Journal of Computer and Communications, 2024, 12, 1-25
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

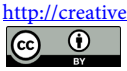
A Secure Communication Framework for Drone Swarms in Autonomous Surveillance Operations

Ahad Alotaibi, Chris Chatwin, Phil Birch

School of Engineering & Informatics, University of Sussex, Brighton, UK
Email: aa2758@sussex.ac.uk

How to cite this paper: Alotaibi, A., Chatwin, C. and Birch, P. (2024) A Secure Communication Framework for Drone Swarms in Autonomous Surveillance Operations. *Journal of Computer and Communications*, **12**, 1-25.
https://doi.org/10.4236/jcc.2024.1211001

Received: September 10, 2024
Accepted: October 28, 2024
Published: October 31, 2024



Abstract

Drones have become indispensable tools in various domains, from surveillance and environmental monitoring to disaster response and communication relay. However, their growing use in critical missions necessitates robust security measures to protect against potential threats and ensure the integrity of operations. This research presents a novel secure architecture for a swarm of drones deployed on surveillance missions. Leveraging a reliable foundation established through Delaunay triangulation for communication among drones, this work introduces advanced security protocols to enhance the protection and integrity of the network. The architecture employs a mesh network topology connecting six drones, each configured for specific surveillance tasks, including perimeter monitoring, area scanning, thermal imaging, traffic observation, communication relay, and incident response. The mesh network design ensures extended coverage, redundancy, load balancing, and self-configuration, significantly improving reliability and resilience. Security validation was conducted using GNS3 and Ettercap, simulating various vulnerability scenarios. Comparative performance analysis between a classic drone network and the proposed secure mesh network demonstrates superior traffic management and robustness against potential attacks. The results underscore the architecture's suitability for secure and reliable operations in critical surveillance environments.

Keywords

Drone Swarm Security, Mesh Network Architecture, Surveillance Missions, Vulnerability Testing, GNS3 Simulation

1. Introduction

Unmanned aerial vehicles (UAVs), commonly known as drones, have seen wide-

spread adoption across various industries, including logistics, agriculture, environmental monitoring, and especially surveillance and defense applications. Their ability to provide real-time situational awareness, coupled with their capability to reach hazardous or inaccessible areas, has made them indispensable tools in modern surveillance operations [1]. However, as the deployment of drones increases, particularly in mission-critical applications, securing these systems from potential cyber threats has become an essential requirement [2].

Drone swarms—multiple UAVs working in coordination—offer significant advantages over single drones in terms of coverage, redundancy, and efficiency, particularly for surveillance missions such as border monitoring, disaster management, and critical infrastructure protection [3]. However, these advantages come with increased complexity, especially in ensuring secure and reliable communication between drones. A coordinated attack or network disruption could compromise the entire swarm, making security a top priority for these systems [4]. The introduction of secure, scalable communication architectures for drone swarms is crucial for their successful deployment in high-risk environments.

Traditional point-to-point communication architectures, often used in single-drone systems, are not well-suited for the demands of swarm operations. These systems suffer from limitations such as single points of failure, limited range, and weak security protocols, which make them vulnerable to attacks or failures in complex mission environments [5]. To address these challenges, this research presents a novel architecture for secure drone swarm operations that integrates mesh network topology with advanced security protocols.

Mesh networks are known for their decentralized nature, allowing drones to communicate with multiple nodes in the network and eliminating the risks associated with single points of failure. The dynamic routing and self-healing capabilities of mesh networks are particularly advantageous in hostile or unpredictable environments where communication reliability is critical. Furthermore, mesh networks enable scalability, allowing additional drones to join the swarm without requiring a complete network reconfiguration [6]. However, while mesh networks provide a reliable communication framework, they are not inherently secure against sophisticated cyber threats such as spoofing, jamming, or man-in-the-middle (MITM) attacks. To address these risks, this research incorporates advanced security protocols, including encryption and firewall protection, into the mesh network architecture.

One of the innovative aspects of the proposed architecture is the use of Delaunay triangulation to optimize communication paths between drones. This geometric method ensures that each drone maintains reliable communication with its nearest neighbors, maximizing coverage while minimizing communication failures. By leveraging both Delaunay triangulation and mesh networking, the architecture enhances both reliability and security, ensuring continuous operation in dynamic mission environments [7].

The security and performance of the proposed architecture were validated

through extensive testing in simulated environments using GNS3 and Ettercap. GNS3 was used to simulate various attack scenarios, such as denial-of-service (DoS) and MITM attacks, to assess how the architecture responds under adverse conditions. Ettercap was employed for vulnerability testing, focusing on traffic interception and spoofing attempts. Comparative analysis between the proposed secure mesh network and conventional drone communication architectures demonstrated that the secure mesh network offers superior performance, reliability, and resistance to cyber threats.

Despite their widespread deployment, traditional drone communication architectures, such as point-to-point and star topologies, remain vulnerable to numerous threats and limitations, particularly when scaled to swarm operations [8]. These architectures lack the redundancy and flexibility necessary for dynamic environments, where drones must adapt quickly to changing conditions. The proposed secure mesh network architecture addresses these shortcomings by providing a more robust, scalable, and secure framework for drone swarm operations.

As drone technology continues to evolve, particularly in critical surveillance and defense applications, the need for secure, reliable communication architectures has never been more pressing. This paper contributes to the advancement of drone swarm technology by proposing a secure architecture that combines the reliability of mesh networks with advanced security measures, offering a comprehensive solution for mission-critical operations.

The paper is organized as follows: The materials and methods section outlines the technical details of the proposed architecture, and the tools used for security validation. The results section presents the findings from the simulated attack scenarios and performance testing, highlighting the security and reliability of the architecture. The discussion explores the implications of these findings for real-world applications and suggests potential improvements for future deployments. The paper concludes with a summary of the key contributions and recommendations for future research in the conclusion section.

2. Materials and Methods

2.1. Drone Swarm Architecture Overview

The concept of using a swarm of drones has gained significant traction in various industries, particularly in surveillance, search and rescue, and military operations. A drone swarm refers to a coordinated group of autonomous drones that work together to achieve a common objective. The importance of using a swarm of drones lies in their ability to provide enhanced diverse coverage, redundancy, and adaptability in complex and dynamic environments [9]. In a surveillance mission, where real-time data and continuous monitoring are critical, a swarm of drones offers several advantages over a single drone system [10]. By distributing tasks across multiple drones, swarms can cover larger areas, operate more efficiently, and reduce the risk of mission failure due to individual drone malfunctions. Furthermore, swarms are inherently scalable, meaning that additional drones can be

added as needed without requiring significant changes to the existing system architecture.

Swarm technology leverages the principles of decentralized control, where each drone can communicate and collaborate with others in the network [11]. This allows the swarm to function cohesively, even if individual drones experience communication disruptions or technical issues. The swarm's collective intelligence and redundancy ensure that the mission continues without compromising data integrity or operational effectiveness. For instance, in surveillance operations, different drones can be assigned specific roles—such as perimeter monitoring, thermal imaging, or communication relay—allowing the swarm to perform multiple tasks simultaneously [12]. This division of labor enhances the overall efficiency of the mission and reduces the time needed to complete complex tasks.

2.1.1. Description of the Swarm Configuration

In this research, a drone swarm consisting of six drones was configured to carry out a comprehensive surveillance mission. Each drone within the swarm was assigned a unique role to ensure the successful execution of the mission. The swarm operates with a decentralized control system, allowing each drone to communicate with its peers and the control center in real time. The selected drone models were specifically chosen for their ability to perform under challenging environmental conditions, extended flight range, and high-resolution imaging capabilities.

The first drone in the swarm was designated as the Perimeter Surveillance Drone, which was responsible for monitoring the perimeter of the target area. Equipped with high-resolution cameras, this drone provided continuous video feeds and real-time situational updates to the control center. The second drone, the Area Scanning Drone, performed a systematic scan of the entire target area. Its high-resolution imaging system allowed for detailed mapping and detection of objects within the surveillance zone. Meanwhile, the third drone, the Thermal Imaging Drone, was equipped with advanced infrared cameras to monitor temperature variations and detect heat signatures. This capability was especially crucial during night-time operations or in low-visibility environments, where thermal imaging provided a distinct advantage.

The fourth drone, the Traffic Monitoring Drone, was tasked with monitoring traffic flow within and around the surveillance zone. Its advanced imaging system, supported by artificial intelligence, enabled the real-time identification of vehicles and tracking of movement patterns. The fifth drone, serving as the Communication Relay Drone, acted as an intermediary to maintain robust and continuous communication between drones and the control center, particularly in situations where direct communication was hindered by environmental obstacles or extended operational range. Finally, the Incident Response Drone was configured for rapid deployment in the event of an anomaly or security breach. This drone provided high-resolution zoom capabilities and quick situational assessments in response to critical events detected by the other drones.

