A Review of Security Frameworks in Flying Ad-hoc Networks

Jim Diockou
School of Computer Science
Leeds Trinity University
Leeds, UK
j.diockou@leedstrinity.ac.uk

Dehao Wu
Department of Computing & Informatics
Bournemouth University
Bournemouth, UK
dwu@bournemouth.ac.uk

Xin Lu
School of Computer Science
Leeds Trinity University
Leeds, UK
x.lu@leedstrinity.ac.uk

Yanguo Jing
School of Computer Science
Leeds Trinity University
Leeds, UK
y.jing@leedstrinity.ac.uk

Antesar Shabut
School of Computer Science
Leeds Trinity University
Leeds, UK
a.shabut@leedstrinity.ac.uk

Martin Barwood
School of Sport & Well Being
Leeds Trinity University
Leeds, UK
m.barwood@leedstrinity.ac.uk

***Abstract*—Flying ad-Hoc networks (FANETs) are the embodiment of a vital expansion in wireless communication in that they have become enablers of a variety of applications ranging from disaster management to military operations. Nonetheless, the dynamic and decentralized nature of FANETs introduces significant security challenges like sibyl attacks, hidden and exposed node problems that necessitate robust and adaptable security frameworks. The review categorizes and evaluates from the general to the granular current security solutions, encompassing secure routing protocols, intrusion detection systems (IDS), lightweight cryptographic methods, and trust management frameworks before outline the limits and research gaps of the currently available literature. The paper then suggests a novel security framework based on the dynamic integration of the advanced technologies of blockchain, edge and fog computing and enabler tools. With this novel framework, this paper aims to signpost stakeholders like academic and industrial researchers and practitioners towards innovative solutions that ensure the confidentiality, integrity, availability, non-repudiation, scalability, and performance aware operation of UAV networks in increasingly intricate and antagonistic milieus.**

Keywords—FANET security, flying ad-hoc networks security, UAV network security, drone network security frameworks, secure FANET communication, FANET threat mitigation.

I. INTRODUCTION

Recently, FANETs have gained significant attention across academia, industrial, and social domains due to their applications in professional areas like precision farming, journalism, aviation, and disaster management [1]. These networks are composed of multiple unmanned aerial vehicles (UAVs) that dynamically exchange data and information in real time without relying on fixed infrastructure like traditional networks. The current research works have extensively explored the features, characteristics, and challenges of FANETs. For instance, [1] provided a broad outline of FANETs by emphasizing their high mobility, dynamic topology, resource constraints, and multi-hop communication capabilities. [2] highlighted the importance of resilient routing protocols, introducing a topology-aware routing protocol that adapts to network changes using Q-learning. [3] reviewed nature-inspired routing algorithms, discussing how bio-inspired methods can improve network performance and stability in FANETs. [4] investigated the security aspects of FANETs, providing understandings of how the network's characteristics negatively impact security weaknesses and vulnerabilities before proposing mitigation approaches. In summary, FANETs can be characterised by their dynamic nature, topology changes, high mobility, multi-hop communication, decentralised management, and resource constraints. The dynamic aspect of these networks relates to the fact that nodes frequently change their altitude, longitude, and latitude. Even a minor change in these coordinates of their location require robust and dynamic routing protocol to maintain effective and efficient communication [2]. One of the consequences of their dynamism is high movements which may result in directions changes. These directions changes can or may impact the stability, reliability, consistency, performance, scalability, and security of communication links and that requires real-time adjustments to network configurations [2]. Another key feature is multi-hop communication, where data often needs to be relayed through UAVs in transit transmit nodes to reach its destination. This increases the complexity of keeping the integrity of the data being routed [1]. Their ad hoc nature makes them distributed in an autonomous and self-managed way since they do not rely on any centralised management system. As such they use distributed algorithms procedure and processes for their self-management. It is this decentralised variant of network management that improves the robustness, resilience, and reliability but this is paralleled by the introduction of new challenges in coordination and synchronization [3, 4] such as limited computational power, battery life, and storage space. These constraints negatively impact key metrics like the ones of security, performance, scalability, and regulatory compliance. So, efficient resource management is essential to ensure prolonged network security, operationality and functionality [5]. Addressing FANETs security challenges along with efficient resources management are not only critical but paramount as networks such as these tend to be particularly susceptible to various types of attacks, including sibyl attacks, GPS spoofing, denial of service (DoS), and data tampering. Additionally, FANETs are increasingly deployed in sensitive and context aware applications, where robust, reliable, comprehensive, regulatory compliant, and scalable security frameworks are indispensable to protect both the network and its users and entity nodes. However, achieving this requires a thorough review of existing security frameworks within the literature to identify effective solutions and research gaps. This paper aims to explore currently available security technologies, tools, and frameworks technologies to identify research gaps and suggest potential

