World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(Review Article)

A comprehensive overview of privacy, security and performance issues in flying Ad Hoc Networks

Emmanuel Asituha *

Jaramogi Oginga Odinga University of Science and Technology, 40601, Bondo

World Journal of Advanced Research and Reviews, 2024, 23(01), 1902–1930

Publication history: Received on 08 June 2024; revised on 15 July 2024; accepted on 18 July 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.23.1.2166

Abstract

Flying Ad Hoc Networks (FANETs) represent an ever evolving area in wireless network communications, despite this massive achievements, FANETs faces significant security, privacy, and performance issues due to their highly mobile and decentralized nature. This paper aims to address these challenges, focusing on robust privacy, security, and efficient performance in dynamic environments with frequent topology changes and high data demands. Existing solutions, including cryptographic techniques and secure routing protocols, show limitations in adaptability and efficiency. This paper reviews these issues, identifying gaps such as the need for adaptive security measures and improved communication protocols. The proposed methodology includes advanced encryption, secure key management, continuous threat monitoring, and adaptive communication strategies. The results highlight opportunities for improvement, emphasizing the development of resilient security frameworks and efficient data management. Addressing these issues will enhance FANET reliability and effectiveness, supporting broader applications in military operations, disaster management, and environmental monitoring.

Keywords: Flying Ad Hoc Networks; MANETs; VANETs; Decentralized Networks; Security issues; Privacy issues.

1. Introduction

Flying Ad Hoc Networks are wireless communication networks that specialized types of MANETs (Mobile Ad Hoc Networks) that consist of unmanned aerial vehicles (UAVs) to establish communication links and work together to achieve the designated goal [1]-[5]. It is a subset of Mobile Ad Hoc Networks (MANETs) specifically designed for unmanned aerial vehicles (UAVs). These networks enable UAVs to communicate with each other and ground stations, forming a dynamic, self-organizing network without relying on a fixed infrastructure. This technology supports various applications, including disaster management, environmental monitoring, and military operations, by providing real-time data exchange [6] and enhanced coordination. Key challenges in FANETs include maintaining connectivity, ensuring data security, and managing the high mobility of UAVs, which necessitate robust and efficient routing protocols and communication strategies. As explained in [7]-[10], FANETs are dynamic in nature because the UAVs are constantly in motion. The advantages of FANETs in adaptability, localization, and scalability poses security, and privacy challenges, making it difficult to establish secure and privacy-oriented communication platform [11] - [16]. In FANETs, ensuring privacy and security is of importance because of their use, for example, FANETs are used in weather forecasting, military operations, terrestrial movement tracking, and many others [17], [18]. The mobility and highly decentralized nature of FANETs increase their vulnerability to various attacks thus making security and privacy a concern [19]-[22]. Protecting the integrity, availability, and confidentiality of the data transmitted within FANETs is crucial to maintaining their reliability and effectiveness [23] - [25]. Without proper security and privacy measures, the entire network could be compromised, leading to data breaches, mission failures, and unauthorized access.

* Corresponding author: Emmanuel Asituha

Security challenges in FANETs poses greater risk to the operations of FANETs. The high mobility of FANETs results in frequent changes in network topology, making it difficult to establish and maintain secure communication links [26]. This ever-changing environment is susceptible to attacks such as eavesdropping [27], where an adversary intercepts sensitive information, and jamming [28], where communication signals are intentionally disrupted. Additionally, FANETs are prone to spoofing attacks, where an attacker masquerades as a legitimate node to gain unauthorized access and denial-of-service attacks, which can overwhelm the network and render it non-operational, and unable to respond to commands from the original sender [29], [30]. Ensuring secure communication in such a volatile environment requires advanced encryption techniques, secure key management, and continuous monitoring for potential threats.

Privacy challenges in FANETs also need as much attention because the data collected and transmitted by UAVs often includes sensitive information, such as real-time location data, surveillance footage, and communication logs [31] - [34]. Unauthorized access to the said information can of gross privacy misconduct. The decentralized nature of FANETs implies that data is often transmitted across multiple nodes, increasing the risk of exposure, for example when one node is vulnerable to attack, the attacker can take advantage of that [35]- [38]. Privacy in FANETs involves protecting the data from external, and internal threats but also ensuring that internal nodes are configured to strict privacy protocols.

Security and privacy solutions for FANETs include the use of advanced cryptographic techniques, secure routing protocols, and intrusion detection systems [39], [40]. It also incorporates the use of encryption methods like AES (Advanced Encryption Standard) and ECC (Elliptic Curve Cryptography) to encrypt the data in transit [41] **-** [46]. Secure routing protocols, for example, ARAN (Authenticated Routing for Ad hoc Networks), which ensure that the secure paths are maintained during data communication. This is in addition to the fact that intrusion detection systems are designed using machine learning principles [47], to identify and mitigate potential threats in real-time [48] **-** [50]. Despite these advancements, continuous research and development are essential to address the evolving challenges and ensure the robust security and privacy of FANETs.

In addition to security and privacy challenges, FANETs also face significant performance issues that impact their efficiency and reliability [51]. The high mobility and frequent topology changes in FANETs lead to increased packet loss and delays, which can degrade the overall network performance [52], [53]. The limited bandwidth available for communication among UAVs can result in congestion, especially in scenarios where multiple UAVs need to transmit large volumes of data simultaneously. This congestion can lead to higher latency and reduced data transmission rates, affecting the timely delivery of critical information [54].

Moreover, the varying flight speeds and altitudes of UAVs introduce additional complexity to maintaining stable communication links **[55]**. Ensuring seamless handoffs and maintaining connectivity in such a dynamic environment is a challenging task. The need for real-time data processing and decision-making in FANET operations further exacerbates these performance issues **[56]**. To address these challenges, it is essential to develop adaptive communication protocols and efficient data management strategies that can handle the dynamic nature of FANETs while ensuring high performance and reliability [57]**-** [59]. Continuous research and innovation are required to overcome these performance bottlenecks and enhance the overall effectiveness of FANETs in various applications.

1.1. Motivation of the Study

This research is motivated by the fact that Flying Ad Hoc Networks, are continuously increasing their dependence on UAVs and their various essential applications like disaster management, military operations, environmental monitoring, and logistics [60], [61]. FANETs provide unique advantages such as adaptability, rapid deployment, cost-effectiveness, and scalability [62]. Nevertheless, these advantages bring substantial privacy and security challenges due to the inherent mobility and decentralized nature of FANETs [63], [64]. Ensuring secure and privacy-preserving communication [65] within these networks is vital for their successful implementation and reliability. This study seeks to thoroughly investigate these challenges, evaluate current solutions, and suggest future research directions to improve the security and privacy of FANETs. of FANETs.

1.2. Research contributions

This research paper provides a comprehensive understanding of the security, and privacy issues of Flying Ad Hoc Networks. The research begins by providing clear grounds for understanding the history, architecture, and applications of FANETs. The findings of this comprehensive study contribute to the existing body of knowledge; providing researchers, industries, and policymakers with a clear understanding and knowledge of the security, and privacy issues in FANETs. The findings of this study offer valuable contributions to the knowledge base on wireless networks, helping in the future design, development, and implementation of secure, and privacy-preserving Flying Ad Hoc Networks:

- *Comprehensive Review*: The study provides a detailed review of the unique privacy and security issues faced by FANETs, highlighting the complexities introduced by their mobile and decentralized nature.
- *Assessment of Current Solutions*: The research evaluates the strengths and limitations of existing solutions designed to address privacy, security, and performance challenges in FANETs, including cryptographic techniques, secure routing protocols, and intrusion detection systems.
- *Identification of Gaps*: The research identifies significant gaps and unresolved issues in the current body of knowledge, emphasizing areas where further investigation is needed.
- *Future Research Directions*: Building on these findings it would be useful to propose potential directions for future research, specialized designs, and implementations to enhance the security and privacy of FANETs.

1.3. Structure

The remainder of this paper is structured as follows: Section 2 covers the methodology used in the research, it also covers the historical evolution and architectural components of FANETs, emphasizing network topologies and communication models. Applications across agriculture, disaster management, and military operations underscore their versatility. A comparative analysis with MANETs and VANETs highlights unique challenges in FANETs. The core sections delve into security, detailing requirements like confidentiality and integrity, analyzing threats such as eavesdropping and spoofing, and assessing current solutions. Privacy concerns encompass data breaches and location tracking, evaluating mitigation strategies such as encryption and data anonymization; performance challenges discussed, delves into issues in Node mobility, bandwidth limitations, and resource constraints challenges. The conclusion analyzes the findings, underscores limitations of current approaches, and advocates for future research enhancing FANET security and privacy measures.

2. Methodology

In this comprehensive study, the following methodologies were employed to systematically review and perform an analysis of existing knowledge on security and privacy challenges in FANETs:

- **Literature Review** A review of existing knowledge on security and privacy issues in FANETs.
- **Security Evaluation:** By using this technique the study aims to identify security issues based on their nature and impact on FANETs operations, common mitigation strategies, and gaps that has not been addressed.
- **Privacy Assessment:** The research assesses the existing solutions in the privacy of FANETs by analyzing their effectiveness, strengths, and limitations in addressing the identified issues.
- **Performance Assessment:** The research delves deep into the current performance challenges, analyzing the solutions available, and addressing the gaps identified.
- **Gap Analysis:** The research aims to identify numerous gaps in the current research and highlight unresolved issues that need further investigation.
- **Proposal of Future Directions:** Based on the findings, the comprehensive research proposes potential research directions with the aim of providing enhanced security and efficient privacy-preserving mechanisms on FANETs. the privacy and security of FANETs

3. FANETs History and Architecture

3.1. FANETs History

The history of FANETs is related to the design, and development of UAVs [66], which the conversation and design started between the 1940s and 1950s with military applications like the German V-1 flying bomb and the Radioplane OQ-2 [67] - [70]. Between1960s to 1980s, UAVs such as the Ryan Firebee were greatly applied in reconnaissance and aerial surveillance [71]-[73]. As more technological advancements were discovered, in the 1990s there were designs such as Predator drones, which specialized in long-distance activities, especially in the military, it was equipped with advanced sensors and wireless communication systems [74].

The idea of FANETs came into play in the 2000s as UAVs began operating with dynamic reconfiguration [75]. Further advancements were made in the 2010s, with an exploration in applications such as disaster management, military operations, weather forecasting, and agriculture [76]. Known big projects like the DARPA's Gremlins Program, which focuses on mid-air launch and recovery of UAVs [77], [78], and the European Union's SESAR Project, which was aimed at integrating UAVs into the air traffic management system, with an emphasis on building and implementing a secure and privacy-preserving wireless communication system [79]-[82].

3.2. General FANETs Architecture

Flying Ad Hoc Networks (FANETs) represent a unique type of Mobile Ad Hoc Networks (MANETs), designed specifically for unmanned aerial vehicles (UAVs) [83] - [85]. They stand out for their dynamic, decentralized, and remarkably adaptable architecture, facilitating seamless communication and cooperation among UAVs to achieve the set goals, as eset goals as evident in Figure 1[86]. This unique framework is particularly advantageous in scenarios where conventional communication networks are insufficient or non-existent, including remote regions, disaster-stricken areas, and hostile environments [87], [88]. FANETs thus serve as a critical technology for enhancing operational capabilities and extending the reach of UAV missions across diverse and challenging landscapes [89]-[91].

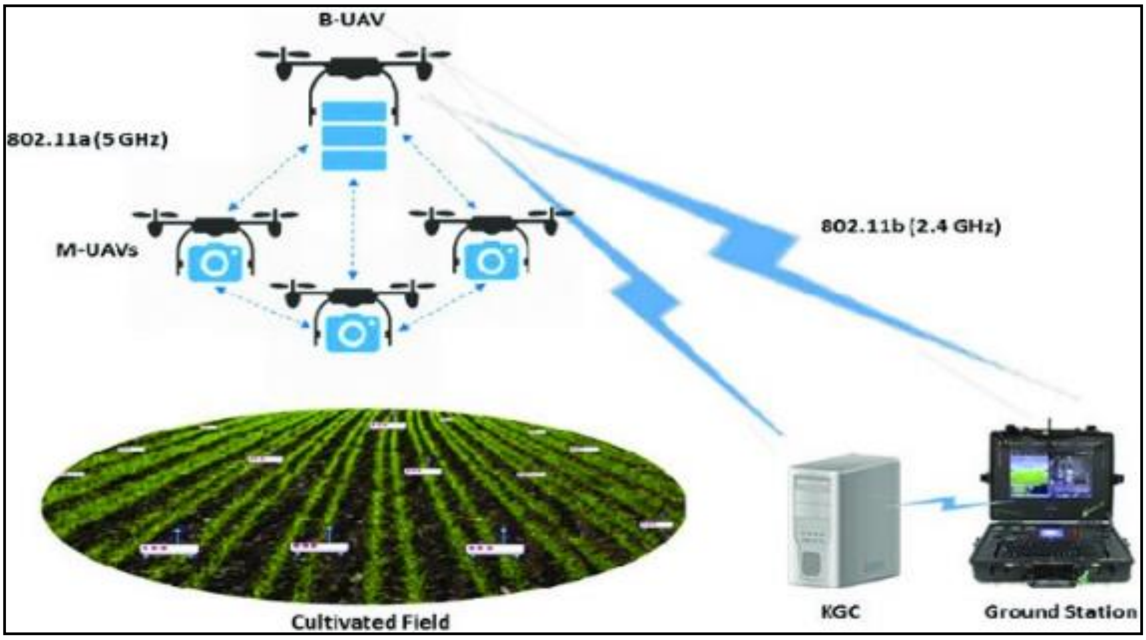

Figure 1 Basic Architecture of FANETs

3.3. Components of FANETs

One of the major components of FANETs is the UAV which functions as an autonomous mobile node, equipped with several essential components, including communication modules, sensors, and processing units as shown in Figure 2 [92]. The communication modules do facilitate data exchange between UAVs using various technologies, while the sensors, such as cameras, LiDAR, and thermal sensors, gather environmental data [93] - [95]. The onboard processors handle data analysis, decision-making, and control tasks, enabling autonomous operations and real-time responses [96]. FANETs take advantage of multiple communication technologies to ensure efficient connectivity among UAVs, including Wi-Fi for short-range, high-bandwidth communication suitable for dense UAV formations, LTE for broader coverage and higher data rates ideal for medium-range communication, and satellite links essential for long-range communication [97] - [100].

Ground Control Stations (GCS) act as the central point for FANET operations, performing all the activities as directed the operator [101], [102]. They receive data collected by UAVs, which is then processed and analyzed to provide meaningful information.