2.1.2. Mission Parameters and Requirements

The drone swarm was deployed to carry out a surveillance mission over a large geographic area. The mission parameters included maintaining continuous observation of the target area, detecting and responding to incidents in real time, and ensuring seamless data transmission back to the control center. To meet these operational demands, the drones were required to possess extended flight ranges of up to 15 kilometers and have the ability to remain airborne for up to 55 minutes, ensuring that the swarm could maintain continuous coverage without frequent interruptions for recharging or refueling. Additionally, each drone was equipped with high-resolution sensors, such as RGB cameras and thermal imaging systems, to enable precise detection of objects and events within the surveillance zone.

One of the key operational requirements was the swarm's ability to operate autonomously. The drones were programmed to navigate the surveillance area independently, adjust their flight paths based on environmental conditions, and avoid obstacles in real time. Moreover, the architecture was designed to provide a high level of redundancy and reliability. If one drone in the swarm experienced a failure, the others were configured to adapt and compensate for the lost functionality, ensuring that the mission continued uninterrupted. While optimizing available resources, the system also has the ability to request an appropriate replacement drone.

2.1.3. System Architecture

The system architecture employed in this research was designed to facilitate seamless collaboration and communication between the drones, allowing them to function as a cohesive swarm. The architecture was based on a mesh network topology, which provided decentralized communication between the drones. In a mesh network, each drone acts as a node that can communicate directly with multiple drones. This creates a self-healing network that is highly resistant to individual node failures. If one drone loses communication or experiences a malfunction, the other drones can dynamically reroute the communication through alternative paths, ensuring continuous data transmission.

Each drone was equipped with essential network components, including routers, firewalls, and edge processing servers. The router facilitated real-time data transmission between the drones and the control center, while the firewall protected the communication channels from unauthorized access. The edge processing servers allowed the drones to process data locally, reducing latency and enabling them to make autonomous decisions without relying solely on the control center for instruction. This local processing capability was particularly important for time-sensitive tasks, such as incident response or real-time traffic monitoring.

Additionally, the communication between drones was optimized through Delaunay triangulation, a geometric method that ensures efficient communication between the drones by creating triangles between nodes. An overview of the swarm distribution using Delaunay triangulation is shown in **Figure 1** below.

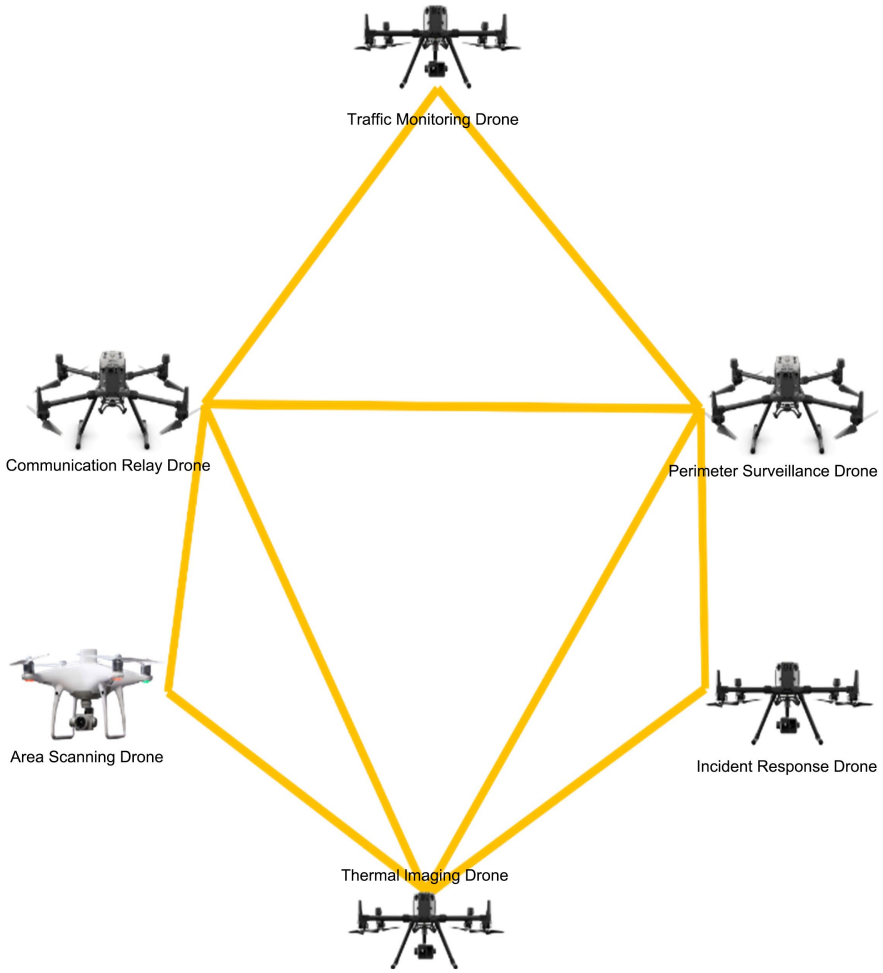


Figure 1. Overview of the swarm distribution using Delaunay triangulation.

This minimizes communication delays and ensures each drone maintains reliable links with its nearest neighbors. The Delaunay triangulation approach enhances the robustness of the network by ensuring optimal communication paths. A more detailed description of the network design, including the mesh topology and its specific benefits, will be covered later in the Network Design subsection.

2.1.4. Operational Challenges and Considerations

The deployment of a drone swarm for surveillance missions presents several operational challenges, including environmental variability, communication integrity, and resource management [13]. Drones must be able to operate in diverse and sometimes harsh environmental conditions, such as extreme weather, uneven obstructive terrain, and varying light levels. The mesh network topology provided the flexibility needed to maintain communication in these challenging environments, while the autonomous navigation capabilities of the drones allowed them to adjust to real-time changes in terrain and obstacles.

Communication integrity was another critical challenge. Ensuring that the drones maintained continuous and secure communication with both each other

and the control center was essential for mission success. The mesh network provided redundancy, plus additional measures, such as encrypted communication and firewall protection, were implemented to ensure the security and integrity of the transmitted data.

Battery life and resource management were also key considerations. Each drone had a limited operational time, and the system architecture included features to monitor battery levels and manage resources efficiently. Tasks were assigned to drones based on their remaining power, ensuring that no drone was overburdened or risked running out of battery power during a critical moment of the mission.

Through this carefully designed system architecture, the research demonstrates how a drone swarm can effectively execute surveillance missions while addressing the inherent challenges of redundancy, communication, and security.

2.2. Network Design

The network design for the drone swarm is critical for ensuring seamless communication between the drones and the control center, particularly in a mission-critical surveillance scenario. To achieve reliable and resilient communication, the network relies on a mesh topology for the routers that connect the drones and facilitate data transmission across the system. Unlike traditional point-to-point or centralized networks, where communication depends on a single hub or direct connections between devices, a mesh network allows each router in the system to connect with multiple other routers [14]. This creates a decentralized, self-healing network that can withstand disruptions, making it particularly suitable for drone swarms operating in dynamic and unpredictable environments.

In the proposed architecture, each drone is equipped with a dedicated router that is part of the overall mesh network. The routers handle the transmission of all data between the drones and the control center, ensuring that the data flows efficiently and securely across the swarm. In a mesh topology, the routers communicate directly with one another, forming a network where data can take multiple paths to reach its destination. This means that if one router (or drone) becomes unavailable due to a failure or interference, the data can be rerouted through other routers in the network, ensuring continuous operation without a single point of failure. An overview of the proposed mesh network design is shown in **Figure 2** below.

The key advantage of a mesh network for the routers is its fault tolerance. Since each router is connected to several other routers, the failure of a single node does not interrupt the network's communication [15]. Instead, the system dynamically reroutes data through alternative paths, maintaining a stable connection between the drones and the control center. This self-healing ability is crucial in surveillance missions where uninterrupted communication is essential, and the environment may cause interference or physical obstructions. For example, if one drone flies out of range or its router malfunctions, the other drones in the swarm can still communicate with the control center by passing data through the remaining routers.