areas for further research. It seeks to contribute significantly to the field by:

- providing a consolidate overview of the diverse security challenges faced by FANETs through the synthesis of insights from various studies,
- identifying the strengths, weaknesses, and gaps in current methodologies of existing security frameworks by critically analysing various recently proposed approaches and systems,
- highlighting opportunities and future directions to develop novel, dynamic and integrative architectural security mechanisms tailored specifically to the unique characteristics of FANETs.

The remainder of the paper is structured as follow: section II explores the current security challenges in flying ad hoc networks, section III investigated FANETs vulnerabilities, section IV examines the literature of FANETs security frameworks, section V and VI sequentially scrutinise the potential challenges and their possible solutions, and section VII provides closing arguments in the conclusion coupled with future research directions.

II. Security & Privacy Threats in FANETs

To review FANET security and privacy literature, search keywords like "hardware threats," "software threats," "network layer threats," "cross-layer threats," and "regulatory compliance threats" were used. Recent studies on addressing issues like jamming (e.g., frequency hopping) and privacy risks (e.g., data interception) were considered. Suggested solutions such as secure routing protocols (e.g. Ad Hoc on Demand Routing protocol) and encryption methods for UAVs, considering latency, energy consumption, scalability, and regulatory compliance were also examined. Through the review of the current literature, threat modeling, simulations, real-world testing, and case studies security and privacy challenges in FANETs were identified. Vulnerabilities in hardware, software, network layers, cross layer, and regulatory compliance were analyzed.

FANETs are networks of multiple autonomous UAVs that establish an ad-hoc network to communicate among them [6]. For their uniqueness, given their architectural structure and logical layout characteristics like dynamic, high mobility, and decentralized management, they tend to be affected by, not only, security challenges from classical networks like computers and digital telephony but also those unique to them like hidden and exposed node attacks [7]. This subsection will comprehensively explore the spectrum of security threats in FANETs ranging from overarching categories to specific challenges posed to the key data properties of confidentiality, integrity, availability, and non-repudiation. By investigating these aspects, it aims not only to highlight their critical security vulnerabilities but also outline effective strategies for safeguarding FANETs against potential risks to ensure their resilience, scalability, and overall performance. According to current research works, the security challenges in FANETs can be examined from different perspectives that include among others structural and functional.

A. Hardware Layer

FANETs have a wide physical attack surface from themselves as networks as well as constituent nodes and their respective components. Each constituent node – a UAV that's connected to an ad hoc network of drones - can be used to physical attack the network or a node if no appropriate security measures has been put in place. The literature is rich with examples of case studies. For instance, [4] used a combination of literature review and simulation methodologies to analyze the impact of security breaches in FANETs at the physical level. The attacks analyzed included sensor attacks, GPS spoofing, and battery depletion attacks. Sensor attacks occur when a malicious user intentionally disrupts any of the UAV's sensors. GPS spoofing happens when a cybercriminal injects fake signals to misdirect a UAV from its programmed path. Battery depletion attacks work by overloading communication requests, such as during drone-to-drone (D2D) interactions. Through simulations and comparative analysis, they found that battery depletion occurs 18.5% faster, potentially leading to uncontrollable failures within the network. [1] provided a comprehensive study on physical attacks in hostile environments where UAV functions can be disabled. These diverse physical attacks highlight the complexity of securing FANETs against both intentional and environmental threats. Addressing these challenges requires the development of robust security frameworks and protocols tailored to the unique operational dynamics and vulnerabilities inherent in FANET environments.