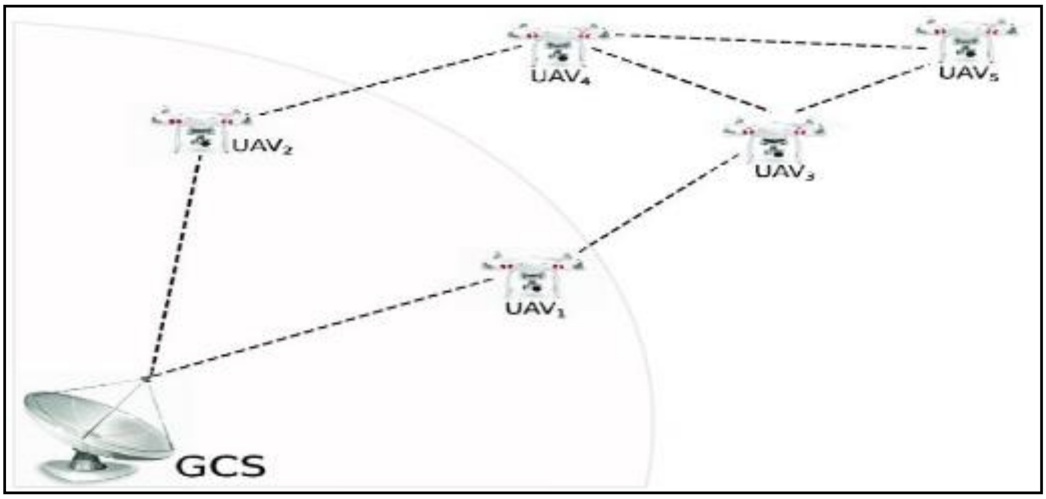

Figure 2 FANETs UAVs

FANETs rely on supportive infrastructure to maintain effective communication and operational efficiency [103], including ground-based base stations that extend communication range and provide additional processing capabilities, and satellites that facilitate global communication coverage and ensure continuous connectivity in remote areas as illustrated in Figure 3 [104].

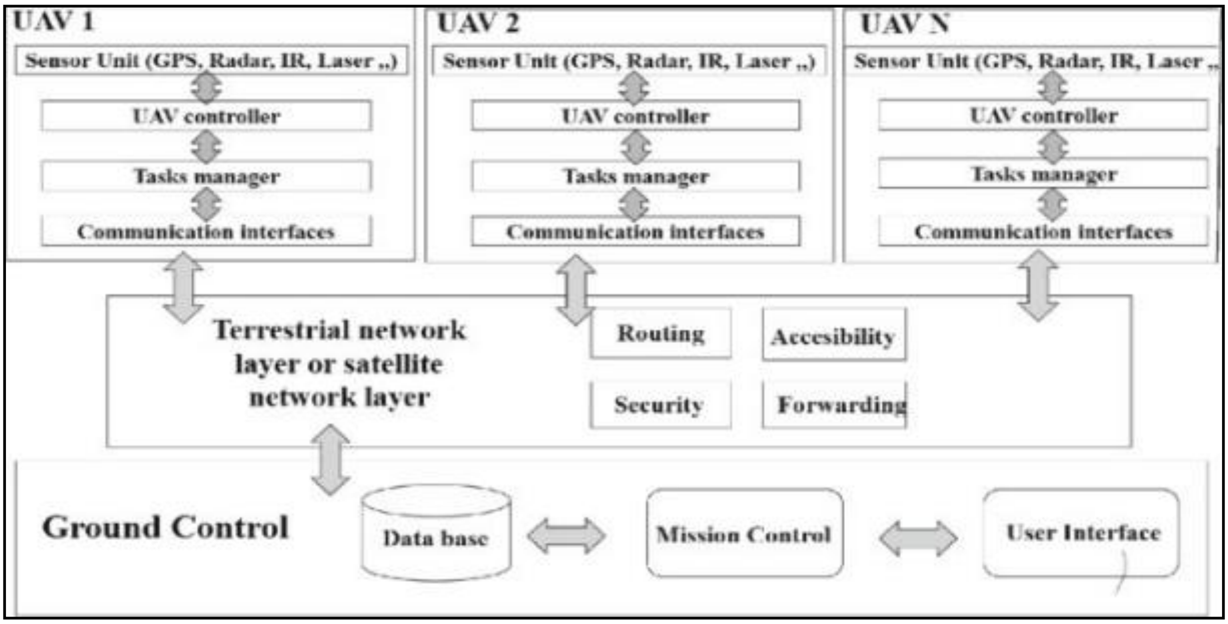

Figure 3 UAV communication architecture with GCS

Communication models in FANETs include single-hop communication, which involves direct communication between UAVs within each other's range and is straightforward and low-latency but limited by the communication range of the UAVs, and multi-hop communication, where data is relayed through multiple UAVs to reach its destination [105], [106]. Network topologies in FANETs majorly is star topology, where all UAVs communicate directly with a central GCS, which is simple to implement and manage but has the significant drawback of relying entirely on the GCS, making the network vulnerable if the GCS fails [107]. Mesh topology allows UAVs to communicate with each other in a peer-to-peer manner [108], forming a robust and redundant network with self-healing capabilities that reroute communication paths if a UAV node fails, enhancing overall reliability [109]. Hybrid topology combines elements of both star and mesh topologies, providing a balance between the simplicity and centralized control of star topology and the robustness and redundancy of mesh topology, improving network performance and resilience against failures [110], [111].

3.4. FANETs Applications

FANETs have diverse applications across multiple fields, leveraging the flexibility and autonomy of UAVs. In disaster management, FANETs facilitate real-time communication and coordination for search and rescue operations, damage assessment, and delivery of essential supplies. Environmental monitoring benefits from FANETs through efficient data collection on air quality, wildlife tracking, and forest fire detection. In agriculture, FANETs enable precision farming by providing detailed aerial surveys, crop health monitoring, and automated irrigation management. Military applications of FANETs include surveillance, reconnaissance, and secure communication in hostile environments. Additionally, FANETs are used in urban planning, traffic management, and telecommunications, showcasing their potential to revolutionize how we collect and disseminate information in various domains. Authors in [112] - [114], discussed the applications of FANETs, and classified them into different categories, as explained in Table 1.

Table 1 FANETs Applications

Application	**Description**	**Example**
Agriculture	Crop Monitoring, Irrigation Management	Smart Farming
Disaster Management	Search and Rescue, Damage Assessment, Medical Delivery	Earthquake Response, Fire Response, LandSlides Response
Environmental	Air Quality Monitoring, Wildlife Tracking	Forest Fire Monitoring
Logistics	Package Delivery	Amazon prime Air
Infrastructure	Inspection of Bridges, Power Lines, and Road Networks.	Utility Maintenance
Military	Surveillance, Target Acquisition, Communication Relay	Border Patrol, Enemies war zone.
Aerial Photography	Film Production, and Events	Drone Cinematography

3.5. Comparison with Other Ad Hoc Networks

Ad hoc networks are decentralized wireless systems, where nodes communicate directly without fixed infrastructure, encompassing types like MANETs, VANETs, and FANETs [115]-[117]. Mobile Ad Hoc Networks (MANETs) are networks of mobile devices with highly dynamic topology, limited bandwidth, and power constraints, commonly used in military communication, disaster recovery, and mobile social networks. Vehicular Ad Hoc Networks (VANETs) are formed by vehicles communicating with each other and roadside infrastructure, known by its high mobility, predictable movement patterns, and frequent topology changes, and used in traffic management, collision avoidance, and infotainment systems [118] - [120].

In comparison, FANETs have three-dimensional mobility necessitating sophisticated control algorithms, typically longer communication ranges due to higher altitudes and line-of-sight advantages and often employ hybrid topologies combining mesh and star elements for robust communication. While all three networks face significant security challenges [121], FANETs demand more advanced solutions because of their unique mobility patterns and operational environments as discussed in Table 2 below [122] - [124].

Table 2 Comparison between MANETs, VANETs, FANETs

Feature	MANETs	VANETs	FANETs
Topology	Mesh, Star	Mesh, Cluster	Hybrid
Communication Range	Limited	Medium	Long
Mobility (Node)	Low	High	Very High
Computational Power	Limited	High	Very High
Density	Low	Very High	Very Low

4. Security, Privacy, and Performance Issues in FANETs

Flying Ad Hoc Networks (FANETs) are considered to be dynamic and decentralized in nature, thus making them vulnerable to a number of security, privacy, and performance attacks [125], [126]. These issues originate from the characteristics of FANETs, such as their mobility, limited computational resources [127], and the open nature of wireless communication. Addressing these challenges is important for ensuring the confidentiality, integrity, and availability of FANET operations in various applications, from military to general uses [128]. This section provides a comprehensive overview of the security and privacy requirements for FANETs, details the major security and privacy challenges, assesses current solutions, and identifies significant gaps in the existing research.

4.1. Security, Privacy, and Performance Requirements for FANETs

To provide effective security of FANETs, the followinh requirements must be fulfilled:

- **Confidentiality**: Confidentiality ensures that sensitive information transmitted across the network is protected from unauthorized access [129]. This is particularly important in military and surveillance applications, for example, confidential data is transmitted from one point to another, even in an unsecured wireless communication environment.
- **Integrity**: Data integrity ensures that the data being communicated from the nodes to UAVs and the Ground Station is not altered or tampered with during transmission [130].
- **Availability:** Availability ensures that the wireless communication networks are accessible to authorized users when needed [131].
- **Authentication**: Authentication verifies and authenticates the identities of communicating entities to prevent unauthorized access to the already set up and working communication systems [132], [133]. This is important because it establishes trust among the UAVs and the ground control stations (GCS).

Privacy in FANETs is a basic requirement; this is because confidential, and sensitive in nature data is collected, processed, and transmitted by the UAVs to the nodes and finally to the Base Station:

- **Data Anonymity**: It protects the identity of the UAVs and the data they collect from unauthorized disclosure is essential to prevent tracking and identification by adversaries [134].
- **Location Privacy**: Hiding the location of the UAVs in action, thus not exposed to unauthorized entities that may interfere with the normal functioning of Flying Ad Hoc Networks [135].
- **Usage Privacy**: Usage privacy ensures protection of information about the purpose and usage of the UAVs preventing adversaries from inferring with the set objectives [136].
- Access Control: Access control provides mechanisms in which all authorized users, authorized UAVs, and Nodes can be able to access and perform activities designated, thus ensuring operations security and data privacy [137]-[139]. In Figure 4, authors in [140] classified security and privacy attacks on the CIA triad.

4.2. Security Challenges in FANETs

The high mobility of UAVs leads to frequent topology changes, making it difficult to maintain stable security measures. Threats include eavesdropping, jamming, spoofing, and Denial of Service (DoS) attacks, which can disrupt communication and compromise data integrity [141]. Additionally, the limited computational resources and power constraints of UAVs hinder the implementation of robust security protocols [142]-[145].

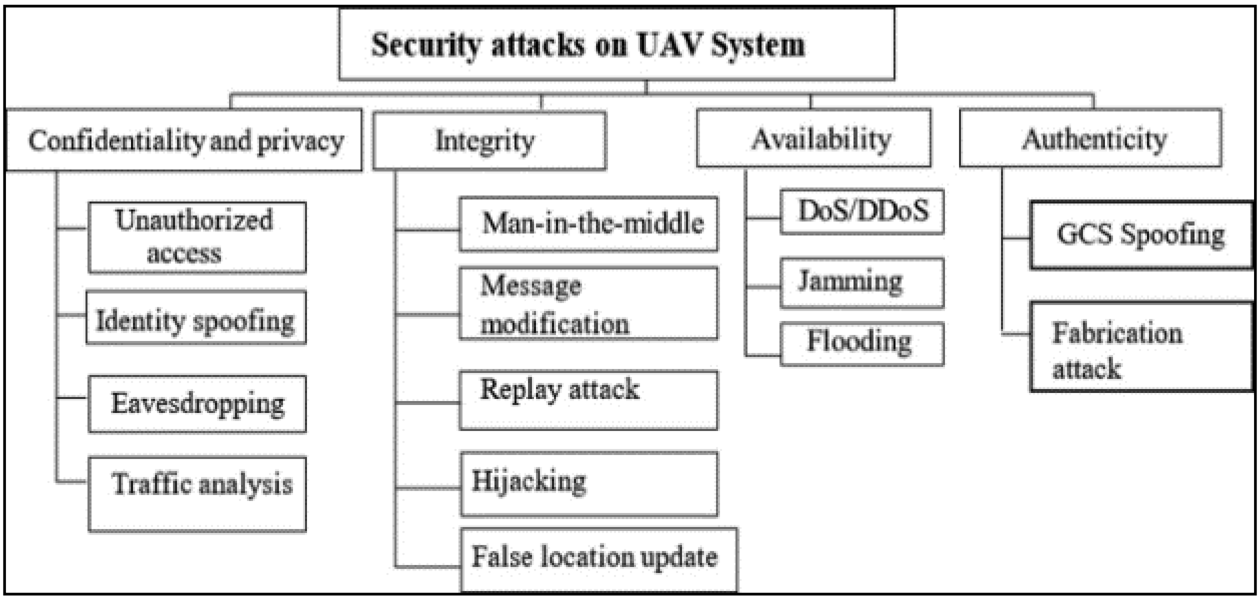

Figure 4 CIA Triad FANETs Attacks

Ensuring secure communication in FANETs requires adaptive and lightweight cryptographic solutions, efficient key management systems, and resilient intrusion detection mechanisms to safeguard against potential vulnerabilities [146]. This research discusses four major types of attacks: eavesdropping, jamming, spoofing, and denial-of-service (DoS) attacks; with a summary of the attacks in Table 3 below.

Table 3 Security Challenges in FANETs

Security Issue	Description	Effects	Probability of Occurrence
Eavesdropping	Intercepting and listening to UAV communication to gain unauthorized access to sensitive information.	Loss of sensitive information, breach of confidentiality and privacy.	Medium
Jamming	Disrupting communication by overwhelming the network with interference.	Disruption of communication between UAVs, mission failure due to loss of control, and decreased availability of network services.	High
Spoofing	Masquerading as a legitimate UAV to gain unauthorized access or manipulate network communication.	Unauthorized control of UAVs, manipulation of mission operations, loss of data integrity and authenticity.	Medium
DOS Attacks	Overwhelming the network with excessive traffic, rendering it incapable of serving legitimate users.	Network downtime and unavailability, operations, and resource exhaustion.	High

4.2.1. Eavesdropping Attack

Eavesdropping involves intercepting and listening to the communication between UAVs, the nodes, and the Ground Station to gain unauthorized access to sensitive data and transmissions. This type of attack exploits the open nature of wireless communication channels, inadequate encryption methods, and insufficient authentication mechanisms [147] - [149]. An attacker can use specialized equipment, such as radio frequency scanners, to tune into the frequency bands used by the UAVs, or even intercept the communications with a fake UAV. By capturing these signals, the attacker can listen to the exchanged data, which may include control commands and other sensitive information.

4.2.2. Jamming Attack

Jamming disrupts communication in FANETs by overwhelming the network with numerous interferences, thus preventing legitimate communication from taking place as evident in Figure 5 [150]. The attack targets the availability of network services by exploiting vulnerabilities such as susceptibility to signal interference and the lack of robust frequency-hopping or spread-spectrum techniques [151] - [154]. This results in disrupted communication between UAVs, potential loss of control, and mission failure. The decreased availability of network services thereby impacting the operational efficiency and effectiveness of the UAVs.