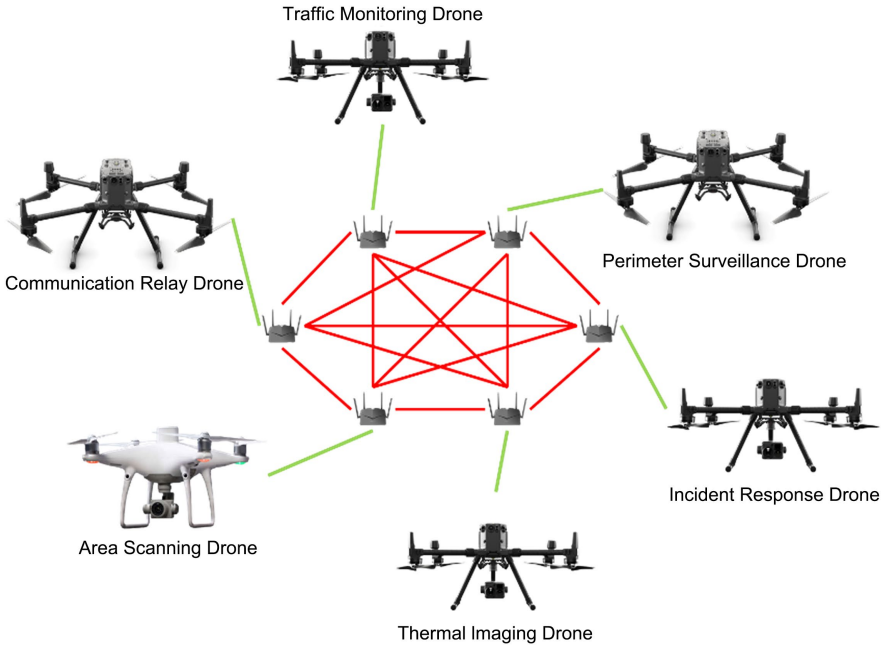


Figure 2. Overview of the proposed mesh network design.

In addition to fault tolerance, the mesh network offers significant scalability [14]. As new drones are added to the swarm, their routers automatically become part of the existing mesh network without requiring major reconfigurations. This is particularly beneficial for large-scale or evolving surveillance operations where the number of drones may change based on mission requirements. The flexible nature of the mesh network allows the system to scale up or down seamlessly, maintaining consistent performance even as the network size grows.

The redundancy inherent in the mesh topology also enhances communication reliability [16]. Since multiple communication paths are available between any two points in the network, data traffic is distributed across the available routers, preventing congestion and reducing the likelihood of communication bottlenecks. This redundancy ensures that critical data—such as video feeds, telemetry, and control signals—can be transmitted without delay, even under conditions of heavy network load or interference.

The mesh network used for the drone swarm's routers also supports dynamic routing [17]. This feature enables the routers to continuously adjust their communication pathways in response to changing network conditions. For instance, if one drone moves out of range or its communication path is blocked by an obstacle, the network automatically reroutes the data through alternative routers, ensuring that the drones and the control center remain in constant communication. This dynamic routing capability is especially important for drone swarms, where movement and changing operational conditions can frequently alter the network topology.

Delaunay triangulation is employed to optimize communication efficiency within the mesh network. Delaunay triangulation is a geometric method used to

optimize communication paths between nodes in a network. It creates a triangulated network by connecting each node to its nearest neighbors, ensuring that no point lies inside the circumcircle of any triangle. This approach minimizes the longest edges in the network, enhancing the efficiency and reliability of communication paths. In the context of drone swarms, Delaunay triangulation helps to reduce latency and improve the robustness of data transmission. This geometric method ensures that the routers form the most efficient communication paths by connecting each drone to its nearest neighbors in a triangular network [18]. By minimizing the distance between communication nodes, Delaunay triangulation reduces communication delays and ensures that data is transmitted through the most direct and reliable routes. This helps prevent long, inefficient communication paths and enhances the overall performance of the network, particularly in large or complex surveillance areas.

While the mesh network provides significant advantages in terms of reliability and flexibility, it also introduces certain security challenges, particularly in mission-critical environments where the confidentiality and integrity of the data are paramount. To address these concerns, the network design incorporates robust encryption protocols to secure communication between the routers. The proposed encryption method for this system is Advanced Encryption Standard (AES) with 256-bit keys. AES-256 is widely recognized for its strong security and is approved for use in protecting sensitive government and military data [19]. Its large key size makes it highly resistant to brute-force attacks, providing a high level of security for the data transmitted between the drones and the control center.

In a mesh network where data flows through multiple routers, it is essential to ensure that the communication remains secure at each point. AES-256 encryption ensures that all data—including video streams, control signals, and telemetry—is encrypted before being transmitted through the network [20]. Even if an attacker intercepts the communication at one of the routers, they will not be able to decrypt the data without the appropriate key. A public key infrastructure (PKI) is used to facilitate the secure exchange of encryption keys [21]. Each drone is equipped with a unique public-private key pair, ensuring that encryption keys can be exchanged securely without risk of interception. The public key is used to encrypt the data, and only the corresponding private key can decrypt it, adding an extra layer of security to the communication process.

Beyond encryption, the network design includes firewalls at both the router level and the control center. Firewalls play a crucial role in maintaining the security and integrity of the network by monitoring, filtering, and controlling the flow of data [22]. At the router level, firewalls help to protect each drone's communication by preventing unauthorized access and ensuring that only legitimate traffic passes through the network. They analyze incoming and outgoing data packets, comparing them against a set of predefined security rules to block any suspicious or potentially malicious activity.

In addition to blocking unauthorized access, firewalls at the router level can

also prevent certain types of attacks, such as DoS attacks, by limiting the rate at which packets are allowed to pass through the router [23]. This rate-limiting capability helps prevent attackers from overwhelming the network with excessive traffic, thereby maintaining the availability of communication channels. Firewalls are also instrumental in thwarting MITM attacks, where an attacker attempts to intercept and manipulate communication between drones [24]. By enforcing strict traffic rules and ensuring that only authorized entities can communicate with the routers, firewalls act as a first line of defense against such attacks.

At the control center level, more advanced firewalls are employed to monitor the entire network's traffic. These firewalls perform deep packet inspection (DPI), which allows them to examine the content of data packets beyond just the headers [25]. DPI can detect and block advanced threats such as malware or sophisticated intrusion attempts, providing an additional layer of security. The control center firewall also logs all network traffic, creating an audit trail that can be used to analyze any suspicious activity or breaches that may occur. This audit capability is essential for forensic analysis in the event of a security incident, helping to trace the origin and method of the attack.

The combination of encryption and firewalls in the network design ensures that the mesh network for the drone swarm is secure, reliable, and resilient against various cyber threats. By protecting communication channels at both the router and control center levels, the system maintains the confidentiality and integrity of all transmitted data, enabling the drone swarm to operate effectively in mission-critical surveillance tasks without the risk of data breaches or communication failures.

2.3. Simulation Environment

In developing a secure and reliable communication framework for drone swarms, the creation of a robust simulation environment is essential. Simulation environments provide a controlled and repeatable platform for testing the performance, resilience, and security of network architectures. They allow researchers to rigorously assess how systems respond to real-world conditions without the expense and risk associated with deploying physical hardware in live environments. These environments are particularly important in scenarios where mission-critical operations, such as surveillance, disaster response, or military applications, depend on the seamless coordination of multiple autonomous systems [26]. By simulating these conditions, researchers can identify and address potential weaknesses, evaluate the effectiveness of different network configurations, and ensure that security protocols operate as intended.

The use of specialized tools within these environments further enhances the ability to simulate realistic operational conditions. Network simulators such as GNS3 (Graphical Network Simulator-3) offer the flexibility to model complex, large-scale network topologies, allowing for the dynamic testing of network performance under a variety of scenarios. Security-focused tools like Ettercap enable researchers to evaluate how well a network can defend against potential cyber

threats, providing insights into the effectiveness of encryption protocols and firewall configurations. Such simulations are invaluable, as they replicate the kinds of attacks and operational disruptions that drone swarms may encounter in real-world deployments. Through these simulations, it becomes possible to test the limits of the proposed network architecture in a risk-free environment, while gaining valuable data on how the system behaves under both normal and adverse conditions. In this work, GNS3 and Ettercap were used to thoroughly test the proposed mesh network architecture and its security mechanisms for a drone swarm in mission-critical surveillance operations.

2.3.1. Simulation Tools and Software

The core of the simulation environment was built around GNS3, a powerful and widely used network simulation tool that allows for the emulation of real-world network components and protocols. GNS3 was chosen for its flexibility in designing complex network topologies and its ability to provide a virtual representation of the drone swarm's mesh network [27]. By using GNS3, it was possible to create a dynamic simulation of the routers that connect the drones, modeling their interactions and ensuring that the mesh network could handle real-time communication needs.

