1_13

[19] Honguntiker, K.P.H. (2023) Analysis of Facial Expressions with Amazon Rekognition. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4597968

[20] Arnab, A. and Torr, P.H.S. (2017) Pixelwise Instance Segmentation with a Dynamically Instantiated Network. 2017 *IEEE Conference on Computer Vision and Pattern Recognition* (*CVPR*), Honolulu, 21-26 July 2017, 879-888. https://doi.org/10.1109/cvpr.2017.100

[21] Zhou, L., Zhou, D., Yang, H. and Yang, S. (2023) Two-Subnet Network for Real-World Image Denoising. *Multimedia Tools and Applications*, **83**, 14757-14773. https://doi.org/10.1007/s11042-023-16153-8

[22] Lin, W., Zhang, Z., Drake, J., Rabadan, J. and Sajassi, A. (2024) RFC 9625: EVPN Optimized Inter-Subnet Multicast (OISM) Forwarding.

https://dl.acm.org/doi/abs/10.17487/RFC9625?casa_token=5L4Yl7kInbsAAAAA%3A2oOsXhaA1INMkWRYmWt-javx4lsSdS2n54hD9vx2_BFWZ42BGbcgX7A93rq3YqozQQGnHLaTb0uocqw

[23] Brännström, A. and Vandermaesen, T. (2025) The Role of Network Segmentation in Enhancing Cybersecurity in Substation Communication Networks. https://www.diva-portal.org/smash/get/diva2:1966026/FULLTEXT01.pdf

[24] Li, T., Yang, C., Wang, Y., Cai, L., Anpalagan, A. and Han, Z. (2026) A Survey on Network Management for xANET: Evolution, Challenges, and Future Directions. *IEEE Communications Surveys & Tutorials*, **28**, 1209-1247. https://doi.org/10.1109/comst.2025.3545254

[25] Cao, P., Lei, L., Cai, S., Shen, G., Liu, X., Wang, X., *et al.* (2024) Computational Intelligence Algorithms for UAV Swarm Networking and Collaboration: A Comprehensive Survey and Future Directions. *IEEE Communications Surveys & Tutorials*, **26**, 2684-2728. https://doi.org/10.1109/comst.2024.3395358

[26] Chandru, J. and Bagyalakshmi, C. (2025) A Comprehensive Review of MITM Attack Based on Detection and Prevention in Wireless Network Environment. In: Ramachandran, G., Subramaniam, S., Krishnamurthy, V., Ramamoorthy, S., *et al.*, Eds., *Recent Trends in Advanced Computing*, Springer, 77-89. https://doi.org/10.1007/978-3-032-02537-1_8

[27] Alameri, I., Komarkova, J., Al-Hadhrami, T. and Lotfi, A. (2022) Systematic Review on Modification to the *ad-Hoc* On-Demand Distance Vector Routing Discovery Mechanics. *PeerJ Computer Science*, **8**, e1079. https://doi.org/10.7717/peerj-cs.1079

Appendix

In this work, the confidence score represents an application-level metric derived from AI detection outputs and predefined evaluation logic. The confidence score is used to assess the reliability of detected defects and is compared against a fixed threshold (80%) to determine alert generation.

Confidence interval: The confidence interval is the range in which the population parameter is most likely to be found. The degree of certainty for which it is likely to be within that range is called the confidence level. When gathering sample data, the precise value of the parameter is unknown.

Confidence level: The confidence level is the required degree of certainty that the population parameter will be in the confidence interval. This is the probability that the calculated confidence interval contains the population parameter. Researchers frequently employ a confidence level of 0.95. The 95% confidence interval postulates that if one were to compute the confidence interval for an infinite number of samples, then 95% of the calculated ranges would encompass the population parameter.

When the population's standard deviation (σ) is known, the normal distribution is utilized. The distribution of the sample mean ($\bar{X}$) is normal with a mean of Mean and a standard deviation of $\sigma/\sqrt{n}$. If the population standard deviation is unknown, the t distribution with n − 1 degrees of freedom is used, employing the sample standard deviation. The distribution of ($\bar{X}$ − Mean)/(S/$\sqrt{n}$) is T.

The mean confidence interval formula

- The population standard deviation is known:

$$\bar{X} \pm Z_{\alpha/2} * \frac{\sigma}{\sqrt{n}}$$

- The population standard deviation is unknown:

$$\bar{\mathrm{X}} \pm \mathrm{T}_{\frac{\alpha}{2}}(\mathrm{df}) * \frac{\mathrm{S}}{\sqrt{\mathrm{n}}}$$

The standard deviation confidence interval formula

$$\frac{(n-1)\mathrm{S}^2}{\mathrm{X}_{\left(1-\frac{\alpha}{2}\right)}(\mathrm{df})} \leq \sigma^2 \leq \frac{(n-1)S^2}{X_{\left(\frac{\alpha}{2}\right)}(df)}$$

where:

$\bar{\mathrm{X}}$: The sample average.

σ : The population standard deviation, typically, the population standard deviation is unknown and may be obtained from other research as a sample standard deviation with a larger sample size. In this scenario, it is permissible to assume it as the population standard deviation.

S: The sample standard deviation.

n: The sample size (the number of observations).

CL: confidence level.

$\alpha = 1 - \mathrm{CL}$.

$Z_{\alpha/2}$ —The z-score based on the standard normal distribution, p ($z < Z_{\alpha/2}$) = $\alpha/2$.

$T_{\alpha/2}$ —The t-score based on the t distribution, p ($t < T_{\alpha/2}$) = $\alpha/2$.

df —Degrees of freedom. $df = n - 1$.