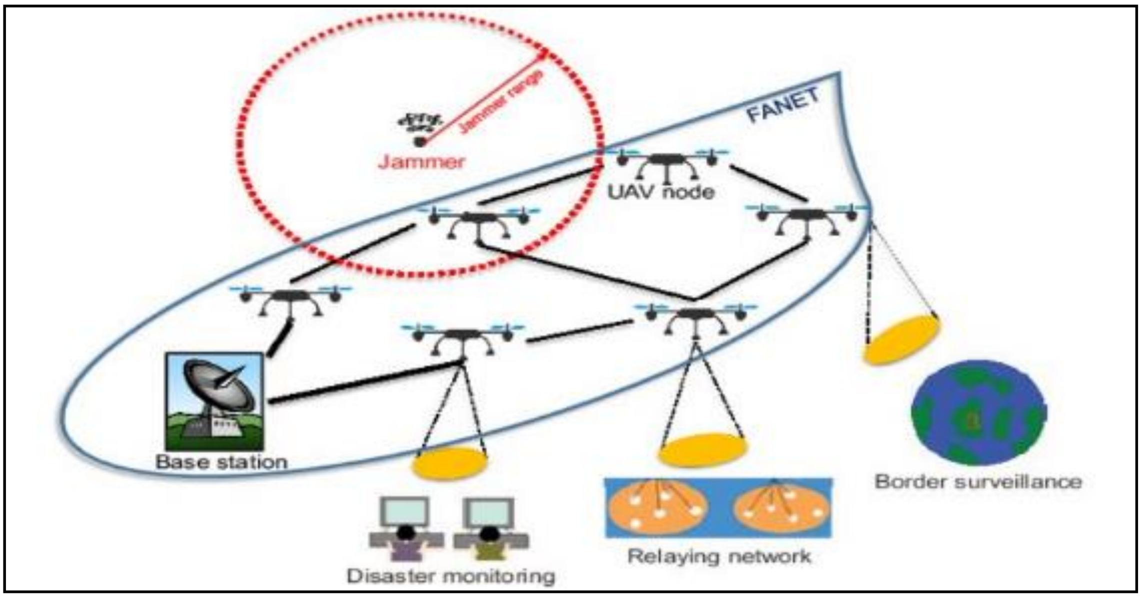

Figure 5 Jamming Attack on FANETs

4.2.3. Spoofing Attack

Spoofing involves an attacker masquerading as a legitimate UAV to gain unauthorized access or manipulate network communication. This attack compromises the integrity and authenticity of the data by exploiting weak authentication protocols and inadequate identity verification mechanisms [155], [156]. The attacker can send false signals or messages, pretending to be a legitimate UAV, to deceive the network into granting access or executing unauthorized commands as shown in Figure 6. As a result, the attacker can gain unauthorized control of UAVs, manipulate operations, and compromise the integrity and authenticity of the data being exchanged within the FANETs architecture [157] - [159]. These attacks involve malicious entities impersonating legitimate UAVs or ground stations to gain unauthorized access to the network. These attacks can deceive UAVs into accepting false data, redirecting their routes, or even hijacking control commands, leading to potential mission failures and security breaches. The high mobility and dynamic nature of FANETs exacerbate the challenge of detecting and mitigating spoofing attacks, as the constantly changing network topology makes it difficult to establish trust among nodes. Effective countermeasures against spoofing attacks include robust authentication mechanisms, such as digital signatures and public key infrastructure (PKI), and continuous monitoring systems that detect anomalies in UAV behavior or communication patterns. However, implementing these solutions is constrained by the limited computational resources and energy availability of UAVs, necessitating lightweight yet effective security measures.

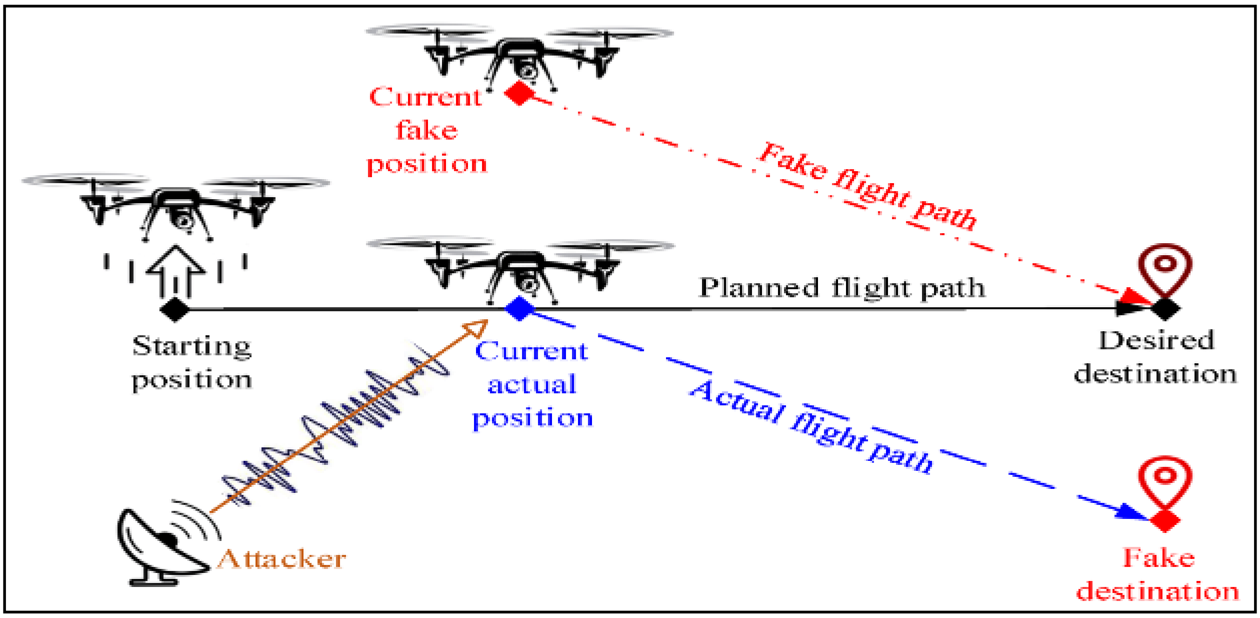

Figure 6 Spoofing Attack

4.2.4. Denial-of-Service (DoS) Attacks

Figure 7 DoS Attack On FANETs

Denial-of-Service (DoS) attacks overwhelm the network with excessive traffic, rendering it incapable of serving legitimate users [160]. As showcased in Figure 7, this attack targets the availability of the network by exploiting limited computational and communication resources and the lack of effective traffic management and filtering mechanisms. The attacker can flood the network with an excessive number of requests or data packets, consuming the available bandwidth and processing capacity [161] -[163]. This leads to network downtime and unavailability of services. The exhaustion of resources significantly impacts the overall performance and reliability of the FANET, hindering its operational capabilities. The aim of DoS attacks is to disrupt the normal operation of the network by overwhelming UAVs or communication channels with excessive traffic or malicious requests. These attacks can degrade network performance, cause loss of critical data, and even immobilize UAVs by exhausting their computational and energy resources. The dynamic and decentralized nature of FANETs, coupled with the high mobility of UAVs, makes it challenging to detect and mitigate DoS attacks. Effective countermeasures include implementing robust intrusion detection systems (IDS) that monitor traffic patterns for anomalies, employing rate-limiting techniques to control the flow of data, and using secure routing protocols that can adapt to changing network conditions. However, the limited processing power and battery life of UAVs constrain the complexity of these security measures, necessitating lightweight yet efficient solutions to ensure network resilience against DoS attacks.

4.2.5. Assessment of Current Security Solutions and Limitations

This research explores various security solutions have been proposed/developed to mitigate the mentioned attacks. Encryption methods, such as Advanced Encryption Standard (AES) and Public Key Infrastructure (PKI), are widely used to protect data integrity and confidentiality, preventing eavesdropping [164] - [167]. However, these methods often face limitations such as increased computational overhead, which can be problematic for UAVs with limited processing power and battery life [169].

Anti-jamming techniques, including spread-spectrum methods like Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS), aim to mitigate jamming attacks. These techniques enhance the resilience of communication channels by making it harder for jammers to disrupt signals [170] - [172]. Nevertheless, these solutions can be complex to implement and may require additional hardware, increasing the overall system cost and complexity.

Authentication protocols, such as digital signatures and mutual authentication schemes, are implemented to prevent spoofing attacks. These protocols verify the identity of UAVs within the network, ensuring that only authorized entities can communicate [173] - [179]. Despite their effectiveness, these protocols may introduce latency and require significant computational resources, which can be challenging for real-time operations in FANETs.

For DoS attacks [180], traffic management and filtering mechanisms, like rate limiting and anomaly detection systems, are used to identify and mitigate excessive traffic [181] - [183]. These mechanisms help maintain network availability by filtering out malicious traffic and prioritizing legitimate requests [184]. However, they can sometimes result in false positives, blocking legitimate traffic and potentially disrupting normal operations.

Table 4 provides a comprehensive overview of the current security solutions in FANETs, along with their limitations.

Table 4 Comprehensive analysis of the security of FANETs and Limitations

Security Attacks	Security Solutions	Limitations
Eavesdropping	Encryption methods (AES, PKI)	Increased computational overhead, limited processing power, and battery life.
Jamming Attacks	Spread-spectrum techniques (FHSS, DSSS)	Complexity of implementation, need for additional hardware, increased system cost and complexity.
Spoofing Attack	Authentication protocols (digital signatures, mutual authentication)	Latency, significant computational resources, challenging real-time operations.
DoS Attacks	Traffic management and filtering mechanisms (rate limiting, anomaly detection)	Potential for false positives, blocking legitimate traffic, and disruption of normal operations.

4.3. Privacy Issues in FANETs

Privacy in FANETs needs critical understanding, given the sensitive nature of the data collected and transmitted by UAVs [185]. Here the research takes a look at four major privacy challenges: data breaches, location tracking [186], inference attacks, and unauthorized data access. These privacy issues arise from the potential for unauthorized access to sensitive data transmitted between UAVs and ground stations, as well as the possibility of tracking and profiling UAVs based on their communication patterns. Given the open wireless communication channels used in FANETs, adversaries can intercept, eavesdrop, or manipulate data, leading to breaches of confidentiality and privacy. Additionally, the integration of FANETs with various applications, such as surveillance, environmental monitoring, and disaster management, heightens the risk of exposing private information about individuals, locations, and activities. Addressing these privacy concerns requires implementing robust encryption techniques, anonymization protocols, and secure data aggregation methods. However, the UAVs' limited computational resources and energy constraints present challenges in deploying comprehensive privacy-preserving measures, necessitating ongoing research for more efficient and adaptive solutions.

4.3.1. Data Breaches

Data breaches involve unauthorized access to sensitive information stored or transmitted by UAVs [187] - [189]. These breaches can occur due to inadequate data encryption and weak access control mechanisms, making it easier for attackers to intercept and access confidential data [190], [191]. Attackers often use techniques such as sniffing or man-in-the-middle attacks to intercept data transmissions between UAVs [192]. When data is not sufficiently encrypted or access controls are not robust, unauthorized parties can exploit these vulnerabilities to gain access to sensitive information. The impact of such attacks includes the exposure of confidential information, resulting in significant legal, and regulatory consequences for the organization.

4.3.2. Location Tracking

Location tracking involves unauthorized monitoring of the real-time locations of UAVs, potentially revealing sensitive operational details [193] - [195]. Attackers exploit vulnerabilities such as the lack of location obfuscation techniques and insufficient use of secure communication channels [196] - [198]. By using techniques like triangulation or signal interception, adversaries can determine the positions and movements of UAVs [199]-[201]. The impact of this attack includes the compromise of mission secrecy, increased risk of physical attacks on UAVs, and a breach of operational privacy [202] - [204]. By tracking the real-time locations of UAVs, adversaries can gain insights into mission details and plan targeted physical attacks [205], thereby undermining the effectiveness and safety of the mission.

4.3.3. Inference Attacks

Inference attacks involve extracting sensitive information from seemingly harmless data through correlation and analysis [206] - [210]. Attackers take advantage of vulnerabilities like inadequate data anonymization and a lack of privacy-preserving techniques. By studying patterns in the data, they can deduce sensitive details [211] that were not explicitly shared as shown in Figure 8, where Participant 1…k is considered as UAVs in a FANETs Architecture [212]. For instance, they might link UAV movements to specific objectives.

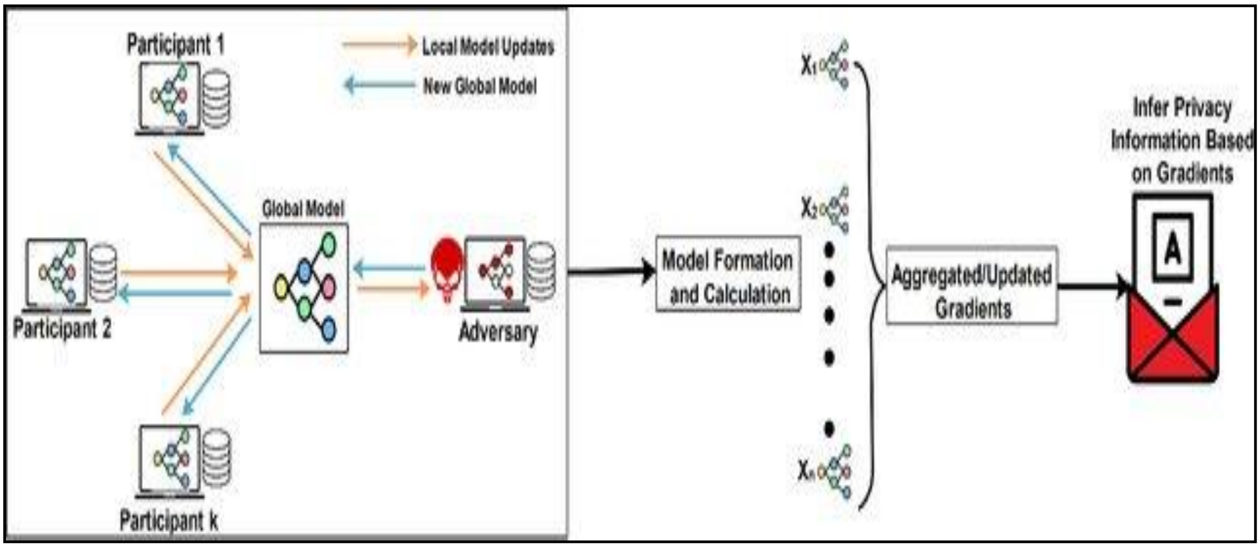

Figure 8 Interference Attack on FANETs Model

The consequences of inference attacks include the accidental disclosure of sensitive information, breaches of data privacy, and the compromise of mission integrity. Even without direct access to sensitive data, attackers can infer crucial details from patterns and correlations, leading to unintended exposure and undermining privacy.