GNS3 allows users to visually map out and configure network components, which makes it ideal for modeling the proposed mesh network. Each drone in the swarm was represented by a node in the GNS3 environment, connected via virtual routers that mirrored the real-world communication infrastructure. The software allowed for detailed control over each router's settings, including routing protocols and communication parameters. This made it possible to simulate dynamic routing, where data could be rerouted through alternative paths in the event of node failure or disruption, an essential feature of the mesh network. Furthermore, GNS3's real-time monitoring capabilities provided a clear view of network traffic and performance, ensuring that the network could handle various operational loads without encountering significant delays or communication breakdowns. The proposed network design in GNS3 software is shown in **Figure 3** below.

In addition to GNS3, Ettercap was used extensively to simulate and test the security aspects of the drone swarm network. Ettercap is a comprehensive tool for network analysis and security testing, particularly focused on MITM attacks and other forms of intrusion [28]. By using Ettercap, it was possible to simulate a range of cyberattacks on the network, from basic eavesdropping to more sophisticated attempts to alter or intercept data between drones. The ability to simulate these attacks in a controlled environment was crucial for evaluating the robustness of the network's encryption protocols and firewall protections. Ettercap also allowed for the analysis of network traffic at a granular level, making it possible to identify any vulnerabilities that could be exploited by attackers, and ensuring that the security measures in place were effective at preventing unauthorized access and data manipulation. The interface of Ettercap software is shown in **Figure 4** below.

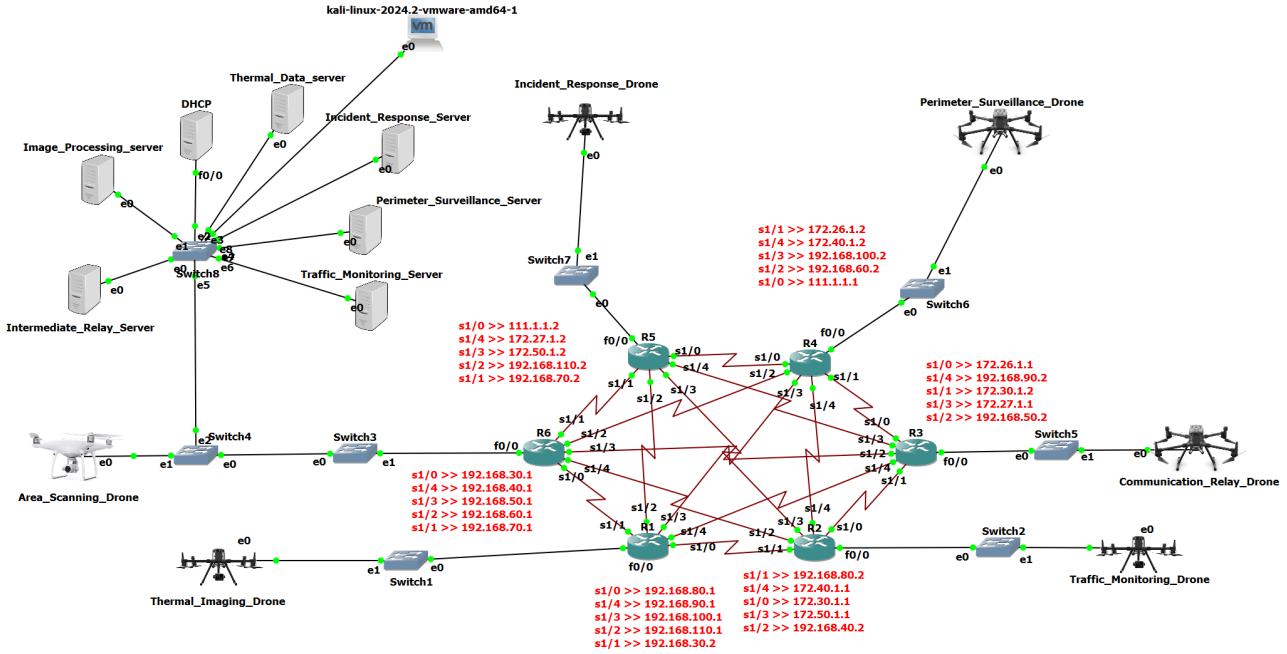


Figure 3. The proposed network design in GNS3 software.

Figure 4. Ettercap software.

2.3.2. Hardware and Network Infrastructure

While the majority of the simulation environment was virtual, it was run on a physical hardware infrastructure capable of handling the complex requirements of the network. The simulation was hosted on high-performance servers, each equipped with multi-core processors (Intel Xeon) with substantial memory (128 GB RAM) to support the large-scale emulation of the drone swarm's network. These servers ran virtual machines that represented individual drones, each with its own router. The routers were interconnected to form the mesh topology, with dynamic routing protocols enabled to ensure that communication paths could be adjusted in real-time based on network conditions.

The hardware infrastructure was selected to ensure that the simulation could run smoothly, and that the performance metrics collected would be accurate and

representative of real-world operations. The servers' high processing power and memory allowed for the seamless operation of the GNS3 environment, even when simulating large amounts of data traffic, such as video feeds and telemetry from multiple drones. This ensured that the network's scalability and fault tolerance could be thoroughly tested without the limitations that might be encountered in less robust hardware environments.

To simulate real-world conditions, latency simulators were used within the GNS3 environment to introduce artificial delays in data transmission between nodes [29]. This replicated the effects of distance, interference, and other factors that could impact communication in a live deployment. By incorporating these delays into the simulation, it was possible to evaluate the network's ability to maintain communication under less-than-ideal conditions. The dynamic routing protocols were tested to ensure that they could reroute data efficiently when communication paths became congested or disrupted, validating the self-healing properties of the mesh network.

2.3.3. Network Configuration and Parameters

The configuration of the network within the simulation environment was designed to closely mimic the conditions under which the drone swarm would operate in a real surveillance mission. Each drone was represented as a node within the mesh network, connected through virtual routers. The network was designed to handle a variety of data types, including real-time video streams, telemetry data, and control signals. These data types were tested under different levels of network load to evaluate the performance and stability of the system.

One of the key features of the mesh network was its dynamic routing capabilities. In a dynamic routing environment, the network is able to adjust its communication paths automatically based on real-time conditions. For example, if one drone in the swarm moves out of range or its communication path is blocked by an obstacle, the network can automatically reroute data through alternative nodes. This ability to adapt to changing conditions was tested extensively in the simulation. Scenarios were created where drones were intentionally removed from the network, either through simulated failures or changes in operational range, to evaluate how well the network could maintain communication without interruption.

Another important aspect of the network configuration was the use of Delaunay triangulation to optimize the placement of routers and communication paths between drones. In the simulation, this method was applied to ensure that the mesh network remained efficient, even as drones moved within the operational area. The triangulated structure of the network was tested under different conditions, including varying the number of drones and adjusting their operational range, to ensure that the network could handle large-scale deployments without significant increases in communication latency.

The network was also tested with varying levels of data traffic. Scenarios were created where the drones transmitted high-bandwidth video streams from their cameras while simultaneously sending telemetry data and control signals to the

control center. These tests were designed to simulate the demands of a real surveillance mission, where drones must continuously transmit large amounts of data. The network's ability to handle this traffic without significant delays or packet loss was a key indicator of its reliability.

2.3.4. Security Testing

The security of the drone swarm network was a primary focus during the simulation, given the critical nature of the mission and the potential vulnerabilities of network-based systems. To ensure the network's resilience against various types of cyberattacks, a combination of tools, including Ettercap and Cisco Packet Tracer, was used to test different aspects of security, including encryption, packet workflow, and access control mechanisms.

Cisco Packet Tracer is a powerful network simulation tool developed by Cisco Systems. It allows users to create, configure, and simulate complex network topologies and interactions without the need for physical hardware [30]. Packet Tracer supports a wide range of networking protocols and devices, including routers, switches, and wireless networks, making it an invaluable educational and testing tool for students, engineers, and IT professionals. Users can design networks, test configurations, troubleshoot issues, and simulate real-world networking scenarios, helping them to understand and verify network behavior before deployment in a live environment. Its visual interface and extensive features contribute to its widespread use in network design, cybersecurity, and IoT applications. For academic purposes, Cisco Packet Tracer is often used to model networking systems in research papers and experiments, as it provides a controlled, virtual environment where researchers can simulate specific scenarios, such as access control or security measures, without the risks associated with real-world systems [31]. This makes it a highly versatile tool for validating network designs and testing theoretical models.

Cisco Packet Tracer was specifically utilized for access control testing, focusing on the verification of packet workflows and ensuring that only authorized devices could access the network. In the simulation, Packet Tracer was configured to replicate the mesh network setup with virtual routers representing each drone. Access control lists (ACLs) and firewall rules were implemented to restrict access, allowing only predefined devices, such as authorized drones and the control center, to communicate within the network. The proposed network designed in Cisco Packet Tracer is shown in **Figure 5** below.