B. Network Layer

These attacks specifically target the network protocols that manage the routing of data from source to destination within FANETs, which are particularly vulnerable due to frequent changes in topology. In [8], through case studies, literature review, vulnerability analysis, and comparative analysis, it was found that attacks on dynamic source routing protocols significantly impact network performance, particularly in terms of route discovery, route maintenance, and data forwarding. Attacks on route discovery can lead to network disruption by introducing malicious nodes and false routes, resulting in increased overhead from storing and processing irrelevant traffic, which in worst-case scenarios, may cause mission failure. Given that topological dynamism is a key feature of FANET networks, these attacks make it difficult for legitimate nodes to efficiently route packets.

[4] simulated attacks such as sinkhole, blackhole, flooding, and packet dropping to critically analyze the impact of security breaches on the performance of routing protocols like Ad Hoc On Demand Distance Vector (AODV). The study found that these attacks negatively affect packet delivery ratio (PDR), end-to-end delay (E2E), and routing overhead, with the last two metrics increasing and the former decreasing. For example, in the context of a flooding attack, PDR can drop to around 60%. In a standard network context, if the average E2E latency for data packets is 1000 milliseconds (1 second), meaning it takes 1 second on average for a packet to travel from its source to its destination, a routing attack like a wormhole attack, where a cybercriminal creates a shortcut in the network to misroute packets, could increase E2E latency to 2000 milliseconds (2 seconds) due to the additional processing power and time required, causing delays. This increase in routing delay can significantly impact the performance of real-time UAV applications, such as video streaming or navigation.

C. Software Layer

At this layer, threats are related to path planning and coordination of UAVs in an ad hoc network. The software's

functionalities include the management of communication and coordination protocols between network nodes. These types of attacks differ from the ones examined in the previous sections in that they exploit the vulnerability and security weaknesses resulting from the architecture of software algorithms. Examples include malware, backdoors, and zero-day attacks, impersonation attack, and identity attack software. [9] found that identity impersonation, and data interception security challenges can negatively affect the performance and the key security features of FANETs networks. In identity impersonation attacks like sibyl, an attacker can make a drone take off at an incorrect time and direct it to a wrong landing location by transmitting false signals using a false identity. The aforementioned security challenges explicitly target the identities of identifiable components within FANET networks, such as users, UAVs, and other network entities, posing significant risks to the security of FANET data. The following paragraphs will discuss these security challenges at a granular level, specifically focusing on data security.

D. Cross Layer Threats

Data-related threats in FANETs can be identified based on the key security properties of confidentiality, integrity, availability (CIA), and non-repudiation, which apply across hardware, software, and network layers in the context of the following communication scenarios: drone to drone (D2D), drone to ground control station (D2GCS), drone to satellite (D2S), and drone to third-party communication systems (D2TPCS), such as passenger communication in drones-as-taxis or parcel delivery systems. Each communication type can suffer from specific data breach scenarios.

In D2D communication, confidentiality—ensuring that data is only accessible to authorized nodes and users—is maintained through cryptographic technologies. Integrity—ensuring that data is correct, accurate, and trustworthy—is achieved by applying hashing algorithms. Availability ensures that data is accessible to legitimate nodes and users when needed, resulting from proper implementation of the first two security properties alongside non-repudiation, which is guaranteed by digital signatures. These signatures ensure that nodes or users exchanging data cannot later deny their participation in the communication process.