4.3.4. Unauthorized Data Access

Unauthorized data access involves gaining access to sensitive information without proper authorization [213] - [215]. This can occur due to weak authentication mechanisms and inadequate access control policies. Attackers may use methods such as brute force attacks, exploiting default credentials, or exploiting vulnerabilities in access control systems to gain unauthorized entry. The impact of unauthorized data access includes the loss of sensitive data, breaches of data confidentiality, and the potential for data manipulation [216], [217]. Attackers can exploit these vulnerabilities to access critical data without authorization, manipulate the information, and use it for malicious purposes, thereby compromising the security and integrity of the FANETs Model [218] - [221].

5. Assessment of Current Privacy Solutions and Limitations

Current privacy solutions for FANETs focus on encryption, anonymous communication protocols, and secure data aggregation to protect sensitive information transmitted between UAVs and ground stations. Encryption techniques, such as AES and RSA, safeguard data against unauthorized access, while anonymous communication protocols hide the identities and locations of UAVs to prevent tracking and eavesdropping. Secure data aggregation ensures that only aggregated data, rather than raw data, is transmitted, reducing the risk of sensitive information leakage. However, these solutions face limitations due to the UAVs' constrained computational resources and energy supply, which make implementing complex cryptographic algorithms challenging. Additionally, the high mobility and dynamic topology of FANETs complicate the maintenance of robust privacy measures, necessitating ongoing research for more efficient and adaptable privacy-preserving techniques.

5.1. Data Breaches

Current solutions to mitigate data breaches involve the use of robust encryption techniques and access control mechanisms. These measures enhance data confidentiality and limit unauthorized access. However, encryption overhead and complex key management can be challenging for resource-limited UAVs, affecting their performance and operational efficiency [222], [223]. Despite their effectiveness in protecting data, the computational demands of encryption can lead to increased energy consumption and reduced operational time, posing a significant limitation for UAVs with limited resources [224] - [227].

5.2. Location Tracking

To counter location tracking, location obfuscation techniques and secure communication protocols are implemented. These methods protect the real-time location of UAVs, maintaining operational secrecy. However, obfuscation can impact the accuracy and efficiency of operations, making it necessary to balance privacy protection with operational needs [228] - [230]. The trade-off between maintaining the secrecy of UAV locations and ensuring precise and efficient mission execution remains a critical challenge that needs careful management [231]-[234].

5.3. Inference Attacks

Data anonymization and differential privacy techniques are used to mitigate inference attacks. These methods reduce the risk of sensitive information being inferred from data, ensuring better privacy protection [235]-[237]. However, balancing privacy and data utility remains a challenge, requiring careful consideration of both aspects. Ensuring that data remains useful for operational purposes while preventing sensitive information from being inferred is a complex task that often requires sophisticated algorithms and approaches [238], [239].

5.4. Unauthorized Data Access

Multi-factor authentication (MFA) and strict access control policies are deployed to prevent unauthorized data access [240] - [242] . These measures enhance the security of data access, ensuring that only authorized users can access sensitive information. However, MFA can be cumbersome and impact user experience, necessitating user-friendly solutions that do not compromise security [243]. Finding the right balance between security and usability is essential to ensure that these measures are effective without hindering operational efficiency. Table 5, provides a comprehensive summary of the limitations of the current privacy solutions

Table 5 Summary of Limitations

Limitation	Description
Adaptive Privacy Mechanisms	Existing solutions often lack the necessary adaptability to the dynamic nature of FANETs. Developing more flexible privacy mechanisms that can detect and respond to changing network conditions in real-time is crucial for continuous privacy protection.
Balancing Privacy and Performance	Ensuring robust privacy protection without compromising operational efficiency remains a significant challenge. Innovative solutions that balance privacy and performance, such as lightweight cryptographic algorithms and efficient privacy-preserving protocols, are needed
Integrating emerging technologies	Leveraging emerging technologies such as blockchain, AI, and machine learning for enhanced privacy protection in FANETs is still underexplored. Further research is needed to adapt and integrate these technologies effectively into FANETs.
User Awareness and Training	Ensuring that operators and users are aware of privacy best practices is crucial. Current research often overlooks the importance of user awareness and training, highlighting the need for comprehensive training programs and updated guidelines.

6. Performance issues in FANETs

Unique features that make FANETs advantageous also introduce several performance challenges. These challenges range from the high mobility of UAVs, limited bandwidth, susceptibility to interference, and resource constraints. Addressing these issues is crucial to ensuring the efficiency, reliability, and security of FANETs. This paper delves into four unique performance issues in FANETs, exploring how they occur and their impact on network performance, while highlighting the need for innovative solutions to overcome these challenges. Basically, performance issues in FANETs stem from the inherent characteristics of UAVs and the dynamic nature of the network. One primary challenge is maintaining stable and reliable communication links amidst constant changes in topology due to the high mobility of UAVs. This mobility can lead to frequent link breaks, resulting in packet loss, increased latency, and reduced throughput. Moreover, the aerial environment introduces unique factors such as varying altitudes, weather conditions, and obstacles that can affect signal propagation and communication quality. Efficient routing protocols are essential to adapt to these conditions, but their design is complicated by the need to balance responsiveness and resource consumption.

Additionally, the limited computational power and battery life of UAVs impose significant constraints on FANET performance. UAVs must perform multiple tasks, including communication, navigation, and data processing, within their limited energy budgets. High computational demands from complex algorithms can drain batteries quickly, reducing the operational lifespan of the network. This makes energy-efficient protocol design crucial to sustaining network performance over extended periods. Furthermore, the integration of heterogeneous UAVs with different capabilities and performance characteristics can complicate network management and optimization. Ensuring seamless interoperability and efficient resource utilization in such diverse environments remains a significant challenge for FANET performance enhancement.

6.1. Node Mobility and Network Partitioning

One significant performance issue in FANETs is network partitioning, caused by the high mobility of UAVs. In FANETs, UAVs constantly change positions, which can result in temporary disconnections and the formation of isolated subnetworks [244]. This phenomenon, known as network partitioning, severely impacts data routing efficiency and leads to increased latency and packet loss [245], [246]. As UAVs move away from each other or out of communication range, the network topology changes, causing disruptions in established communication paths. These disruptions necessitate frequent re-routing, consuming additional bandwidth and computational resources [247]. The dynamic nature of FANETs requires robust protocols that can quickly adapt to topology changes and minimize the negative impacts on network performance, such as delays in data transmission and reduced throughput.

6.2. Congestion and Bandwidth Limitations

Congestion in FANETs arises from the limited bandwidth available for communication among multiple UAVs. As the number of UAVs in the network increases, the demand for bandwidth grows, leading to congestion, especially when multiple UAVs attempt to transmit large volumes of data simultaneously [248]-[250]. This congestion results in higher latency and reduced data transmission rates, affecting the timely delivery of critical information [251], [252]. In scenarios where real-time data processing and rapid response are essential, such as disaster management or military operations, congestion can lead to significant performance degradation. Effective congestion control mechanisms are necessary to manage bandwidth efficiently, ensuring smooth data flow and optimal network performance.

6.3. Interference and Signal Jamming

Interference and signal jamming are critical performance issues in FANETs, where adversaries intentionally disrupt communication channels to degrade network performance. Jamming attacks can be executed by transmitting high-power signals on the same frequencies used by FANETs, causing communication failures [253]. This results in increased packet loss, delayed transmissions, and in some cases, complete communication breakdowns. Signal jamming is particularly detrimental in FANETs due to the reliance on wireless communication for coordination and data exchange [254], [255]. Implementing robust anti-jamming techniques and adaptive frequency-hopping methods is crucial to maintaining reliable communication links and ensuring the network's resilience against such attacks.

6.4. Resource Constraints and Energy Consumption

UAVs in FANETs are typically constrained by limited onboard resources, particularly battery life and computational power [256], [257]. High energy consumption due to constant communication, data processing, and mobility can lead to rapid depletion of battery power, reducing the operational lifespan of UAVs. Resource-intensive tasks, such as encryption, routing, and real-time data processing, make more impact on performance [258], [259]. As UAVs exhaust their energy reserves, they may need to return to a base station for recharging, resulting in reduced network coverage and availability. Effective energy management strategies, such as optimizing communication protocols and utilizing energy-efficient hardware, are essential to prolong the operational duration of UAVs and maintain network performance.

7. Limitations and Gaps in Addressing Performance Issues in FANETs

Current routing protocols in FANETs struggle to adapt quickly to frequent topology changes, causing delays and increased packet loss, indicating a need for more adaptive and resilient algorithms to handle high mobility and prevent network partitioning [260]. Existing congestion control mechanisms are often ineffective in managing high data transmission demands, necessitating advanced techniques to optimize bandwidth usage and reduce latency during peak traffic [261]. Anti-jamming techniques currently fall short against sophisticated attacks, highlighting the requirement for more robust and adaptive strategies to maintain reliable communication despite interference [262]. Additionally, the high energy consumption due to constant communication and data processing rapidly depletes UAV batteries, underscoring the need for innovations in energy-efficient communication protocols and hardware to extend operational times and ensure sustained network performance [263], [264].

Table 6 below provides a summary of the limitations and the gaps identified.

Table 6 Performance Issues; Limitation, and Gaps

Performance Challenges	Limitations	Gaps
Node Mobility and Network Partitioning	Routing protocols struggle with frequent topology changes, causing delays and packet loss.	Need for more adaptive and resilient routing algorithms to handle high mobility.
Congestion and Bandwidth Limitations	Congestion control mechanisms are ineffective for high data transmission demands.	Development of advanced techniques to optimize bandwidth usage and reduce latency.
Interference and Signal Jamming	Current anti-jamming techniques may not protect against sophisticated jamming attacks.	Need for more robust and adaptive anti-jamming strategies.
Resource Constraints and Energy Consumption	High energy consumption depletes UAV batteries quickly.	Innovations in energy-efficient protocols and hardware to extend UAV operational times.

Addressing performance issues in FANETs is fraught with limitations and gaps, primarily due to the high mobility and dynamic topology of the network. Existing routing protocols often struggle to maintain consistent performance as UAVs move rapidly, frequently leading to broken links and increased packet loss. Traditional routing algorithms, designed for more static environments, cannot cope effectively with the rapid topology changes inherent in FANETs. Furthermore, while reactive protocols can adapt to these changes, they tend to introduce latency as new routes are discovered. Proactive protocols, on the other hand, consume significant resources to maintain up-to-date routing tables, exacerbating energy constraints and reducing the operational life of UAVs.

The limited computational power and energy resources of UAVs also present a significant challenge in addressing performance issues. Most UAVs have strict power budgets that must be shared across multiple functions, including communication, navigation, and sensing. Implementing advanced algorithms for routing, security, and data processing can quickly deplete these limited resources, leading to shorter mission durations and reduced network reliability. While some energy-efficient protocols have been proposed, they often sacrifice performance in terms of latency and throughput to conserve power. The challenge is to develop lightweight yet robust solutions that can strike a balance between resource consumption and network performance.

Another gap in addressing performance issues in FANETs is the integration and management of heterogeneous UAVs. FANETs often consist of UAVs with varying capabilities in terms of speed, altitude, communication range, and energy reserves. Coordinating these diverse assets to work seamlessly together is complex and requires advanced network management strategies. Additionally, environmental factors such as weather conditions and physical obstacles can further complicate communication and routing. Current research is exploring adaptive protocols and machine learning techniques to predict and mitigate these issues, but practical implementation remains challenging. There is a need for comprehensive frameworks that can dynamically adapt to the varying conditions and resource constraints while maintaining high performance and reliability in FANET operations.

7.1. Future research scopes

Future research in FANET security and privacy encompasses several promising areas aimed at enhancing the robustness, reliability, and confidentiality of these networks. Key areas include:

Advanced Cryptographic Techniques: Research into lightweight and energy-efficient cryptographic algorithms is crucial. These algorithms must provide robust security without overburdening the limited computational and power resources of UAVs. Future studies could focus on developing novel encryption methods tailored specifically for FANETs, balancing security with performance.

Intrusion Detection Systems (IDS): Enhancing IDS tailored for FANETs to detect and mitigate various attacks, including spoofing, jamming, and DoS, is a vital area of research. Leveraging machine learning and artificial intelligence can help create adaptive and intelligent IDS capable of identifying new and evolving threats in real-time.

Secure Routing Protocols: Developing secure and efficient routing protocols that can dynamically adapt to the highly mobile and changing topology of FANETs is essential. These protocols need to ensure data integrity and confidentiality while maintaining high performance and reliability.

Privacy-Preserving Mechanisms: Research on privacy-preserving techniques such as anonymization, pseudonymization, and secure multi-party computation can help protect the identities and data of UAVs and users. These mechanisms should be lightweight to fit within the resource constraints of UAVs.

Blockchain Technology: Exploring the use of blockchain for decentralized and tamper-proof data management in FANETs can provide enhanced security and transparency. Blockchain can help ensure data integrity and facilitate secure communication and coordination among UAVs without relying on a central authority.

Quantum Cryptography: Investigating the potential of quantum cryptography to offer unparalleled security for FANETs is an exciting frontier. Although practical implementation may be years away, early research can lay the groundwork for integrating quantum-resistant algorithms in future UAV networks.

Resilience to Physical Layer Attacks: Studying methods to protect against physical layer attacks such as jamming and eavesdropping is crucial. Techniques like spread spectrum, frequency hopping, and advanced error correction codes can enhance the resilience of FANET communications.

Trust Management Systems: Developing robust trust management frameworks to ensure reliable interaction among UAVs is vital. These systems should dynamically assess the trustworthiness of nodes based on their behavior and communication patterns, adapting to the evolving network environment.

AI and Machine Learning for Security: Leveraging AI and machine learning to predict and respond to security threats dynamically can significantly enhance FANET security. These technologies can analyze vast amounts of data to detect anomalies and initiate proactive measures to counteract potential attacks.

Regulatory and Ethical Considerations: Researching the regulatory and ethical implications of FANET deployments can help address concerns related to privacy, data protection, and lawful usage. Establishing clear guidelines and frameworks will be essential as FANETs become more prevalent in civilian and commercial applications.

By addressing these research scopes, the future of FANET security and privacy can be significantly strengthened, ensuring safer and more reliable UAV networks for various critical applications.

8. Conclusion

The research has provided an in-depth analysis of the privacy and security issues in to Flying Ad Hoc Networks (FANETs). Due to the highly dynamic and decentralized nature of these networks, FANETs pose unique challenges that distinguish them from traditional and terrestrial ad hoc networks. Deep analysis of current solutions demonstrates that while numerous approaches exist to mitigate threats in FANETs, each has its own set of strengths and limitations. Techniques such as encryption, secure routing protocols, and intrusion detection systems have shown effectiveness in specific scenarios; however, their applicability is often constrained by factors such as computational overhead, energy consumption, and the need for real-time operation in highly mobile environments. To bridge these gaps, future research must focus on developing innovative approaches tailored specifically to the unique demands of FANETs. Emphasis should be placed on lightweight cryptographic solutions that can operate efficiently in resource-constrained environments, as well as adaptive security frameworks that can dynamically respond to changing network conditions and threat landscapes. By addressing these gaps and exploring proposed future directions, researchers can contribute to the creation of more resilient and secure FANETs capable of operating in increasingly complex and adversarial environments.