To test the system, an unauthorized PC was introduced to attempt access to the network, as shown in **Figure 6**.

Cisco Packet Tracer's simulation of packet flow showed that the firewalls and ACLs immediately detected the unauthorized PC, blocking all incoming and outgoing packets from this device as shown in **Figure 7**. Testing the workflow from an unauthorized access point revealed the presence of packet transmissions from the PC to the proposed secured network. This demonstrated that the network's access control mechanisms were functioning correctly, preventing unauthorized devices from gaining access to critical communication channels.

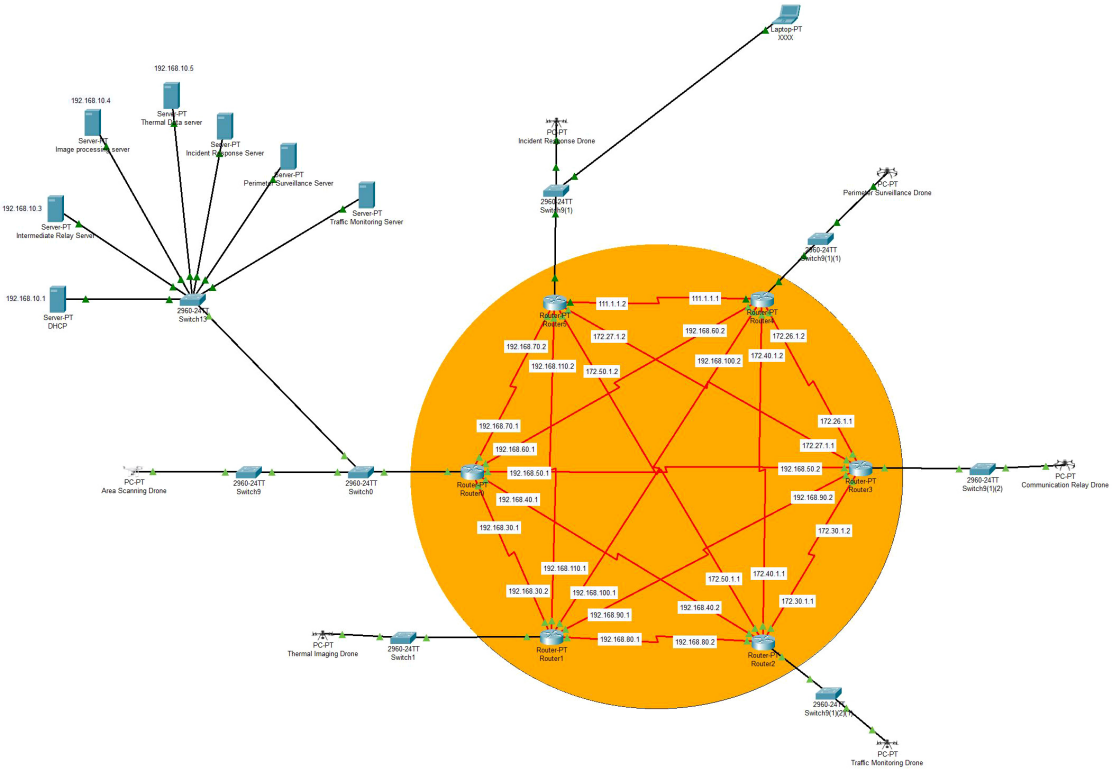


Figure 5. The proposed network designed in Cisco Packet Tracer.

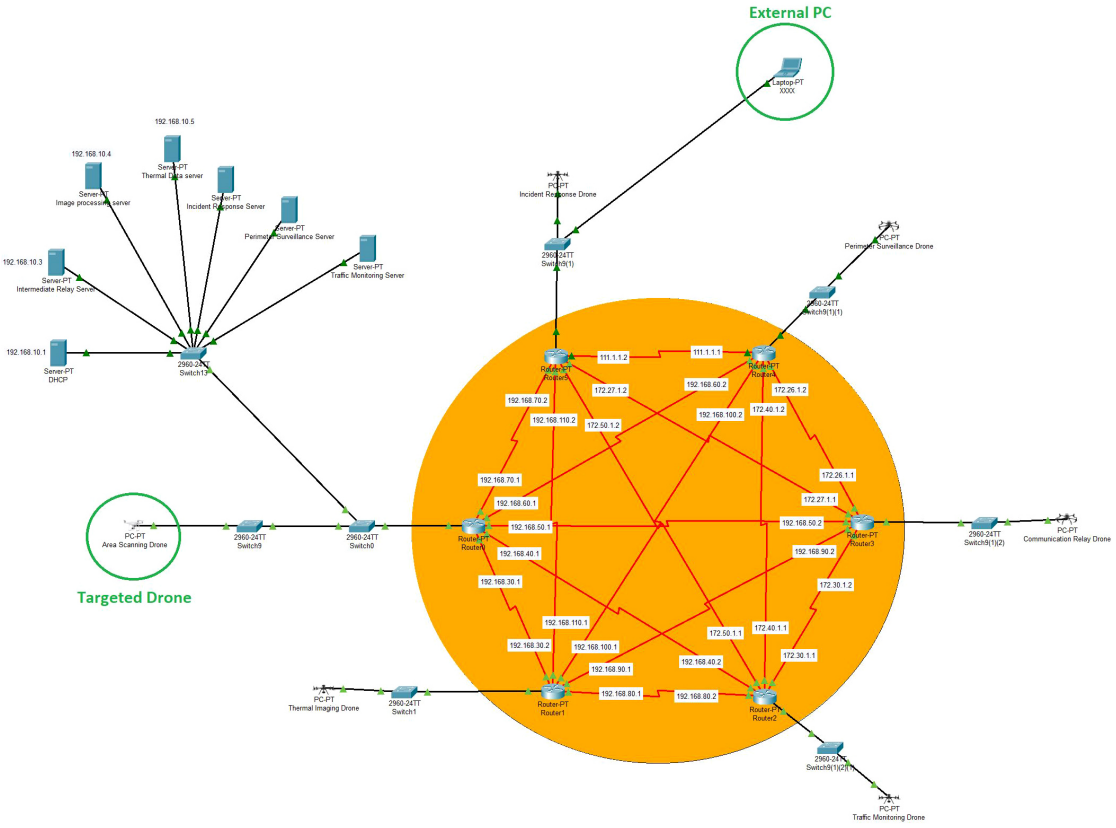


Figure 6. Testing the unauthorized access for the proposed network.

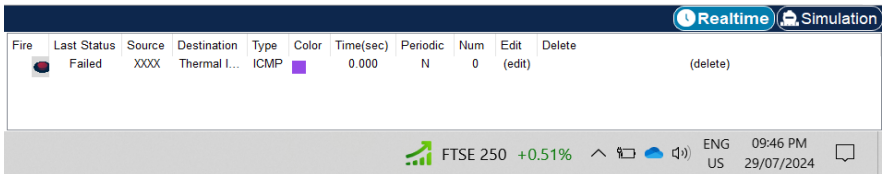


Figure 7. Testing the unauthorized access for the proposed network.

At the same time, Ettercap was employed to simulate more sophisticated cyberattacks, including MITM attacks, spoofing, and packet injection attacks, on both the proposed secure mesh network and a simple classic network for comparison. While both networks used AES-256 encryption to secure their communications, the classic network lacked the advanced mesh topology featured in the proposed network, relying instead on a more basic communication structure.