The threats to these essential data security properties were covered in [10, 11]. In [2], the Q-Learning adaptive learning approach and topology change detection were applied to analyse CIA and non-repudiation security threats comprehensively, revealing impacts on packet delivery, end-to-end delay, and energy efficiency. [7] utilized DoS mitigation techniques and adaptive learning algorithms to examine security challenges related to CIA and non-repudiation. Studies [5, 12-14] analysed interception (C), interference (I), and injection (NR) of data in the context of D2GCS communication. D2S communication data threats were comprehensively reviewed in [15-18]. Data threats related to D2TPCS during data exchange, particularly concerning drones operating as taxis, were examined in [19], highlighting their significant impact on key properties of data protection and user privacy.

E. Regulatory Compliance Layer

Security attacks at this layer are consequences of cross-cutting challenges that can be impactful on all layers of FANETs. Thus, influencing how hardware is configured and deployed, how software is installed, configured, and utilized, and how networks are managed in compliance not only with legal standards but also policies and recommended best practices. Expressed differently, regulatory compliance attacks on FANETs refer to threats or vulnerabilities that emanate from the lack of adherence to regulatory standards, policies, procedures, processes, and protocols. Consequences can lead to security breaches, data leaks, or disruptions in service. Most of the security threats that have been viewed so far from [4] to [18] apply.

But analysing security challenges from the above categorizations is akin to understanding them as an assemblage of discrete elements of security threats and not as an analogue system of integrated security challenges of physical [20, 21], data link [22-24], network [25-27], transport [28, 29], and application layers [30-32]. That is why some papers have examined their security challenges from the multidimensional and integrative approach. Examples include [33]. This integration paradigm can be explained by the fact that FANETs networks are dynamic, and not static. Only this dynamic approach can provide a multidimensional, thorough, and integrative examination of their security challenges. In conclusion, the categorisation of data-related threats in FANETs highlights the critical security challenges across various communication scenarios. While some studies explored valuable insights into these specific threats, others focused on the ones related to networks theoretical frameworks, design principles, and protocols or logical arrangements of devices and their associated communication links. Future research should focus on developing adaptive security frameworks that can dynamically respond to their dynamic environments and applications and not on discrete specifics. But before that, to be more comprehensive, security vulnerabilities require an exploration.

III. FANETS VULNERABILTIES

This section provides an overview of some of the published papers on FANETs security vulnerabilities, focusing on their topologies, communication protocols, operations, hardware, physical environment, and applications. Each of these contexts is characterized by its own unique security threats. Additionally, each context is faced by multifaceted types of threats as per their multi-layered features given vulnerability is "…an intended characteristics of a computing component or system configuration that multiplies the risk of an adverse event or a loss occurring either due to accidental exposure, deliberate attack, or conflict with new system components" [34]. The following paragraphs explore some of the vulnerabilities from the literature.

A. Network Structure & Connectivity

FANETs topologies range from tree to mesh through to ring. Due to their dynamism, they are vulnerable to disruptions from high mobility that can cause frequent link outages and network partitioning. Sparse node density can affect connectivity issues, while single points of failure in hierarchical topologies risk network failure if key nodes fail. These vulnerabilities undermine communication stability and network resilience as their topologies significantly impact resilience by determining connectivity, communication stability, and fault tolerance. The solution resides in the

effective topology management to enhance resilience by ensuring stable, scalable, and fault-tolerant communication paths. [4] analyzed the weaknesses in currently available routing protocols in the context of the effectiveness and efficiency of suggested cryptographic and trust-based platforms. Their weaknesses can be the root cause of vulnerability attacks, such as blackhole attacks, where malicious UAVs drop packets instead of forwarding them, and wormhole attacks, where hackers create false links to misroute packets. The dynamic topology and mobility of FANETs can compromise overall network resilience, as these factors increase the risks associated with disrupted communication, incorrect routing decisions, and potential network partitioning. FANET routing protocols directly impact resilience by determining how effectively the network adapts to dynamic topologies, node mobility, and link failures. Robust protocols like Dynamic Source Routing (DSR) ensure reliable communication, minimize delays, and maintain network connectivity, enhancing the network's ability to recover from disruptions and sustain critical operations.