References

[1] Hoc Networks (FANETs): A -gh Bhandari, Suden R. Flying AdTarandeep Kaur Bhatia, Sanya Gilhotra, Suraj Sin eview. ICST transactions on energy web. 2024 Mar 20;11

[2] Hoc Networks (FANETs): Review -Soran Ahmed Hasan, Marwan Aziz Mohammed, Sazan Kamal Sulaiman. Flying Ad ations, Future direction and Open Research Topics. ITM web of conferences.024 f Communications, Challenges, Applic .2–64:01002;1Jan

[3] Ahmad S, Muhammad Abul Hassan. Secure Communication Routing in FANETs: A Survey. Studies in computational .110–97;1intelligence. 2022 Jan

[4] y, Fatima Hashim Abbas, Almohamadi M, Mustafa Asaad Hasan, Mohamed Ayad Alkhafaji, et dolaim-Nahi HA, F. Al Hoc Network Environment. -Objective Optimization for enhancing the efficiency of Service in Flying Ad-al. A Multi un 13ICST transactions on scalable information systems. 2023 J

[5] Kumar S, Vasudeva A, Sood M. Security Issues in the Routing Protocols of Flying Ad Hoc Networks. Lecture notes in .29–215;23networks and systems. 2022 Sep

[6] Hussien ZA, Abdulmalik HA, Hussain MA, Nyangaresi VO, Ma J, Abduljabbar ZA, Abduljaleel IQ. Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems. Applied Sciences. 2023 Jan;13(2):691.

[7] Ding F, Li X, Liang Y. Research on characterizing the high dynamic performance of distributed FANETs. Journal of .3–012013:(1)2615;1ence series. 2023 Oct physics Confer

[8] Bilal Muhammad Khan, Bilal R, Ali Hanzala Khan. Next Generation of Flying Adhoc Networks (Fanets). 2022 May 25

[9] Krishnan N, Yoosuf MS, Murugan K. Establishment of FANETs using IoT-based UAV and its issues related to mobility and authentication. InModelling and Simulation of Fast-Moving Ad-Hoc Networks (FANETs and VANETs) 2023 (pp. 74-93). IGI Global.

[10] Alsamhi SH, Shvetsov AV, Kumar S, Shvetsova SV, Alhartomi MA, Hawbani A, Rajput NS, Srivastava S, Saif A, Nyangaresi VO. UAV computing-assisted search and rescue mission framework for disaster and harsh environment mitigation. Drones. 2022 Jun 22;6(7):154.

[11] P. Krishna Srivathsav, Sai Abhishek, Thyagarajan J. FANET Routing Survey: An Application Driven Perspective. .27–217;1notes in electrical engineering. 2023 Jan Lecture

[12] Vasilyev GS, Surzhik DI, Kuzichkin OR, Kurilov IA. Algorithms for Adapting Communication Protocols of Fanet .22–114;1Networks. Journal of software. 2020 Jul

[13] life -vehicular ad hoc network and flying ad hoc network for real Swain S, Senapati BR, Khilar PM. Evolution of Hoc Networks (FANETs and -Moving Ad-applications: Role of vanet and fanet. InModelling and Simulation of Fast .IGI global .(73-VANETs) 2023 (pp. 43

[14] based weighted cluster routing scheme for FANETs. -obilityKhedr AM, Salim A, PV PR, Osamy W. MWCRSF: M .Vehicular Communications. 2023 Jun 1;41:100603

[15] Hoc Networks for Dynamic Connectivity. International Journal of Computing-Empowered Flying Ad-Mohammed B. AI .77-and Digital Systems. 2024 Jan 1;15(1):167

[16] Nyangaresi VO, Al-Joboury IM, Al-sharhanee KA, Najim AH, Abbas AH, Hariz HM. A Biometric and Physically Unclonable Function-Based Authentication Protocol for Payload Exchanges in Internet of Drones. e-Prime-Advances in Electrical Engineering, Electronics and Energy. 2024 Feb 23:100471.

[17] hoc network application scenarios and -Bujari A, Calafate CT, Cano JC, Manzoni P, Palazzi CE, Ronzani D. Flying ad .mobility models. International Journal of Distributed Sensor Networks. 2017 Oct;13(10):155014771773819

[18] Terrestrial Networks with UAVs: A Projection on -mati M, Al Homssi B, Krishnan S, Park J, Loke SW, Choi J. NonNe .Hoc Networks. Drones. 2022 Oct 31;6(11):334-Flying Ad

[19] Threats, Analysis of ,Ozlem Ceviz, Pinar Sadioglu, Sevil Şen. A Survey of Security in UAVs and FANETs: Issues ;Attacks, and Solutions. arXiv (Cornell University). 2023 Jun 25

[20] based UAV networks: A systematic survey. Internet of Things. -Sharma J, Mehra PS. Secure communication in IOT .Oct 1;23:100883 2023

[21] Tsao KY, Girdler T, Vassilakis VG. A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. Ad Hoc Networks. 2022 Aug 1;133:102894.

[22] Al Sibahee MA, Abduljabbar ZA, Ngueilbaye A, Luo C, Li J, Huang Y, Zhang J, Khan N, Nyangaresi VO, Ali AH. Blockchain-Based Authentication Schemes in Smart Environments: A Systematic Literature Review. IEEE Internet of Things Journal. 2024 Jul 3.

[23] Mekdad Y, Aris A, Babun L, Fergougui AE, Conti M, Lazzeretti R, et al. A survey on security and privacy issues of .Networks. 2023 Apr;224:109626 UAVs. Computer

[24] Wani AR, Gupta SK, Khanam Z, Rashid M, Alshamrani SS, Baz M. A novel approach for securing data against adversary attacks in UAV embedded HetNet using identity based authentication scheme. IET Intelligent Transport ;Sep 12 2022 .Systems

[25] Gupta A, Anurag Barthwal, Harsh Vardhan, Shivani Kakria, Kumar S, Ashish Singh Parihar. Evolutionary study of assisted FANET. Multimedia tools and applications. -distributed authentication protocols and its integration to UAV 30–42311:(27)Apr 11;82 2023

[26] Based Reconnaissance -UAV-Kim T, Lee S, Kyong Hoon Kim, Jo YI. FANET Routing Protocol Analysis for Multi .1–161:(3)7;25Mobility Models. Drones. 2023 Feb

[27] Nyangaresi VO. Extended Chebyshev Chaotic Map Based Message Verification Protocol for Wireless Surveillance Systems. InComputer Vision and Robotics: Proceedings of CVR 2022 2023 Apr 28 (pp. 503-516). Singapore: Springer Nature Singapore.

[28] oc Pasandideh F, Costa JPJ da, Kunst R, Hardjawana W, de Freitas EP. A systematic literature review of flying ad h art, challenges, and perspectives. Journal of Field Robotics. 2023 Jan 24-the-of-networks: State.

[29] Ala Altaweel, Hena Mukkath, Kamel I. GPS Spoofing Attacks in FANETs: A Systematic Literature Review. IEEE .80–11:55233;1Access. 2023 Jan

[30] Based Framework for UAVs -miha Ayed, Lamia Chaari Fourati. A New Hybrid Adaptive Deep LearningFadhila Tlili, Sa .39–4128:(6)16;1Faults and Attacks Detection. IEEE transactions on services computing. 2023 Nov

[31] ab Sikdar. PIC: Preserving Data Integrity Nalam Venkata Abhishek, Muhammad Naveed Aman, Teng Joon Lim, Bipl IEEE Conference on Computer Communications -in UAV Assisted Communication. IEEE INFOCOM 2022 ;Workshops (INFOCOM WKSHPS). 2022 May 2

[32] t. Applied and computational Liu W. Analysis of UAV data communication stability method in extreme environmen .5–131:(1)53;28engineering. 2024 Mar

[33] Based Secure Data Communication: Multilevel Authentication Perspective. Sensors. 2024 -Abdullah Aljumah. UAV .6–996:(3)24;3Feb

[34] Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Khalefa MS, Honi DG. MAC-Based Symmetric Key Protocol for Secure Traffic Forwarding in Drones. InFuture Access Enablers for Ubiquitous and Intelligent Infrastructures: 6th EAI International Conference, FABULOUS 2022, Virtual Event, May 4, 2022, Proceedings 2022 Sep 18 (pp. 16-36). Cham: Springer International Publishing.

[35] Tomás E, Mario Quiles Pérez, Miguel P, Sergio López Bernal, Gérôme Bovet, Manuel Gil Pérez, et al. Decentralized IEEE Communications .Federated Learning: Fundamentals, State of the Art, Frameworks, Trends, and Challenges .3013–2983:(4)25;1Surveys and Tutorials. 2023 Jan

[36] hoc -hop routing for secure communication in flying ad-Kumar R, Sharma B, Senthil Athithan. TBMR: trust based multi ;networks. Wireless Networks. 2023 Sep 2

[37] based trusted fuzzy scheme. Complex & -curing flying ad hoc network using clusterse-Gupta S, Sharma N. SCFS ;Intelligent Systems. 2024 Feb 23

[38] Hadi HJ, Cao Y, Nisa KU, Jamil AM, Ni Q. A comprehensive survey on security, privacy issues and emerging defence .al of Network and Computer Applications. 2023 Apr;213:103607technologies for UAVs. Journ

[39] Nair AS, Thampi SM. Flying Ad Hoc Networks: Security, Authentication Protocols, and Future Directions. InInternet of Things and Secure Smart Environments 2020 Nov 4 (pp. 223-272). Chapman and Hall/CRC.

[40] Nyangaresi VO. Provably secure authentication protocol for traffic exchanges in unmanned aerial vehicles. High-Confidence Computing. 2023 Sep 15:100154.

[41] s 'manager-i .EA3ACKa-K. Thamizhmaran. Secure efficient communication in routing protocol in MANETs using ECC .2–12:(1)10;1journal on mobile applications & technologies. 2023 Jan

[42] Based -S. Venkatramulu, Shekar C, K. Vinay Kumar, Srinivas C, B. Raghuram, Rasool S. A Novel Cryptography al journal on recent and innovation trends in Multipath Routing Protocol for Wireless Communications. Internation .62–computing and communication. 2023 Jul 13;11(7s):550

[43] Amar N, None Anagha Udupa Y N, None Anirudh Kamath, None Ananya. A Review on Ad Hoc Network and Security .62–454;15h in Science, Communication and Technology. 2023 Sep Issues. International Journal of Advanced Researc

[44] Khezri E, Esmaeil Zeinali, Hadi Sargolzaey. SGHRP: Secure Greedy Highway Routing Protocol with authentication .1–82031and increased privacy in vehicular ad hoc networks. PLOS ONE. 2023 Apr 6;18(4):e02

[45] Hoc Network. 2023 Aug -Ashish Singh Parihar, Pandey A. Proposing A Novel Key Agreement Protocol For Flying Ad ;3

[46] Aissaoui R, Deneuville JC, Guerber C, Pirovano A. A survey on cryptographic methods to secure communications for .management. Vehicular Communications. 2023 Aug 19:100661 UAV traffic

[47] Yenurkar G, Mal S, Nyangaresi VO, Kamble S, Damahe L, Bankar N. Revolutionizing Chronic Heart Disease Management: The Role of IoT-Based Ambulatory Blood Pressure Monitoring System. Diagnostics. 2024 Jun 19;14(12):1297.

[48] Rahman K, Muhammad Adnan Aziz, Usman N, Tayybah Kiren, Tanweer Ahmad Cheema, Hina Shoukat, et al. Enabled FANET to Detect Cyberattacks. Journal of -Based IDS for IoT-Cognitive Lightweight Logistic Regression .11–2023:1;29Apr 2023 .mobile information systems

[49] Yadala Sucharitha, Shaker C, G. Suryanarayana. Network Intrusion Detection of Drones Using Recurrent Neural .92–375;12Networks. 2023 May

[50] y: A Tiny Machine Wu Y, Yang L, Zhang L, Nie L, Zheng L. Intrusion Detection for Unmanned Aerial Vehicles Securit .1–1;1Learning Model. IEEE internet of things journal. 2024 Jan

[51] Swain S, Senapati BR, Khilar PM. Evolution of vehicular ad hoc network and flying ad hoc network for real-life applications: Role of vanet and fanet. InModelling and Simulation of Fast-Moving Ad-Hoc Networks (FANETs and VANETs) 2023 (pp. 43-73). IGI global.

[52] Ali F, Zaman K, Shah B, Hussain T, Ullah H, Hussain A, Kwak D. LSTDA: link stability and transmission delay aware routing mechanism for flying ad-hoc network (FANET). Computers, Materials and Continua. 2023;77(1):963.

[53] Nyangaresi VO, Moundounga AR. Secure data exchange scheme for smart grids. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[54] Guo J, Jones MR, Djahel S, Wang S. AVARS-Alleviating Unexpected Urban Road Traffic Congestion using UAVs. In2023 IEEE 98th Vehicular Technology Conference (VTC2023-Fall) 2023 Oct 10 (pp. 1-6). IEEE.

[55] Javaid S, Saeed N, Qadir Z, Fahim H, He B, Song H, et al. Communication and Control in Collaborative UAVs: Recent Advances and Future Trends. IEEE Transactions on Intelligent Transportation Systems. 2023 Jun 1;24(6):5719–39.

[56] Mohammed B. AI-Empowered Flying Ad-Hoc Networks for Dynamic Connectivity. International Journal of Computing and Digital Systems. 2024 Jan 1;15(1):167-77.

[57] Zheng Z, Sangaiah AK, Wang T. Adaptive communication protocols in flying ad hoc network. IEEE Communications Magazine. 2018 Jan 12;56(1):136-42.

[58] Bhardwaj V, Kaur N. SEEDRP: a secure energy efficient dynamic routing protocol in fanets. Wireless personal communications. 2021 Sep;120(2):1251-77.

[59] Ali ZA, Abduljabbar ZA, AL-Asadi HA, Nyangaresi VO, Abduljaleel IQ, Aldarwish AJ. A Provably Secure Anonymous Authentication Protocol for Consumer and Service Provider Information Transmissions in Smart Grids. Cryptography. 2024 May 9;8(2):20.

[60] Dhall R, Dhongdi S. Review of protocol stack development of flying ad-hoc networks for disaster monitoring applications. Archives of Computational Methods in Engineering. 2023 Jan;30(1):37-68.

[61] Mohammed B. An Overview of Flying Ad-Hoc Networks. InInternational Conference on Artificial Intelligence in Renewable Energetic Systems 2023 Nov 26 (pp. 290-303). Cham: Springer Nature Switzerland.