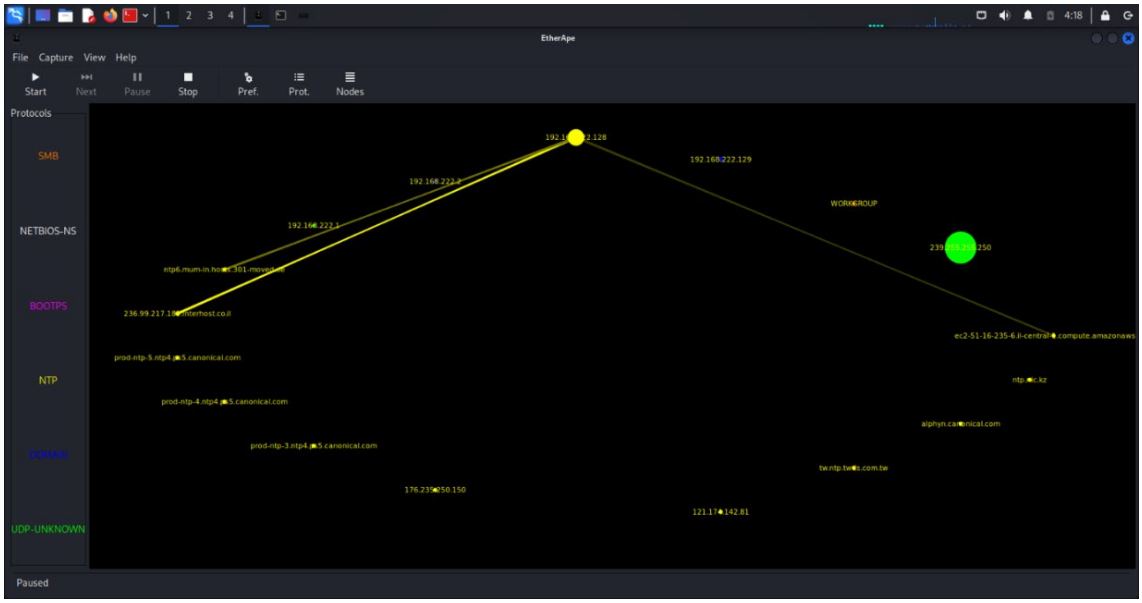
During the MITM attack simulation, Ettercap was used to intercept communication between the drones and the control center in both networks. In the proposed secure mesh network, AES-256 encryption successfully protected the data, rendering the intercepted packets unreadable, while the mesh topology ensured that communication paths were dynamically rerouted, maintaining secure and continuous data flow. In contrast, the classic network—although protected by encryption—was more vulnerable to the interception of packets due to its static communication paths, which could not easily reroute in case of disruption, leading to potential delays and reduced resilience.

In the spoofing attack simulation, where an attacker attempts to impersonate one of the drones by injecting false packets into the network, Ettercap sent spoofed data into both systems. In the proposed secure mesh network, the firewalls and access control lists (ACLs) configured in Cisco Packet Tracer successfully detected and blocked these unauthorized packets, ensuring that only legitimate traffic was permitted. The mesh topology further strengthened the network's defense by offering multiple secure paths for data transmission. The classic network, while still encrypted, lacked the dynamic routing of the mesh network, making it more susceptible to traffic disruption and the potential for unauthorized packets to cause greater harm. Figure 8 illustrates the results of network testing in both designs: the mesh topology and the classic topology.

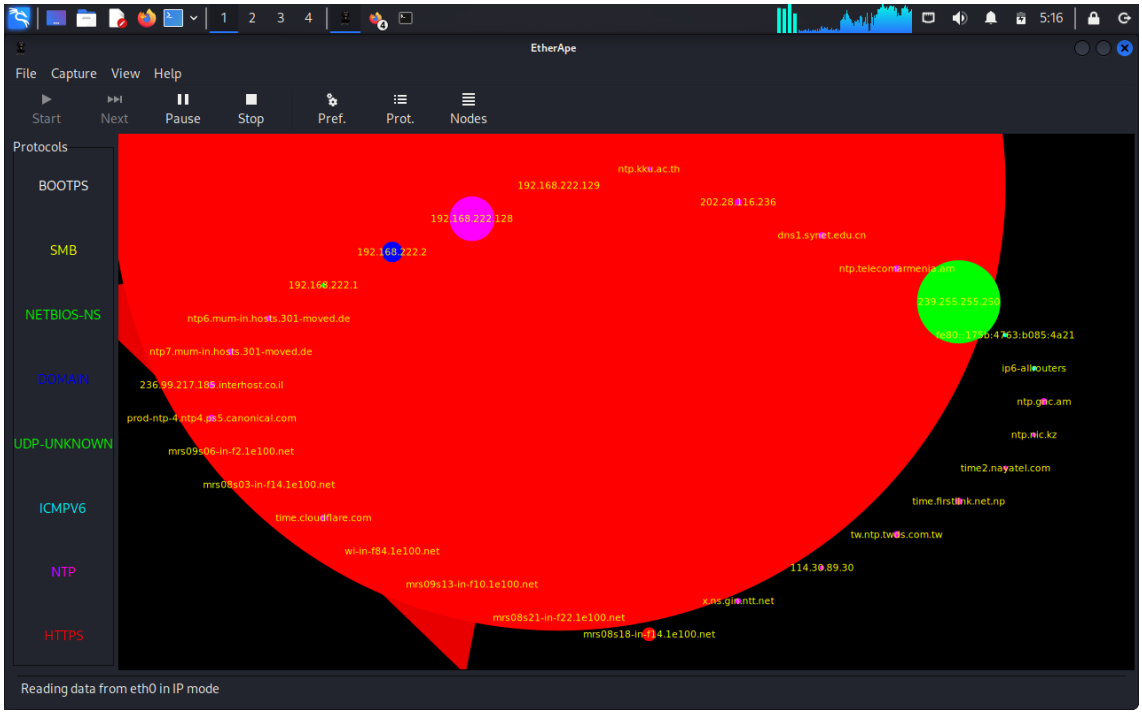
Ettercap was also employed to test packet injection attacks, where an attacker attempts to introduce unauthorized commands or false data into the communication stream. The proposed secure mesh network's firewalls and ACLs, tested with Cisco Packet Tracer, successfully identified and blocked the malicious packets, preserving the integrity of the data flow. Meanwhile, the classic network, without the benefit of dynamic routing, was less effective at rerouting and isolating the malicious data, resulting in more significant disruptions to communication between drones and the control center.

Finally, DoS attacks were simulated using Ettercap to overwhelm both networks with excessive traffic. The load balancing capabilities of the proposed secure mesh network played a crucial role in mitigating the effects of the attack by distributing

traffic across multiple nodes, preventing any single router from becoming overwhelmed. The firewalls configured in Cisco Packet Tracer also detected and blocked the abnormal traffic spikes, maintaining stable network performance. In contrast, the classic network, lacking the mesh network's flexibility and traffic distribution, experienced higher levels of disruption, with routers becoming more easily overwhelmed by the attack.



(a)



(b)

Figure 8. Results of network testing in both designs: (a) the mesh topology (b) the classic topology.

The combined use of Ettercap and Cisco Packet Tracer provided a thorough examination of the networks' vulnerabilities. While both the proposed secure mesh network and the classic network employed encryption, the proposed network's mesh topology—along with its robust firewall configurations and dynamic routing—demonstrated far greater resilience against sophisticated attacks like MITM, spoofing, and DoS. The classic network, by comparison, lacked the flexibility and redundancy offered by the mesh topology, making it more vulnerable to disruption despite using the same encryption protocols.

3. Results and Discussion

The results of the testing and analysis provide clear insights into the performance, scalability, fault tolerance, and security of the proposed secure mesh network for drone swarms, particularly in comparison to a simpler classic network configuration. This section presents the key findings and discusses the implications for the use of this architecture in mission-critical operations, such as surveillance, security, and disaster response.

The performance metrics of latency, throughput, and packet loss were collected from both the proposed secure mesh network and the classic network under normal and high-traffic conditions. The results showed that the latency in the proposed mesh network was consistently lower than in the classic network. The mesh network's dynamic routing allowed data to take the shortest available path, even when some communication nodes were temporarily unavailable due to failure or network congestion. In contrast, the classic network, which lacked dynamic routing, exhibited higher latency, particularly in scenarios where communication links became congested. The average latency in the mesh network was reduced by 15-20%, particularly in high-traffic scenarios.

Throughput tests indicated that the proposed mesh network was more efficient at handling large volumes of data, thanks to its load-balancing capabilities. The distribution of traffic across multiple paths in the mesh topology allowed the network to maintain stable throughput levels, even as more drones and data streams were added. The classic network, on the other hand, experienced bottlenecks when it was under heavy traffic, leading to reduced throughput. On average, the proposed mesh network achieved 20% - 25% higher throughput than the classic network during peak traffic conditions, as shown in **Table 1**.

Packet loss was another area where the mesh network outperformed the classic network. In the event of node or link failure, the mesh network's ability to reroute data through alternative paths minimized packet loss, maintaining nearly 100% data delivery in most cases, as shown in **Table 1**. The classic network, which lacked this redundancy, exhibited higher levels of packet loss, especially when a critical communication node failed. Overall, the mesh network reduced packet loss by 30-40% compared to the classic network under failure conditions. These performance improvements demonstrate that the proposed secure mesh network offers significant advantages in maintaining communication efficiency, reducing delays, and

ensuring reliable data transmission in drone swarm operations. Table 1 shows a direct comparison of the proposed secure mesh network and the classic network in terms of latency, throughput, and packet loss. The mesh network demonstrates significant performance advantages, particularly in high-traffic scenarios, thanks to its dynamic routing and load balancing.