B. Data Security & Integrity

[35] explored vulnerabilities that are associated with the challenges of ensuring data integrity in an ever-changing topology. Data integrity is essential for resilience, as its compromission can lead to incorrect decision making, mission failures, or data regulatory compliance breach. Data integrity breaches in FANET vulnerabilities include tampering attacks, where adversaries inject false navigation commands during transmission, leading to misinformation; replay attacks, where attackers maliciously resend valid data, making it outdated or misleading; and packet corruption, which can result from interference or weak encryption, causing errors and jeopardizing mission-critical decisions. Guaranteeing data integrity through efficient encryption and error-checking methods improves network reliability, attacks prevention, and maintains the operational reliability of the network, even under adverse conditions or attacks. [4] analyzed the weaknesses in currently available routing protocols in the context of the effectiveness and efficiency of suggested cryptographic and trust-based platforms. Their weaknesses can be the root cause of vulnerabilities attacks like blackhole where malicious UAVs drop packets instead of forwarding them. Dynamic topology and mobility can cause the compromission of overall network resilience given the increase of risks that are consequences to disrupted communication, incorrect routing decisions, and potential network partitioning. FANET routing protocols directly impact network resilience by determining how effectively the network adapts to dynamic topologies, node mobility, and link failures. Robust protocols, such as Ad hoc On-Demand Distance Vector (AODV) or DSR, ensure reliable communication, minimize delays, and maintain network connectivity, thereby enhancing the network's ability to recover from disruptions and sustain critical operations.

C. Access Control & Trust

[35] investigated authentication related security weaknesses before suggesting solutions based on energy efficiency. They range from Sybil attacks to replay and impersonation and insufficient mutual authentication attacks where, for instance, if only the ground station is authentication, UAVs might still be vulnerable to attacks. These vulnerabilities can severely impact FANET resilience by allowing unauthorized access, enabling malicious attacks, and disrupting critical network operations. To address these vulnerabilities, implementing strong, scalable, and distributed authentication mechanisms tailored to the unique challenges of FANETs is essential. FANET authentication is crucial for resilience, as it verifies the legitimacy of participating UAVs, preventing unauthorized access and Sybil attacks. Effective authentication strengthens security, upholds trust, and protects the network from malicious entities, ensuring stable and reliable operations for mission-critical communications. For more information on operational, hardware and physical layer, environmental, application, and privacy visit [4] where they are comprehensively explored. These publications provided a multidimensional exploration of the varied FANETs security vulnerabilities to deepen the understanding of the issues that are at stake. This insightful and exhaustive understanding will help facilitate the proposition of solutions to enable the mitigation of their impact on the privacy of their stakeholders.

IV. FANETS SECURITY FRAMEWORKS

Current research in FANETs networks security is driven by the quest for robust security frameworks Below are examples from the reviewed literature that illustrate the various vulnerabilities and challenges in FANETs, as well as proposed solutions and best practices.

A. Authentication

[36] Used comparative analysis to analyse their certificateless free pairing authentication (CLAS) mechanism to existing technologies like such in [37]. Their CLAS scheme strategy improved the authentication efficiency of nodes through the elimination process of bilinear pairing operations given they are computationally intensive compared to scalar point multiplications. Their results demonstrated that CLAS has lower computational costs in various stages of the process. For instance in key generation CLAS method required 3n TSM, which is the time required to complete a single scalar multiplication operation in elliptic curve cryptography compared to non CLAS like as in [37] that required 2nTSM. [23] aims and objectives that were to enhance the security of FANETs security, suggested a certificateless key-encapsulated signcryption (CL-KESC) scheme that syndicates encryption and signature functionalities to ensure data confidentiality, integrity, availability, and authenticity. Their essential goal was to develop a security framework that does not require certificate management in addition to escrow. Using design methodology, security proof, and performance examination, they found that their newly designed security framework not only improved key performance metrics of performance relating to storage and computational processing power, but also, made security more effective and efficient against security threats. They became more effective and efficient since the proposed CerCL-KESC encryption scheme is based on hyperelliptic curve cryptography (HECC) that requires less computational resources compared to the ones that utilised certificates. It should be remarked that even though their new model is based on the elliptic curve cryptography (ECC) technology, its key characteristic was the utilisation of smaller key length of 80 bits compared to the ECC's 160. The novel approach to their paper can be found in