[62] Safari F, Savić I, Kunze H, Gillis D. The diverse technology of MANETs: a survey of applications and challenges. Int. J. Future Comput. Commun. 2023 Jun;12(2).

[63] Alqarni MA. Secure UAV adhoc network with blockchain technology. PloS one. 2024 May 8;19(5):e0302513–3.

[64] Chandrasekar V, Shanmugavalli V, Mahesh TR, Shashikumar R, Borah N, Kumar VV, Guluwadi S. Secure malicious node detection in flying ad-hoc networks using enhanced AODV algorithm. Scientific Reports. 2024 Apr 3;14(1):7818.

[65] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432). IEEE.

[66] d Aerial Bine S, Svaigen AR, Azzedine Boukerche, Ruiz LB, Antonio. Flavors of the Next Generation of Unmanne .1–1;1Vehicles Networks. IEEE internet of things journal. 2024 Jan

[67] Luis. Brief Introduction to Unmanned Aerial Systems. Management and industrial -Crespo P, Uxía García-Orgeira .22–1;1engineering. 2024 Jan

[68] .ty of Oklahoma Press; 2024Laslie BD. Fighting from Above. Universi

[69] None Lawali Rabiu, None Anuar Ahmad, None Adel Gohari. Advancements of Unmanned Aerial Vehicle Technology in the Realm of Applied Sciences and Engineering: A Review. Journal of Advanced Research in Applied Sciences and .95–74:(2)40;28ng Technology. 2024 Feb Engineeri

[70] Aldemir HO. Evolution of Unmanned Aerial Systems and Inconsistencies Between Strategies, Concepts, and .IGI Global .(111-Technology. InHarnessing Digital Innovation for Air Transportation 2024 (pp. 91

[71] Abduljabbar ZA, Nyangaresi VO, Jasim HM, Ma J, Hussain MA, Hussien ZA, Aldarwish AJ. Elliptic Curve Cryptography-Based Scheme for Secure Signaling and Data Exchanges in Precision Agriculture. Sustainability. 2023 Jun 28;15(13):10264.

[72] Design Scheme and Security Analysis of Unmanned Aerial Vehicle. Springer Yang D, Zhao Y, Wu K, Yi Z, Peng H. A .67–554;1eBooks. 2022 Jan

[73] s usage of tactical unmanned aerial vehicles. Defence Studies. 2020 'Borg S. Below the radar. Examining a small state .201–185:(3)20;2Jul

[74] s development and deployment 's Progress: the bureaucratic challenges to the clinton administration'Predator .Boys JD .20–1;26Intelligence and National Security. 2022 Oct .(2001-of unmanned aerial vehicles (1993

[75] supported Services and -sign Guidelines for Cooperative UAVAl Ridhawi I, Bouachir O, Aloqaily M, Boukerche A. De .35–1:(9)54;31Applications. ACM Computing Surveys. 2022 Dec

[76] Nyangaresi VO, Morsy MA. Towards privacy preservation in internet of drones. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[77] Singh S, Stappert S, Bussler L, Sippel M, Kucukosman YC, Buckingham S. Full-scale simulation and analysis of formation flight during in-air-capturing of a winged reusable launch vehicle. Journal of Space Safety Engineering. 2022 Dec 1;9(4):541-52.

[78] Krause S, Funke A, Cain S. Overview of a planned subscale in-air capturing demonstration. In2024 IEEE Aerospace Conference 2024 Mar 2 (pp. 1-15). IEEE.

[79] nt, and Future of European Air Traffic Management Research. Bolić T, Ravenhill P. SESAR: The Past, Prese .51–Engineering. 2021 Apr;7(4):448

[80] Malavolti E, Wang C. Optimal Contract for Reducing Flight Delays in EU: In the Context of SESAR. Mathematical .17–2022:1;3problems in engineering. 2022 Feb

[81] Gai K, Choo KK, Qiu M, Zhu L. Privacy-preserving content-oriented wireless communication in internet-of-things. IEEE Internet of Things Journal. 2018 Apr 26;5(4):3059-67.

[82] Xu X, Patibandla RL, Arora A, Al-Razgan M, Awwad EM, Nyangaresi VO. An Adaptive Hybrid (1D-2D) Convolution-based ShuffleNetV2 Mechanism for Irrigation Levels Prediction in Agricultural Fields with Smart IoTs. IEEE Access. 2024 Apr 3.

[83] Pasandideh F, da Costa JPJ, Kunst R, Islam N, Hardjawana W, Pignaton de Freitas E. A Review of Flying Ad Hoc .tworks: Key Characteristics, Applications, and Wireless Technologies. Remote Sensing. 2022 Sep 7;14(18):4459Ne

[84] A Comparative Study. Sustainability. 2021 —Absi AA, Sain M, Lee H. Moving Ad Hoc Networks-Absi MA, Al-Al .May 31;13(11):6187

[85] ehrubeoglu M, Tewolde GS, Sherratt RS. Unmanned Aerial Vehicle Communications for Civil Ghamari M, Rangel P, M .531–10:102492;2022Applications: A Review. IEEE Access.

[86] less Khan MA, Ullah I, Nisar S, Noor F, Qureshi IM, Khanzada FU, et al. An Efficient and Provably Secure Certificate .28–8:36807;2020hoc Network. IEEE Access. -Encapsulated Signcryption Scheme for Flying Ad-Key

[87] Shambhavi Prasanna, Manas Ranjan Lenka, Amulya Ratna Swain. A Survey on Routing Protocols for Disaster .(2)Jan 20;5 024Management. SN Computer Science/SN computer science. 2

[88] .27–105;30Rana B, Singh Y. Internet of Things and UAV: An Interoperability Perspective. 2021 Jul

[89] Nyangaresi VO, Petrovic N. Efficient PUF based authentication protocol for internet of drones. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[90] Rolly RM, Malarvezhi P, Lagkas TD. Unmanned aerial vehicles: Applications, techniques, and challenges as aerial base .2211239stations. International Journal of Distributed Sensor Networks. 2022 Sep;18(9):15501329

[91] Telli K, Kraa O, Himeur Y, Ouamane A, Boumehraz M, Atalla S, Mansoor W. A comprehensive review of recent .research trends on unmanned aerial vehicles (uavs). Systems. 2023 Aug 2;11(8):400

[92] UAV -Pereira DS, et al. Performance Evaluation of Multi ,Silva MR, Souza ES, Pablo Javier Alsina, Leite DL, Mateus .5–4895:(22)19;9Network Applied to Scanning Rocket Impact Area. Sensors. 2019 Nov

[93] Wilson AN, Kumar A, Jha A, Cenkeramaddi LR. Embedded Sensors, Communication Technologies, Computing 26–1807:(3)22;1ine Learning for UAVs: A Review. IEEE Sensors Journal. 2022 Feb Platforms and Mach

[94] Scale Environmental Monitoring Using WSN/UAV/Crowdsensing: A Review of -Fascista A. Toward Integrated Large .Feb 25;22(5):1824 22Applications, Signal Processing, and Future Perspectives. Sensors. 20

[95] Assisted -UAV-Zhu M, Wei Z, Qiu C, Jiang W, Wu H, Feng Z. Joint Data Collection and Sensor Positioning in Multi .75–23664:(19)23;1Wireless Sensor Network. IEEE sensors journal. 2023 Oct

[96] Bulbul SS, Abduljabbar ZA, Mohammed RJ, Al Sibahee MA, Ma J, Nyangaresi VO, Abduljaleel IQ. A provably lightweight and secure DSSE scheme, with a constant storage cost for a smart device client. Plos one. 2024 Apr 25;19(4):e0301277.

[97] ies in emergency situations. Electronics. Coch A, Navarro J, Sans C, Zaballos A. Communication technolog-Carreras .Apr 6;11(7):1155 2022

[98] ground integrated network: Key enablers, open challenges, and future direction. -air-Ray PP. A review on 6G for space ;Aug Computer and Information Sciences. 2021 -Journal of King Saud University

[99] Area Networks: Design Goals, Architecture, -Power Wide-Buurman B, Kamruzzaman J, Karmakar G, Islam S. Low .220–8:17179;2020Suitability to Use Cases and Research Challenges. IEEE Access.

[100] -of-flight connectivity: A tutorial of the state-in Bilen T, Ahmadi H, Canberk B, Duong TQ. Aeronautical networks for .79-art and survey of research challenges. IEEE Access. 2022 Feb 16;10:20053-the

[101] time Automated Traffic Management Scheme Using Blockchain Based on -Ali EM, Abdulla SH, Awheed H. Real .les. InITM Web of Conferences 2024 (Vol. 64, p. 01013). EDP SciencesUnmanned Aerial Vehic

[102] Hosseinzadeh M, Ali S, Amir Masoud Rahmani, Lansky J, Vladimir Nulicek, Mohammad Sadegh Yousefpoor, et al. A g ad hoc networks for traffic monitoring. based adaptive optimized link state routing protocol in flyin-smart filtering ḥasib wa -malīk Saud : ùlm al-Journal of King Saud University Computer and information sciences/Maǧalaẗ ǧam'aẗ al .4–102034:(4)36;1ma'lumat. 2024 Apr -al

[103] Eid MM, Arunachalam R, Sorathiya V, Lavadiya S, Patel SK, Parmar J, Delwar TS, Ryu JY, Nyangaresi VO, Zaki Rashed AN. QAM receiver based on light amplifiers measured with effective role of optical coherent duobinary transmitter. Journal of Optical Communications. 2022 Jan 17(0).

[104] i Fourati. Communication Architecture for Unmanned Aerial Vehicle System. Lobna Krichen, Fourati M, Lamia Chaar .25–213;5Lecture Notes in Computer Science. 2018 Sep

[105] hoc network. Ad -hop clustering algorithm for aeronautical ad-Jiang L, Chen Z, Yang H, Zhenyu Na. Distributed multi .7–103547;1May 2024 .hoc networks

[106] Zhang H, Lv X, Liu Y, Zou X. Hedge transfer learning routing for dynamic searching and reconnoitering applications .39-in 3D multimedia FANETs. Multimedia Tools and Applications. 2024 Jan;83(3):7505

[107] review on communication protocols for autonomous unmanned aerial vehicles Shi L, Marcano NJH, Jacobsen RH. A for inspection application. Microprocessors and Microsystems. 2021 Oct;86:104340

[108] Paparistodimou G, Duffy A, Whitfield RI, Knight P, Robb M. A network tool to analyse and improve robustness of system architectures. Design Science. 2020 Jan;6:e8.

[109] Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Spatial single mode laser source interaction with measured pulse based parabolic index multimode fiber. Journal of Optical Communications. 2022 Jun 21.

[110] Javid Z, Kocar I, Holderbaum W, Karaagac U. Future Distribution Networks: A Review. Energies. 2024 Apr .1822:(8)17;10

[111] Hoc Networks (FANETs): Review -Sulaiman. Flying Ad Soran Ahmed Hasan, Marwan Aziz Mohammed, Sazan Kamal of Communications, Challenges, Applications, Future direction and Open Research Topics. ITM web of conferences. .2–64:01002;1Jan 2024

[112] ng: Challenges and Opportunities from a UAV Networks for Disaster Monitori-Chandran I, Kizheppatt Vipin. Multi ;Network Perspective. Drone systems and applications. 2024 Feb 27

[113] Assisted Cooperative Routing Scheme for Seamless Connectivity in -Chughtai O, Nawaz N, Kaleem Z, Yuen C. Drone .1–12:1;1 V2X Communication. IEEE access. 2024 Jan

[114] time military -hoc network routing protocols comparison for real-Shams Al Ajrawi, Tran B. Mobile wireless ad ;application. Spatial Information Research. 2023 Sep 14

[115] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Apr 1;142:103117.

[116] Hosseinzadeh M, Ali S, Ahmad HJ, Alanazi F, Yousefpoor MS, Yousefpoor E, Darwesh A, Rahmani AM, Lee SW. izer in flying ad hoc networks. Vehicular DCFH: A dynamic clustering approach based on fire hawk optim .Communications. 2024 Jun 1;47:100778

[117] Ramphull D, Mungur A, Armoogum S, Pudaruth S. A review of mobile ad hoc NETwork (MANET) Protocols and their puting and control systems (ICICCS) 2021 May 6 Applications. In2021 5th international conference on intelligent com .IEEE .(211-(pp. 204

[118] hoc networks: architecture, applications and challenges. arXiv preprint -Yeferny T, Hamad S. Vehicular ad .arXiv:2101.04539. 2021 Jan 12

[119] hoc networks: A comprehensive survey. Computers & Security. -dMalhi AK, Batra S, Pannu HS. Security of vehicular a .Feb 1;89:101664 2020

[120] Srivastava A, Prakash J. Future FANET with application and enabling techniques: Anatomization and sustainability .issues. Computer science review. 2021 Feb 1;39:100359

[121] Al Sibahee MA, Abduljabbar ZA, Luo C, Zhang J, Huang Y, Abduljaleel IQ, Ma J, Nyangaresi VO. Hiding scrambled text messages in speech signals using a lightweight hyperchaotic map and conditional LSB mechanism. Plos one. 2024 Jan 3;19(1):e0296469.

[122] Based Routing Protocols and Mobility Models -din R, Samah AA, Alsharif MH, Khan MA. TopologyWheeb AH, Nor .for Flying Ad Hoc Networks: A Contemporary Review and Future Research Directions. Drones. 2021 Dec 31;6(1):9

[123] GM, Khalaf OI, Mansoor RF, Ghoneim OA. Classification Agrawal R, Faujdar N, Romero CA, Sharma O, Abdulsahib .25-and comparison of ad hoc networks: A review. Egyptian Informatics Journal. 2023 Mar 1;24(1):1

[124] Fadhila Tlili, Samiha Ayed, Lamia Chaari Fourati. Advancing UAV security with artificial intelligence: A .1–101281;1comprehensive survey of techniques and future directions. Internet of things. 2024 Jul

[125] Enabled Lightweight Intrusion Detection System for Secure MANETs. Journal of -N. Ilakkiya, Rajaram A. Blockchain .81–2667:(4)19;6of electrical engineering & technology. 2024 Jan Electrical Engineering & Technology/Journal

[126] based ubiquitous entity authentication and management scheme with -Xie H, Zheng J, He T, Wei S, Hu C. A blockchain .84–569:(2)17;15Feb 2024 .peer networking and applications-to-homomorphic encryption for FANET. Peer

[127] Nyangaresi VO. A Formally Verified Authentication Scheme for mmWave Heterogeneous Networks. Inthe 6th International Conference on Combinatorics, Cryptography, Computer Science and Computation (605-612) 2021.

[128] Security Protocols and the Vulnerabilities in the -Sight Analysis of Cyber-Balamurugan. An In .Priyadharshini SP, P .59–243;1Drone Communication. Transactions on Computer Systems and Networks. 2023 Jan

[129] Chriki A, Touati H, Snoussi H, Kamoun F. FANET: Communication, mobility models and security issues. Computer Networks. 2019 Nov 9;163:106877.