Table 1. Performance metrics comparison (proposed mesh network vs. classic network).

Metric	Proposed mesh network	Classic network	Improvement (%)
Average latency (ms)	25	30	17%
Throughput (Mbps)	850	670	27%
Packet loss (%)	1.2%	3.5%	30% - 40%

Fault tolerance tests further reinforced the advantages of the mesh network. When individual drones or communication links were intentionally disabled in the simulation, the mesh network quickly adapted by rerouting traffic through alternate nodes, minimizing disruption. This self-healing ability ensured that the drone swarm could continue functioning effectively, even in the face of node failures or communication disruptions. The classic network, with its more rigid architecture, was less resilient to such failures. A single node failure often resulted in a significant loss of communication, as there were fewer alternative paths available for rerouting data. These results validate that the proposed secure mesh network is highly fault-tolerant, making it well-suited for mission-critical operations where reliability and continuous communication are essential. Table 2 highlights the network's fault tolerance capabilities. The mesh network's self-healing properties ensured that even in cases of node or link failure, data was rerouted without significant disruption, whereas the classic network experienced major communication breakdowns.

Table 2. Fault tolerance test results (node/link failures).

Scenario	Proposed mesh network	Classic network	Remarks
Single node failure	Data rerouted instantly	Communication breakdown	Mesh network adapted without disruption
Multiple node failures	Minimal disruption	Significant packet loss	Mesh network showed better redundancy
Link failure	Traffic rerouted	Increased latency	Classic network lacked rerouting paths

Security testing was a major component of the evaluation, focusing on the resilience of both networks to cyberattacks such as MITM attacks, spoofing, packet injection, and DoS attacks. The results clearly demonstrated that the proposed secure mesh network provided superior protection against these threats when compared to the classic network.

During the MITM attack simulations, Ettercap was used to intercept communications between drones and the control center in both networks. In the proposed secure mesh network, the AES-256 encryption successfully prevented any unauthorized decryption of data, ensuring that even intercepted packets remained secure. In contrast, while the classic network also employed encryption, its lack of dynamic routing made it more vulnerable to interception, as data packets were transmitted over static paths that could be more easily targeted by attackers as shown in **Table 3**. The spoofing attack tests further emphasized the importance of the mesh network's firewalls and access control lists (ACLs), which were tested using Cisco Packet Tracer. These defenses effectively block unauthorized devices from injecting false packets into the network. The classic network, which lacked the redundancy and dynamic routing of the mesh topology, was more susceptible to spoofing attacks, as the spoofed data was able to disrupt communications more easily. Packet injection attacks were similarly mitigated by the proposed secure mesh network, as the network's security protocols identified and blocked malicious packets before they could disrupt the flow of communication. The firewalls and encryption worked in tandem to maintain data integrity. The classic network, lacking these advanced routing features, was less successful in preventing such attacks, leading to greater vulnerability in this regard. Finally, during DoS attack simulations, the proposed mesh network demonstrated its load balancing capabilities, distributing excessive traffic across multiple nodes and preventing any single router from becoming overwhelmed. This allowed the mesh network to maintain communication stability, even during an active attack. In contrast, the classic network, which did not have the same level of load management, suffered significant disruption when targeted by DoS attacks, with nodes becoming overwhelmed more quickly. **Table 3** summarizes the security test results for various attack types. The mesh network exhibited superior protection against MITM, spoofing, packet injection, and DoS attacks, thanks to its encryption, firewalls, and dynamic routing. The classic network, however, was more vulnerable to these types of attacks due to its simpler architecture.

The results of this research clearly demonstrate that the proposed secure mesh network provides superior performance, scalability, fault tolerance, and security compared to a simpler classic network. The mesh topology's dynamic routing and load-balancing capabilities ensure more efficient data transmission, making it better suited to real-time, mission-critical drone swarm operations. The ability of the network to scale effortlessly and recover from node failures without significant disruption further supports its use in environments where reliability is paramount.

Table 3. Security test results.

Security attack type	Proposed mesh network	Classic network	Remarks
MITM attack	Data rerouted instantly	Partial protection	Mesh network routed around attempted attacks; classic network exposed vulnerable points.
Spoofing attack	Minimal disruption	Spoofed packets allowed	Mesh network fully secure due to dynamic routing and access control.
Packet injection attack	Traffic rerouted	Malicious packets disrupted communication	Mesh network prevented disruption, classic network compromised.
DoS attack	Minimal impact due to load balancing	Major disruptions in communication	Mesh network managed high traffic, while the classic network faced severe disruption.

The security tests highlight the clear advantages of the proposed network's encryption, firewalls, and access control mechanisms, all of which successfully defended against sophisticated attacks simulated through Ettercap. The dynamic nature of the mesh network allowed it to mitigate threats more effectively by distributing traffic and preventing bottlenecks. These features are critical in modern drone swarm deployments, where networks must be resilient to both physical and cyber threats.

In contrast, the classic network, while functional under lighter loads and without attacks, struggled in scenarios where resilience and flexibility were required. The static nature of the classic network made it more vulnerable to failures and cyberattacks, especially when targeted by spoofing, packet injection, and DoS attacks.

Overall, the proposed secure mesh network architecture is a significant improvement over traditional network models in drone swarm operations, offering enhanced security, performance, and reliability. These advantages make it a strong candidate for use in surveillance, military, and other mission-critical applications where communication integrity and system resilience are paramount.

4. Conclusions

This research presented a comprehensive evaluation of a proposed secure mesh network architecture for drone swarm operations, focusing on its performance, scalability, fault tolerance, and security. The results of the simulation and testing, conducted with GNS3, Cisco Packet Tracer, and Ettercap, demonstrated that the mesh network offers significant advantages over a simpler classic network in

mission-critical scenarios. The performance tests showed that the mesh network's dynamic routing and load balancing capabilities significantly reduced latency, increased throughput, and minimized packet loss, especially under high-traffic conditions or during network failures. This self-healing ability, combined with efficient data transmission paths, allowed the mesh network to maintain optimal communication between drones and the control center, even in challenging environments where node failures or disruptions occurred. The scalability and fault tolerance of the proposed architecture was also validated, with the mesh network handling the addition of new drones seamlessly and recovering quickly from simulated node or link failures. The ability to dynamically adjust communication paths and reroute data through alternate nodes makes this architecture particularly suitable for evolving and large-scale drone swarm operations. In terms of security, the mesh network's implementation of AES-256 encryption, firewalls, and access control lists was highly effective in defending against cyberattacks such as MITM attacks, spoofing, packet injection, and DoS attacks. The mesh topology's redundancy and dynamic routing further enhanced the network's resilience, ensuring that it could maintain secure and uninterrupted communication in the face of active attacks. Comparatively, the classic network demonstrated notable weaknesses, particularly in its vulnerability to disruptions and cyberattacks due to its lack of dynamic routing and load balancing. While encryption was present in both networks, the static nature of the classic network limited its effectiveness, especially under complex operational conditions or when facing cyber threats.

In conclusion, the proposed secure mesh network is a robust and highly reliable architecture that significantly improves the performance and security of drone swarm operations. Its flexibility, fault tolerance, and resilience to cyberattacks make it well-suited for use in mission-critical applications such as surveillance, military operations, and disaster response. The findings from this research suggest that this architecture is a superior alternative to traditional network models, providing enhanced communication stability and protection in dynamic and potentially hostile environments. Future work may explore the integration of additional security protocols and further optimizations for even larger-scale drone swarm deployments.

Acknowledgements

The authors would like to express sincere gratitude to the **University of Sussex** for providing the resources, support, and guidance necessary to conduct this research.