its architectural trade-offs between security and performance by adopting a security scheme that did not involve certificates storage and management. Its mathematical security proofs based on hyperelliptic curve cryptography, which protect the network against various types of threats, make this nascent scheme suitable for resource-constrained devices in terms of storage and computational power. Moreover, it is quintessential to note that the proposed framework in case of dramatic increases in number of drones joining the network, performance problematics would arise. Thus, network scalability is an issue, and no solution from the paper was suggested.

B. Decentralized, Secure & Scalable Data Processing with Blockchain & Fog Computing

[37] developed a blockchain and fog computing based lightweight security framework to address the above-mentioned scalability problem in parallel with data integrity, traceability, availability, and authenticity. To achieve this objective systematic literature review, analysis of fog computing and blockchain technologies, and their contexts of applications were de rigueur. The proposed framework is layered to meet scalability needs and requirements. It is composed of a blockchain layer, which enhances the security, integrity, authenticity, and immutability of both collected and transmitted data; a fog computing layer, designed to process data at the edge device level when needed to minimize latency and end-to-end delay in context-aware applications where real-time decision-making is critical; and a communication layer, responsible for applying secure communication protocols to ensure the secure transmission of data in transit. It also addressed the issues relating to regulatory compliance through the implementation of blockchain that ensure data immutability, traceability, and auditability. Even though this architectural secure network framework enhanced the data security coupled with network operation ability, it did not explicitly examine post quantum computing security challenges even if the application of blockchain and its adaptability to future and potential security requirements is a possibility.

C. Dynamic Integrated Solutions For Intrusion Detection, Performance, & Scalability

Other noticeable advances in the proposition of FANETs security frameworks were evidenced in [15] and [25]. In [25], the authors comprehensively reviewed the security and performance concerns of FANETs. They not only proposed blockchain integration for enhanced security and network scalability but also highlighted the importance of efficient resource management, optimal energy utilization through renewable energy sources, and the adoption of efficient security protocols to extend the lifespan of drone missions. In [15], the authors proposed a comprehensive approach to addressing denial-of-service attacks in FANETs by integrating both anomaly and signature-based intrusion detection systems (IDS), data restraining to manage data overflow, traffic analysis, dynamic and multipath routing, power and energy efficiency, resource monitoring, and blockchain technology. Their focus was on tackling security challenges across the physical, medium access, network, transport, and application layers. While both papers proposed dynamic security frameworks, architectural weaknesses affect key security and performance aspects—confidentiality, integrity, availability, non-repudiation, and scalability—due to the use of blockchain technology and multipath routing algorithms. Confidentiality is weakened by the fact that blockchain and IDS are resources intensive. Integrity weakness is caused by the usage of signature-based IDS that are limited to known attacks signatures. Availability is negatively impacted by delays in data and transmission due to required processing power that is constrained in drones. Non-repudiation can also be negatively impacted as required computational power to process digital signatures in the context of blockchain is also computational power intensive. Scalability weaknesses are again in rapport to the implementation of blockchain due to its high computational resources' requirements especially when proof of work is used as consensus algorithm. Regulatory compliance has not been extensively covered in terms of tools and technologies used.

In summary, the papers discussed have addressed the problem from one or more perspectives using discrete or relatively integrative methodologies, but not in a comprehensive and holistic manner. The consequences of modelling security frameworks as such range from inflexibility as the system grows in numbers to lack of real time response capabilities specially in uses cases where there are urgent requests of flight path change, firmware update, insufficient user and entity node behaviour analytics that require real time decision making.