[130] Bekmezci İ, Şentürk E, Türker T. Security issues in flying ad-hoc networks (FANETS). Journal of Aeronautics and Space Technologies. 2016 Jul 25;9(2):13-21.

[131] Khan MA, Safi A, Qureshi IM, Khan IU. Flying ad-hoc networks (FANETs): A review of communication architectures, and routing protocols. In2017 First international conference on latest trends in electrical engineering and computing technologies (INTELLECT) 2017 Nov 15 (pp. 1-9). IEEE.

[132] Du X, Li Y, Zhou S, Zhou Y. ATS-LIA: A lightweight mutual authentication based on adaptive trust strategy in flying ad-hoc networks. Peer-to-peer networking and applications. 2022 Jul;15(4):1979-93.

[133] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA. Low complexity smart grid security protocol based on elliptic curve cryptography, biometrics and hamming distance. Plos one. 2024 Jan 23;19(1):e0296781.

[134] Khan MF, Yau KL, Noor RM, Imran MA. Routing schemes in FANETs: A survey. Sensors. 2019 Dec 19;20(1):38.

[135] Kanchan S, Choi BJ. An efficient and privacy-preserving federated learning scheme for flying ad hoc networks. InICC 2022-IEEE International Conference on Communications 2022 May 16 (pp. 1-6). IEEE.

[136] Bada M, Boubiche DE, Lagraa N, Kerrache CA, Imran M, Shoaib M. A policy-based solution for the detection of colluding GPS-Spoofing attacks in FANETs. Transportation Research Part A: Policy and Practice. 2021 Jul 1;149:300-18.

[137] Arafat MY, Poudel S, Moh S. Medium access control protocols for flying ad hoc networks: A review. IEEE Sensors Journal. 2020 Oct 29;21(4):4097-121.

[138] Khan IU, Qureshi IM, Aziz MA, Cheema TA, Shah SB. Smart IoT control-based nature inspired energy efficient routing protocol for flying ad hoc network (FANET). IEEE Access. 2020 Mar 18;8:56371-8.

[139] Nyangaresi VO, Alsamhi SH. Towards secure traffic signaling in smart grids. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 196-201). IEEE.

[140] hreats in Flying Ad Hoc Network (FANET). Studies in Lateef S, Rizwan M, Muhammad Abul Hassan. Security T .96–73;1computational intelligence. 2022 Jan

[141] Singh RS, Prasad A, Moven RM, Sarma HK. Denial of service attack in wireless data network: A survey. In2017 Devices for Integrated Circuit (DevIC) 2017 Mar 23 (pp. 354-359). IEEE.

[142] Lei Y, Zeng L, Li YX, Wang MX, Qin H. A lightweight authentication protocol for UAV networks based on security and computational resource optimization. IEEE Access. 2021 Apr 2;9:53769-85.

[143] Mohsan SA, Othman NQ, Li Y, Alsharif MH, Khan MA. Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends. Intelligent Service Robotics. 2023 Mar;16(1):109-37.

[144] Syed F, Gupta SK, Hamood Alsamhi S, Rashid M, Liu X. A survey on recent optimal techniques for securing unmanned aerial vehicles applications. Transactions on Emerging Telecommunications Technologies. 2021 Jul;32(7):e4133.

[145] Ahmad AY, Verma N, Sarhan N, Awwad EM, Arora A, Nyangaresi VO. An IoT and Blockchain-Based Secure and Transparent Supply Chain Management Framework in Smart Cities Using Optimal Queue Model. IEEE Access. 2024 Mar 18.

[146] Sharma D, Gupta SK, Rashid A, Gupta S, Rashid M, Srivastava A. A novel approach for securing data against intrusion attacks in unmanned aerial vehicles integrated heterogeneous network using functional encryption technique. Transactions on Emerging Telecommunications Technologies. 2021 Jul;32(7):e4114.

[147] .17–Ozlem Ceviz, Pinar Sadioglu, Sen S. Analysis of Routing Attacks in FANETs. Springer eBooks. 2022 Jan 1;3

[148] Hoc Networks -organized Ad-hamed Hamadouche. Security Issues in Self'Sihem Goumiri, Mohamed Amine Riahla, M .24–312;1(MANET, VANET, and FANET): A Survey. Lecture notes in networks and systems. 2022 Jan

[149] federated reinforcement learning for intelligent jamming defense Mowla NI, Tran NH, Doh I, Chae K. AFRL: Adaptive .58–244:(3)22;17in FANET. 2020 Jul

[150] Salim S, Moustafa N, Reisslein M. Cybersecurity of Satellite Communications Systems: A Comprehensive Survey of Communications surveys and tutorials/IEEE communications surveys the Space, Ground, and Links Segments. IEEE .1–1;1and tutorials. 2024 Jan

[151] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. InThe Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021 2022 Jun 12 (pp. 81-99). Cham: Springer International Publishing.

[152] Khadeeja Sabah Jasim, Alheeti A, Kareem A. Intelligent Detection System for Spoofing and Jamming Attacks in UAVs. .110–97;1Springer eBooks. 2023 Jan

[153] based -bbati OS, Qureshi IM, Noor F, Khanzada FU. An efficient and secure certificateKhan MA, Ullah I, Kumar N, Ou hoc networks. IEEE Transactions on Vehicular Technology. -access control and key agreement scheme for flying ad .51-Feb 2;70(5):4839 2021

[154] unmanned aerial vehicles (UAVs). Journal of Cyber Security Technology. 2020 Nov Ly B, Ly R. Cybersecurity in .18–1;11

[155] Lamia Chaari Fourati, Chahbani S, Jihene Rezgui. Vulnerabilities Assessment for Unmanned Aerial Vehicles ;Communication Systems. 2020 Oct 20

[156] On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and .Khan SZ, Mohsin M, Iqbal W .future research directions. PeerJ Computer Science. 2021 May 6;7:e507

[157] Al Sibahee MA, Nyangaresi VO, Abduljabbar ZA, Luo C, Zhang J, Ma J. Two-Factor Privacy Preserving Protocol for Efficient Authentication in Internet of Vehicles Networks. IEEE Internet of Things Journal. 2023 Dec 7.

[158] based detection for GPS spoofing attacks on UAVs. -Wei X, Sun C, Lyu M, Song Q, Li Y. ConstDet: control semantics .ov 5;14(21):5587Remote Sensing. 2022 N

[159] Uddin R, Kumar SA, Chamola V. Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats .and solutions. Ad Hoc Networks. 2024 Jan 1;152:103322

[160] rationales, and research challenges. ,flow based DDoS attacks in SDN: Taxonomy-Singh MP, Bhandari A. New .27–Computer Communications. 2020 Mar;154:509

[161] Hassija V, Chamola V, Agrawal A, Goyal A, Luong NC, Niyato D, Yu FR, Guizani M. Fast, reliable, and secure drone .32-Surveys & Tutorials. 2021 Jul 16;23(4):2802 communication: A comprehensive survey. IEEE Communications

[162] Selvakumar S, Ahilan A, Ben Sujitha B, Muthukumaran N. Crystals kyber cryptographic algorithm for efficient IoT .8-D2d communication. Wireless Networks. 2024 Jul 7:1

[163] Nyangaresi VO, Ma J. A Formally Verified Message Validation Protocol for Intelligent IoT E-Health Systems. In2022 IEEE World Conference on Applied Intelligence and Computing (AIC) 2022 Jun 17 (pp. 416-422). IEEE.

[164] e WJ, Hussain M. Data Sindiramutty SR, Jhanjhi NZ, Tan CE, Yun KJ, Manchuri AR, Ashraf H, Murugesan RK, Te Security and Privacy Concerns in Drone Operations. InCybersecurity Issues and Challenges in the Drone Industry 2024 .IGI Global .(290-(pp. 236

[165] nt user authentication IoD: Secure and efficie-Tanveer M, Abdallah Aldosary, Kumar N, Saud Alhajaj Aldossari. SEAF .9–110449;1framework for the Internet of Drones. Computer networks. 2024 Apr

[166] Mohammad Kamrul Hasan, Zhou Weichen, Nurhizam Safie, Rayan F, Ghazal TM. A Survey on Key Agreement and .1–1;1cation. IEEE access. 2024 Jan Authentication Protocol for Internet of Things Appli

[167] Priyadarshani R, Park KH, Ata Y, Alouini MS. Jamming Intrusions in Extreme Bandwidth Communication: A .Comprehensive Overview. arXiv preprint arXiv:2403.19868. 2024 Mar 28

[168] Mohsan SA, Khan MA, Noor F, Ullah I, Alsharif MH. Towards the unmanned aerial vehicles (UAVs): A comprehensive review. Drones. 2022 Jun 15;6(6):147.

[169] Kumar S, Chinthaginjala R, Anbazhagan R, Nyangaresi VO, Pau G, Varma PS. Submarine Acoustic Target Strength Modelling at High-Frequency Asymptotic Scattering. IEEE Access. 2024 Jan 1.

[170] Panda G, Ramasamy TN, Elghali SB, Affijulla S. Digital Communication and Soft Computing Approaches Towards .Sustainable Energy Developments

[171] .May 1;24(9):2897 024Kang M, Park S, Lee Y. A Survey on Satellite Communication System Security. Sensors. 2

[172] Hemanth DJ, Yigit T, Kose U, Guvenc U, editors. 4th International Conference on Artificial Intelligence and Applied .Mathematics in Engineering: ICAIAME 2022. Springer Nature; 2023 Jul 2

[173] Nyangaresi VO. Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In2022 International Conference on Inventive Computation Technologies (ICICT) 2022 Jul 20 (pp. 1-6). IEEE.

[174] enabled data hiding for -ical layerMallikarachchi D, Wong K, Lim JM. A message verification scheme based on phys .21-flying ad hoc network. Multimedia Tools and Applications. 2024 Feb 23:1

[175] Based Online/Offline Signcryption Scheme for -U2G: An Identity-Ali I, Li J, Chen J, Chen Y, Ullah S, Khan S. IOOSC .1–1;1und Station Communication. IEEE internet of things journal. 2024 Jan Unmanned Aerial Vehicle to Gro

[176] HetNet security through functional encryption framework. Concurrency -Gupta SK, Gupta P, Singh P. Enhancing UAV .and Computation: Practice and Experience.:e8206

[177] based -Vinay Chamola, Kumar N, Ashok Kumar Das, Mishra D. Efficient and secure signcryption ,Girraj Kumar Verma ground station communication. Ad hoc networks. 2024 Jun -to-based drone-data aggregation for Internet of Drone 159:103502;1.

[178] D: A Provable Secure and Lightweight Authentication Protocol for Io-Fahad Algarni, Saeed Ullah Jan. PSLAPS .1–1;1Drones (IoD) Environment. IEEE access. 2024 Jan -of-Securing Internet

[179] Alqahtani H, Kumar G. Machine learning for enhancing transportation security: A comprehensive analysis of electric .and flying vehicle systems. Engineering Applications of Artificial Intelligence. 2024 Mar 1;129:107667

[180] Umran SM, Lu S, Abduljabbar ZA, Nyangaresi VO. Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry. Internet of Things. 2023 Dec 1;24:100969.

[181] hoc -Kundu J, Alam S, Dey A. Fuzzy based trusted malicious unmanned aerial vehicle detection using in flying ad .41-network. Alexandria Engineering Journal. 2024 Jul 1;99:232

[182] Berk Canberk, Amirhossein Mohajerzadeh, Symeon Chatzinotas, Grace D, et al. Advancing ,Sun C, Gianluca Fontanesi Edge Machine Learning Techniques. IEEE open journal -UAV Communications: A Comprehensive Survey of Cutting .31–1;1of vehicular technology. 2024 Jan

[183] -W, Pouya Ostovari. Optimal filter assignment policy against link flooding attack. High Biswas R, Wu J, Chang .1–100231;1confidence computing. 2024 Apr

[184] .115–93;28Imdad Ali Shah. Privacy and Security Challenges in Unmanned Aerial Vehicles (UAVs). 2024 Jun

[185] Lagkas T, Argyriou V, Bibi S, Sarigiannidis P. UAV IoT framework views and challenges: Towards protecting drones as "Things". Sensors. 2018 Nov 17;18(11):4015.

[186] Nyangaresi VO. Target Tracking Area Selection and Handover Security in Cellular Networks: A Machine Learning Approach. InProceedings of Third International Conference on Sustainable Expert Systems: ICSES 2022 2023 Feb 23 (pp. 797-816). Singapore: Springer Nature Singapore.

[187] ones. Physical Systems of Dr-Laraib A, Sial A, Ujjan RM. Addresses the Security Issues and Safety in Cyber .IGI Global .(404-InCybersecurity Issues and Challenges in the Drone Industry 2024 (pp. 381

[188] Oracevic A, Salman A. Unmanned Aerial Vehicles in Peril: Investigating and Addressing Cyber Threats to UAVs. ions, Communications and Networking (SmartNets) 2024 May 28 In2024 International Conference on Smart Applicat .IEEE .(7-(pp. 1

[189] Hosseinzadeh M, Ali S, Ahmad HJ, Alanazi F, Yousefpoor MS, Yousefpoor E, Ahmed OH, Rahmani AM, Lee SW. A m against wormhole attacks in flying ad hoc based secure routing scheme with a robust defensive syste-learning-novel Q .networks. Vehicular Communications. 2024 Jul 3:100826

[190] Datta PP. Cyber Security issues and Blockchain-Deep Learning based solutions for UAV and Internet of Drones (FANETs). arXiv preprint arXiv:2404.16848. 2024 Feb 29.

[191] Abdulrazak C. Cybersecurity Threat Analysis And Attack Simulations For Unmanned Aerial Vehicle Networks. arXiv preprint arXiv:2404.16842. 2024 Feb 12.

[192] Al-Chaab W, Abduljabbar ZA, Abood EW, Nyangaresi VO, Mohammed HM, Ma J. Secure and Low-Complexity Medical Image Exchange Based on Compressive Sensing and LSB Audio Steganography. Informatica. 2023 May 31;47(6).

[193] based UAV surveillance systems: A -Bisio I, Chiara Garibotto, Haleem H, Fabio Lavagetto, Sciarrone A. RF/WiFi .1–101201;1rnet of things. 2024 May systematic literature review. Inte

[194] Anagnostis I, Kotzanikolaou P, Douligeris C. Understanding and Securing Unmanned Aerial Vehicle (UAV) Services: .A Comprehensive Tutorial. Authorea Preprints. 2024 Mar 6

[195] diation Through Cloud Security Tools. Journal of Artificial Jimmy FN. Cyber security Vulnerabilities and Reme .71-Apr 12;2(1):129 2024 .4023-Intelligence General science (JAIGS) ISSN: 3006

[196] Richa Goenka, Chawla M, Tiwari N. A comprehensive survey of phishing: mediums, intended targets, attack and ;echniques and a novel taxonomy. International Journal of Information Security. 2023 Oct 19defence t

[197] Qu K, Ye J, Li X, Guo S. Privacy and Security in Ubiquitous Integrated Sensing and Communication: Threats, .8–52:(4)7;1magazine. 2024 Jul Challenges and Future Directions. IEEE internet of things

[198] Nyangaresi VO. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. Journal of Systems Architecture. 2022 Dec 1;133:102763.