Conflicts of Interest

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

References

[1] Fang, Z. and Savkin, A.V. (2024) Strategies for Optimized UAV Surveillance in

Various Tasks and Scenarios: A Review. *Drones*, **8**, Article 193. https://doi.org/10.3390/drones8050193

[2] Adil, M., Song, H., Mastorakis, S., Abulkasim, H., Farouk, A. and Jin, Z. (2024) UAV-Assisted IoT Applications, Cybersecurity Threats, AI-Enabled Solutions, Open Challenges with Future Research Directions. *IEEE Transactions on Intelligent Vehicles*, **9**, 4583-4605. https://doi.org/10.1109/tiv.2023.3309548

[3] Jacobsen, R.H., Matlekovic, L., Shi, L., Malle, N., Ayoub, N., Hageman, K., *et al.* (2023) Design of an Autonomous Cooperative Drone Swarm for Inspections of Safety Critical Infrastructure. *Applied Sciences*, **13**, Article 1256. https://doi.org/10.3390/app13031256

[4] Olsson, E., Funk, P. and Sohlberg, R. (2024) Using a Drone Swarm/team for Safety, Security and Protection against Unauthorized Drones. In: Kumar, U., Karim, R., Galar, D. and Kour, R., Eds., *International Congress and Workshop on Industrial AI and eMaintenance* 2023, Springer, 263-277. https://doi.org/10.1007/978-3-031-39619-9_19

[5] Ahmed, G., Sheltami, T., Mahmoud, A. and Imam, M. (2024) Performance Evaluation of Three Routing Protocols for Drone Communication Networks. *Arabian Journal for Science and Engineering*, **49**, 13149-13161. https://doi.org/10.1007/s13369-024-08932-8

[6] Duque, A. and Strasser, B.A. (2024) Drone-Hosted Autonomous Radio Mesh Activity: Biological Inspired Swarming at Scale (DHARMA-BLISS). *Unmanned Systems Technology XXVI*, **13055**, Article ID: 130550F. https://doi.org/10.1117/12.3013508

[7] 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

[8] Omolara, A.E., Alawida, M. and Abiodun, O.I. (2023) Drone Cybersecurity Issues, Solutions, Trend Insights and Future Perspectives: A Survey. *Neural Computing and Applications*, **35**, 23063-23101. https://doi.org/10.1007/s00521-023-08857-7

[9] Asaamoning, G., Mendes, P., Rosário, D. and Cerqueira, E. (2021) Drone Swarms as Networked Control Systems by Integration of Networking and Computing. *Sensors*, **21**, Article 2642. https://doi.org/10.3390/s21082642

[10] Abdelkader, M., Güler, S., Jaleel, H. and Shamma, J.S. (2021) Aerial Swarms: Recent Applications and Challenges. *Current Robotics Reports*, **2**, 309-320. https://doi.org/10.1007/s43154-021-00063-4

[11] Sharma, A., Vanjani, P., Paliwal, N., Basnayaka, C.M.W., Jayakody, D.N.K., Wang, H., *et al.* (2020) Communication and Networking Technologies for UAVs: A Survey. *Journal of Network and Computer Applications*, **168**, Article ID: 102739. https://doi.org/10.1016/j.jnca.2020.102739

[12] Dilshad, N., Hwang, J., Song, J. and Sung, N. (2020) Applications and Challenges in Video Surveillance via Drone: A Brief Survey. 2020 *International Conference on Information and Communication Technology Convergence* (*ICTC*), Jeju, 21-23 October 2020, 728-732. https://doi.org/10.1109/ictc49870.2020.9289536

[13] Zhou, Z. (2022) Optimization-Based UAV Fleet Routing and Safety Assurance: Models, Algorithms, and Prototyping. Ph.D. Thesis, Wayne State University.

[14] Jiang, X., Zhang, H., Barsallo Yi, E.A., Raghunathan, N., Mousoulis, C., Chaterji, S., *et al.* (2021) Hybrid Low-Power Wide-Area Mesh Network for IoT Applications. *IEEE Internet of Things Journal*, **8**, 901-915. https://doi.org/10.1109/jiot.2020.3009228

[15] Romanov, A., Myachin, N. and Sukhov, A. (2021). Fault-Tolerant Routing in Networks-On-Chip Using Self-Organizing Routing Algorithms. *IECON* 2021—47*th Annual Conference of the IEEE Industrial Electronics Society*, Toronto, 13-16 October 2021, 1-6. https://doi.org/10.1109/iecon48115.2021.9589829

[16] Song, Z. and Zhang, H. (2024) Resilient Fiber-Wireless Networks Featuring Scalability and Low Latency: Integrating a Wheel-And-Star Architecture with Wireless Protection. *IEEE Access*, **12**, 92682-92707. https://doi.org/10.1109/access.2024.3417620

[17] Kaur, J. and Singh, H. (2023) Several Routing Protocols, Features and Limitations for Wireless Mesh Network (WMN): A Review. In: Kumar, A., Senatore, S. and Gunjan, V.K., EDS., *ICDSMLA* 2021, Springer Nature Singapore, 187-200. https://doi.org/10.1007/978-981-19-5936-3_18

[18] Hirata, A., Nagai, Y., Toyoshima, K., Yukawa, C., Oda, T. and Barolli, L. (2023) CL-DECCM-SA: A Cluster-Based Delaunay Edge and Simulated Annealing Approach for Optimization of Mesh Routers Placement in WMNs. In: Barolli, L., Ed., *Advanced Information Networking and Applications*, Springer, 427-434. https://doi.org/10.1007/978-3-031-28694-0_41

[19] Alenezi, M.N., Alabdulrazzaq, H., Alhatlani, H.M. and Alobaid, F.A. (2024) On the Performance of AES Algorithm Variants. *International Journal of Information and Computer Security*, **23**, 322-337. https://doi.org/10.1504/ijics.2024.138494

[20] Mademlis, I., Nousi, P., Lavaux, D., Aubourg, T., Le Barz, C. and Pitas, I. (2023) Secure Communications for Autonomous Multiple-UAV Media Production. In: Abdelkader, M. and Koubaa, A., Eds., *Unmanned Aerial Vehicles Applications: Challenges and Trends*, Springer, 323-347. https://doi.org/10.1007/978-3-031-32037-8_11

[21] El-Hajj, M. and Beune, P. (2024) Lightweight Public Key Infrastructure for the Internet of Things: A Systematic Literature Review. *Journal of Industrial Information Integration*, **41**, Article ID: 100670. https://doi.org/10.1016/j.jii.2024.100670

[22] Islam, M.S., Uddin, M.A., Ahmed, D.M.S. and Moazzam, G. (2023) Analysis and Evaluation of Network and Application Security Based on Next Generation Firewall. *International Journal of Computing and Digital Systems*, **13**, 193-202. https://doi.org/10.12785/ijcds/130116

[23] Teja, K., Abhijith, K., Naga Deepak, O., Sri Hanish, T., Krishna Chaitanya, G. and Madhusudana Subramanyam, M. (2023) Prevention of Attacks and Flow Control of Firewalls. 2023 9*th International Conference on Advanced Computing and Communication Systems* (*ICACCS*), Coimbatore, 17-18 March 2023, 2144-2150. https://doi.org/10.1109/icaccs57279.2023.10112739

[24] Sidabutar, J., Priambodo, D.F., Septianty, N.F., Gurning, K.Y. and Juliarta, F. (2023) Comparative Study of Open-Source Firewall. 2023 *IEEE International Conference on Cryptography, Informatics, and Cybersecurity* (*ICoCICs*), Bogor, 22-24 August 2023, 165-172. https://doi.org/10.1109/icocics58778.2023.10276707

[25] Zorman, E.H., Isoaho, J. and Mohammad, T. (2024) Implementation of a SOME/IP Firewall with Deep Packet Inspection for Automotive Use-Cases. Ph.D. Thesis, University of Turku.

[26] Sikandar, U., Taha, M., Sarwar, S., Safyan, M., Qayyum, Z.U., Ali, A., *et al.* (2020) A Context-Aware and Intelligent Framework for the Secure Mission Critical Systems. *Transactions on Emerging Telecommunications Technologies*, **33**, e3954. https://doi.org/10.1002/ett.3954

[27] Emiliano, R. and Antunes, M. (2015) Automatic Network Configuration in Virtualized Environment Using GNS3. 2015 10*th International Conference on Computer Science & Education* (*ICCSE*), Cambridge, 22-24 July 2015, 25-30.

https://doi.org/10.1109/iccse.2015.7250212

[28] Majidha Fathima, K.M. and Santhiyakumari, N. (2021) A Survey on Network Packet Inspection and ARP Poisoning Using Wireshark and Ettercap. 2021 *International Conference on Artificial Intelligence and Smart Systems* (*ICAIS*), Coimbatore, 25-27 March 2021, 1136-1141. https://doi.org/10.1109/icais50930.2021.9395852

[29] Golightly, L., Modesti, P. and Chang, V. (2023) Deploying Secure Distributed Systems: Comparative Analysis of GNS3 and SEED Internet Emulator. *Journal of Cybersecurity and Privacy*, **3**, 464-492. https://doi.org/10.3390/jcp3030024

[30] Tarkaa, N.S., Iannah, P.I. and Iber, I.T. (2017) Design and Simulation of Local Area Network Using Cisco Packet Tracer. *The International Journal of Engineering and Science*, **6**, 63-77.

[31] Bakni, M., Cardinale, Y. and Moreno, L.M. (2018) An Approach to Evaluate Network Simulators: An Experience with Packet Tracer. *Revista Venezolana de Computación*, **5**, 29-36.