D. Research Gaps & Suggested Solution

Looking ahead, as FANETs find increasing applications in various domains, the security challenges become more and more pronounced. Future directions should aim to develop an integrated and dynamic security framework as stated in [6]. This integrated framework should be structured in a layered approach to modularize the security threat landscape and should include blockchain, edge computing, fog computing, and certificateless authentication. Blockchain is defined in [38] as an encrypted and hashed chronological chain of transactions, where each block contains not only multiple transactions but also a proof necessary to guarantee consensus among concerned entities in the network. For instance, a transaction like a UAV authentication is added to blockchain through a process that ensures security, traceability, transparency, and immutability. First, the concerned creates and signs a transaction, then the transaction is broadcast to the network. To guarantee its legitimacy nodes in the network validate it. With other verified transactions they are grouped into a block. The block is proposed for addition to the blockchain via an agreement algorithm like proof of stake. After agreement, the block is then added to the blockchain, the chain is updated and then, is broadcast to all nodes. Once many more blocks are added, the transaction is fully confirmed, making it tamper-proof and irreversible. Its lightweight form will be implanted given the resource constrained nature of UAVs. Edge Computing as defined in [39, 40] is a distributed computing model that enhances the traditional cloud computing paradigm by forwarding processing capabilities closer to the network's edge. This approach allows for real-time data processing and decision-making at or near the source of data generation, particularly in UAV networks, thereby reducing latency and improving response times. Fog Computing as defined in [39, 40] is a system-level horizontal architecture that distributes computing resources, storage, control, and networking across various nodes within the network, from the cloud to the edge. This decentralized approach enhances the efficiency and functionality of edge computing by enabling complex, context-aware tasks to be handled closer to where they are

needed, providing a more flexible and responsive computing environment, particularly useful in applications like FANETs. The mobile version of both paradigms will be applied given the dynamic nature of FANTs. Certificateless authentication (36) is a cryptographic approach that eliminates the need for traditional public key certificates, which are used to verify the authenticity of a user's public key in a public key infrastructure (PKI). In certificateless authentication, the reliance on certificates and the associated infrastructure (such as Certificate Authorities, or CAs) is removed, simplifying the authentication process and reducing the risk of issues like certificate revocation or expiration. Finally, to guarantee regulatory compliance tools like the ones of National Institute of Standards and Technology (NIST) will be deployed on nodes.

The security framework's integrative and dynamic architecture will be demonstrated through its ability to provide real-time decision-making at the edge device level, ensure secure data communication between nodes, and generate compliant solutions adaptable to the ever-changing landscape of current and future digital environments, all while maintaining energy efficiency. This framework will enable new application strategies and developments due to its embedded agile nature, structural modularity, and potential for new use cases. Its agility allows stakeholders, such as academic and industrial researchers and developers, to rapidly prototype, develop, test, deploy, and maintain applications tailored to specific technologies or tools, leveraging each's strengths as required. However, it is important to acknowledge its weaknesses, such as the lack of coverage for security and performance issues arising from environmental factors like weather conditions, airspace management, and node component architectural design, along with the challenges inherent in integrating these technologies.