[199] based services: A -query privacy in location-dul Ghani N, Ahmad I. Preserving locationRasheed H, Md Noor R, Ab .review. Security and Privacy.:e412

[200] Anthi E, Williams L, Ieropoulos V, Spyridopoulos T. Investigating Radio Frequency Vulnerabilities in the Internet of .80-Jun;5(2):356 2024 .Things (IoT). IoT

[201] .Kallenborn Z, Plichta M. Breaking the Shield: Countering Drone Defenses. Joint Force Quarterly. 2024;113(1):7

[202] .Sfetcu N. Electronic Warfare and Artificial Intelligence. MultiMedia Publishing; 2024 May 20

[203] V, Alishahi M. Indoor Location Fingerprinting Privacy: A Comprehensive Survey. arXiv Fathalizadeh A, Moghtadaiee .preprint arXiv:2404.07345. 2024 Apr 10

[204] Yan B, Li K, Xu M, Dong Y, Zhang Y, Ren Z, Cheng X. On protecting the data privacy of large language models (llms): A survey. arXiv preprint arXiv:2403.05156. 2024 Mar 8.

[205] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA. Symmetric Key Based Scheme for Verification Token Generation in Internet of Things Communication Environment. InApplied Cryptography in Computer and Communications: Second EAI International Conference, AC3 2022, Virtual Event, May 14-15, 2022, Proceedings 2022 Oct 6 (pp. 46-64). Cham: Springer Nature Switzerland.

[206] ed routing Sohoni P, Shrivastava SS, Sharma S. A survey on qos in flying ad hoc network based on fuzzy inference bas .(539-protocol. In2024 International Conference on Automation and Computation (AUTOCOM) 2024 Mar 14 (pp. 534 .IEEE

[207] Ali Abbasi Tadi, Dayal S, Dima Alhadidi, Mohammed N. Comparative Analysis of Membership Inference Attacks in .0–620:(11)14;19ized Learning. Information. 2023 Nov Federated and Central

[208] Wang X, Bryan C, Li Y, Pan R, Liu Y, Chen W, et al. Umbra: A Visual Analysis Approach for Defense Construction computer graphics. 2022 Against Inference Attacks on Sensitive Information. IEEE transactions on visualization and .90–2776:(7)28;1Jul

[209] Zhang S, Yuan W, Yin H. Comprehensive Privacy Analysis on Federated Recommender System Against Attribute .99–987:(3)36;1Inference Attacks. IEEE transactions on knowledge and data engineering. 2024 Mar

[210] Ding J, Ning H. Federated learning attack surface: taxonomy, cyber defences, challenges, and future ,Qammar A .606-directions. Artificial Intelligence Review. 2022 Jun;55(5):3569

[211] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6). IEEE.

[212] Ahmed I, Nahar T, Urmi SS, Taher KA. Protection of sensitive data in zero trust model. InProceedings of the .(5-international conference on computing advancements 2020 Jan 10 (pp. 1

[213] –233:(7)2;2021ion, authorization and administration. Science and Education [Internet]. Usmonov MTO. Autentificat .42

[214] Akhtar DrN, Kerim DrB, Perwej DrY, Tiwari DrA, Praveen DrS. A Comprehensive Overview of Privacy and Data ific Research in Science, Engineering and Technology. 2021 Security for Cloud Storage. International Journal of Scient .52–113;8Sep

[215] Aware Smart -Ballesté A, Solanas A. Sensors for Context-Aguilar P, Martínez-Batista E, Moncusi MA, López .6886:(20)1Healthcare: A Security Perspective. Sensors (Basel, Switzerland). 2021 Oct 17;2

[216] Jan SU, Qayum F, Khan HU. Design and Analysis of Lightweight Authentication Protocol for Securing IoD. IEEE .306–9:69287;2021Access.

[217] Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA, Nyangaresi VO, Honi DG, Abdulsada AI, Jiao X. Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map. IEEE Access. 2022 Feb 11;10:26257-70.

[218] Shafique A, Mehmood A, Elhadef M. Survey of Security Protocols and Vulnerabilities in Unmanned Aerial Vehicles. .48–46927:IEEE Access. 2021;9

[219] Hoc -Dhlan KA. A Review on Communications Perspective of Flying Ad-Zahrani A, Ullah I, Al-Noor F, Khan MA, Al Networks: Key Enabling Wireless Technologies, Applications, Challenges and Open Research Topics. Drones. 2020 .Sep 30;4(4):65

[220] based UAV communication -Turjman F. A smart lightweight privacy preservation scheme for IoT-Al ,Deebak BD .17–systems. Computer Communications. 2020 Oct;162:102

[221] revention Preserving Intrusion Detection and P-Ntizikira E, Lei W, Alblehai F, Saleem K, Lodhi MA. Secure and Privacy .in the Internet of Unmanned Aerial Vehicles. Sensors. 2023 Jan 1 [cited 2023 Oct 14];23(19):8077

[222] Putranto DS, Aji AK, Wahyudono B. Design and implementation of secure transmission on internet of drones. In2019 IEEE 6th Asian Conference on Defence Technology (ACDT) 2019 Nov 13 (pp. 128-135). IEEE.

[223] Nyangaresi VO, Ahmad M, Alkhayyat A, Feng W. Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. Expert Systems. 2022 Dec;39(10):e13126.

[224] Mosladdin Mohammad Shueb, Che X. A Review of Cybersecurity Advancements in Unmanned Aerial Vehicle. Lecture .80–369;1notes in networks and systems. 2023 Jan

[225] ion, Navigation aided uav security. In2023 Integrated Communicat-Dhakal R, Kandel LN. A survey of physical layer .IEEE .(8-and Surveillance Conference (ICNS) 2023 Apr 18 (pp. 1

[226] Efficient and Secure Communication Toward UAV -Teng L, Zhang J, Obaidat MS, Lin C, Lin Y, Shen Y, et al. Energy 76–1Networks. IEEE Internet of Things Journal. 2022 Jun 15;9(12):1006

[227] altitude UAVs: A -preserving location authentication for low-Pan H, Wang Y, Wang W, Cao P, Ye F, Wu Q. Privacy .based approach. Security and Safety. 2024;3:2024004-blockchain

[228] Tracking in Urban Environments Yan X, Fu T, Lin H, Xuan F, Huang Y, Cao Y, Hu H, Liu P. UAV Detection and .Using Passive Sensors: A Survey. Applied Sciences. 2023 Oct 15;13(20):11320

[229] Pandey GK, Gurjar DS, Nguyen HH, Yadav S. Security Threats and Mitigation Techniques in UAV Communications: .97–10:112858;2A Comprehensive Survey. IEEE Access. 202

[230] Zaki Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Signal propagation parameters estimation through designed multi layer fibre with higher dominant modes using OptiFibre simulation. Journal of Optical Communications. 2022 Jun 23(0).

[231] Turjman F, Altrjman C, Mostarda L. Anonymous Mutual and Batch Authentication with -Rajasekaran AS, Maria A, Al .Location Privacy of UAV in FANET. Drones. 2022 Jan 7;6(1):14

[232] Preserving Location Privacy and Utility in the Remote --A, Conti M, Sciancalepore S. Hide and Seek Brighente ;Identification of Unmanned Aerial Vehicles. arXiv (Cornell University). 2022 Jan 1

[233] Time Key. IEEE -IoT Networks: Space Aided-Han R, Bai L, Liu J, Choi J, Liang YC. A Secure Structure for UAV .101–96:(5)28;1wireless communications. 2021 Oct

[234] preserving target tracking strategies using a flying -Reddy SR, Lim S, Choi GS, Chae J, Pu C. DarkSky: Privacy-Chinthi .drone. Vehicular Communications. 2022 Jun;35:100459

[235] Assisted IoT Applications, -Adil M, Song H, Spyridon Mastorakis, Hussein Abulkasim, Farouk A, Jin Z. UAV Enabled Solutions, Open Challenges With Future Research Directions. IEEE transactions on -Cybersecurity Threats, AI 21–1;1intelligent vehicles. 2023 Jan .

[236] .(1)efficient algorithms in big data era. Journal of Big Data. 2021 Jan 26;8-Adadi A. A survey on data

[237] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Sep 1;15:100210.

[238] Preserving Schemes for Safeguarding -tnikova E, Vatsalan D, Moustafa N. PrivacyKeshk M, Turnbull B, Si .97–9:55077;2021Physical Systems. IEEE Access. -Heterogeneous Data Sources in Cyber

[239] ased lightweight b-Khan AS, Yahya MI, Zen KB, Abdullah JB, Rashid RB, Javed Y, Khan NA, Mostafa AM. Blockchain CMAS) cellular network. IEEE Access. 2023 Feb -based (6-dense 6G-free in ultra-multifactor authentication for cell .41-11:20524;27

[240] Khan AS, Sattar MA, Nisar K, Ibrahim AA, Annuar NB, Abdullah JB, Karim Memon S. A survey on 6G enabled light weight authentication protocol for UAVs, security, open research issues and future directions. Applied Sciences. 2022 .Dec 26;13(1):277

[241] Adil M, Hussein Abulkasim, Farouk A, Song H. $R3ACWU$: A Lightweight, Trustworthy Authentication Scheme for .12–1;1IoT Applications. IEEE transactions on intelligent transportation systems. 2024 Jan Assisted-UAV

[242] Karim N, Kanaker H, Abdulraheem W, Ghaith M, Alhroob E, Alali A. Choosing the right MFA method for online .12–201:(1)8;2024Data and Network Science. systems: A comparative analysis. International Journal of

[243] Al Kabir MA, Elmedany W. An overview of the present and future of user authentication. In2022 4th IEEE Middle East .IEEE .(17-and North Africa COMMunications Conference (MENACOMM) 2022 Dec 6 (pp. 10

[244] Aditi Zear, Virender Ranga, Bhushan K. Coordinated network partition detection and bi-connected inter-partition topology creation in damaged sensor networks using multiple UAVs. Computer communications. 2023 Apr 1;203:15–29.

[245] Al Sibahee MA, Abdulsada AI, Abduljabbar ZA, Ma J, Nyangaresi VO, Umran SM. Lightweight, Secure, Similar-Document Retrieval over Encrypted Data. Applied Sciences. 2021 Jan;11(24):12040.

[246] He B, Ji X, Li G, Cheng B. Key Technologies and Applications of UAVs in Underground Space: A Review. IEEE transactions on cognitive communications and networking/IEEE Transactions on Cognitive Communications and Networking. 2024 Jun 1;10(3):1026–49.

[247] Cao P, Lei L, Cai S, Shen G, Liu X, Wang X, et al. Computational Intelligence Algorithms for UAV Swarm Networking and Collaboration: A Comprehensive Survey and Future Directions. IEEE Communications surveys and tutorials/IEEE communications surveys and tutorials. 2024 Jan 1;1–1.

[248] Sohoni P, Shrivastav SS, Sharma S. Congestion detection and quality impact analysis using a fuzzy technique in flying ad hoc networks. In2024 International Conference on Automation and Computation (AUTOCOM) 2024 Mar 14 (pp. 483-489). IEEE.

[249] Mansoor N, Md. Iqbal Hossain, Rozario A, Mahdi Zareei, Alberto Rodríguez Arreola. A Fresh Look at Routing Protocols in Unmanned Aerial Vehicular Networks: A Survey. IEEE Access. 2023 Jan 1;11:66289–308.

[250] Subash N, Nithya B, Bangar R, Patel V. mpQUAD: Multipath Quad TCP Congestion Control in FANETs. In2023 3rd International Conference on Advances in Computing, Communication, Embedded and Secure Systems (ACCESS) 2023 May 18 (pp. 12-18). IEEE.

[251] Maheshwari A, Rajesh Kumar Yadav, Nath P. Congestion Aware Data Transmission in Mobile and Constrained IoT Network. Wireless personal communications. 2023 Mar 29;130(3):2121–36.

[252] Nyangaresi VO. A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN Computer Science. 2022 Jul 9;3(5):364.

[253] Jaimin Ghelani, Prayagraj Gharia, Hosam El-Ocla. Gradient Monitored Reinforcement Learning for Jamming Attack Detection in FANETs. IEEE access. 2024 Jan 1;12:23081–95.

[254] T. Tolga Sarı, Gökhan Seçinti. Using Centrality Based Topology Control for FANET Survivability Against Jamming. Computer networks. 2024 Apr 1;242:110250–0.

[255] Sharma J, Mehra PS. Secure communication in IOT-based UAV networks: A systematic survey. Internet of Things. 2023 Oct 1; 23:100883.

[256] Spina MG, Tropea M, De Rango F. SURA-LB: Software-defined IDS with UAV Resource Aware Load-Balancing in FANET disaster scenarios. Computer Communications. 2024 Jul 1;223:101-14.

[257] Kim T, Lee S, Kyong Hoon Kim, Jo YI. FANET Routing Protocol Analysis for Multi-UAV-Based Reconnaissance Mobility Models. Drones. 2023 Feb 25; 7(3):161–1.

[258] Niccolò Cecchinato, Toma A, Drioli C, Oliva G, Gianluigi Sechi, Gian Luca Foresti. Secure Real-Time Multimedia Data Transmission from Low-Cost UAVs with A Lightweight AES Encryption. IEEE communications magazine. 2023 May 1;61(5):160–5.

[259] Omollo VN, Musyoki S. Global Positioning System Based Routing Algorithm for Adaptive Delay Tolerant Mobile Adhoc Networks. International Journal of Computer and Communication System Engineering. 2015 May 11; 2(3): 399-406.

[260] Malhotra A, Kaur S. A quality of service-aware routing protocol for FANETs. International Journal of Communication Systems. 2024 May 10;37(7):e5723.

[261] Shi H, Wang J. Intelligent TCP Congestion Control Policy Optimization. Applied sciences. 2023 May 30;13(11):6644–4.

[262] Cao K, Zhengkong H. Intelligent anti-jamming methods for wireless networks. In2023 8th International Conference on Intelligent Computing and Signal Processing (ICSP) 2023 Apr 21 (pp. 670-674). IEEE.

[263] Abubakar AI, Ahmad I, Omeke KG, Ozturk M, Ozturk C, Abdel-Salam AM, Mollel MS, Abbasi QH, Hussain S, Imran MA. A survey on energy optimization techniques in UAV-based cellular networks: from conventional to machine learning approaches. Drones. 2023 Mar 20;7(3):214.

[264] Desnitsky V, Kotenko I. Simulation and assessment of battery depletion attacks on unmanned aerial vehicles for crisis management infrastructures. Simulation Modelling Practice and Theory. 2021 Feb 1;107:102244.