V. Challenges

The challenges are many and varied. They relate to technological as well tools choices problems that are inherent to each technology in addition to their seamless integration. What follows is just a nomenklatura of the salient ones. Blockchain has scalability and performance issues [39, 41] especially when proof of work is implemented as the consensus algorithm. From the security perspective some blockchains can lead to metadata exposition due to their public nature especially in public and hybrid ones, which have the potentiality of causing possible privacy and trust issues. Interoperability has the potential to be an issue as different blockchain platforms use different protocols as well as standards [40]. Edge and fog computing challenges have to do with the distribution of the processing of data across many nodes when required. This can lead to the increase of the attack surface and its consequence of finding how to ensure data is transmitted securely. Edge and fog computing have performance related problems as outlined in [42] since the process of distributing digital data to the edge or fog nodes demands vigorous processing and offloading management to ensure performance reliability and robustness. The array of nodes and their computational power can lead to irregular and inconsistent performance. One of the consequences to this may be the interoperability problem which can also be caused by the usage of different protocols by different solutions. From resource management perspective, [42] showed that the efficient management of computational, storage, and energy resources across numerous and varied unrelated edge/fog nodes in setups and configurations demands enhanced orchestration and organisational tools. As listed in [43], implementation blockchain technology in compliance with the general data protection regulation (GDPR) can be complex and challenging due to blockchain's immutability property, which directly conflicts with the GDPR's "right to be forgotten". As described in [44], certificateless free pairing authentication faces several challenges, including key management and distribution issues, where effective key distribution and management are still necessary. Additionally, there are concerns about computational overhead through to interoperability [43], key revocation mechanisms, and security assumptions and proofs [43], which depend on the hardness of the bilinear Diffie-Hellman problem. The results showed that integrating the technology with existing infrastructure can be difficult. So, the choice of technologies and tools is key to addressing the challenges identified above.

VI. Solutions to Challenges

The integration of advanced technologies such as blockchain, edge and fog computing, and certificateless free pairing authentication mechanisms presents various challenges that must be addressed to ensure the seamless operation of FANETs. The next section suggests potential solutions to the identified problems.

A. Blockchain Challenges in FANETs

Blockchain technology, particularly with proof of work (PoW) consensus algorithms, faces significant scalability and performance issues [44]. For FANETs, transitioning to more efficient consensus, algorithms such as proof of stake (PoS), delegated proof of stake (DPoS), or practical byzantine fault tolerance (PBFT) can be applied to significantly reduce the computational burden. PoS reduces the requirement for high computational power as it is based on validators, which are selected based of their stake in the network. Their lower computational needs and faster agreement time make it suitable for drones [35]. DPoS is an enhancement of PoS. It operates by delegating the verification and validation procedures to a small cluster of elected validators to shorten the consensus process time. Furthermore, public and hybrid blockchains can expose metadata, potentially leading to privacy and trust issues. In the context of FANETs, implementing privacy-preserving techniques such as zero-knowledge proofs (ZKPs, elliptic curve cryptography digital signatures (ECDSA), and ring signatures can ensure that transaction details remain confidential while maintaining the transparency and integrity of the blockchain. For instance, ZKPs can be used to authenticate and verify transactions like the transmission and recording of flight path change without revealing metadata to non-authorised users and entities. Besides, different blockchain platforms use varying protocols and standards, making interoperability problematic. Developing and adopting cross-chain communication protocols and standards like the inter-ledger protocol (ILP), and atomic swaps can enable seamless interaction between different blockchain networks, facilitating their use in FANETs. ILP allows FANETs to transact with GCS systems running on different platforms. Swaps can be implemented to enforce trust between cooperating nodes to perform assigned tasks like collecting a parcel and delivering it to its receiver’s address with the focus on the atomicity of the task. But, again, it must be stated that like any technology, these technologies are not immune to attacks. For instance [44] found that PBFT is vulnerable to attacks from latency in view change

requirement as nodes join and leave the network. Others include scalability and high computational overhead given the resource-constrained nature of UAVs. ECDSA is vulnerable to post quantum attacks as it has not yet transitioned to post quantum cryptography. [44] found that atomic swaps as cross chain transactions solution are vulnerable to mining manipulation and has scalability issues.

B. Edge and Fog Computing Challenges in FANETs

Distributing data processing across many nodes in FANETs increases the attack surface. The literature abounds with technologies to minimize the attack surface. They include advanced encryption techniques, secure multi-party computation (SMPC), and blockchain, robust intrusion detection and prevention systems (IDPS). Advanced encryption schemes like bimodal lattice signature scheme (BLISS) [45], for its low computational overhead and future proofing capabilities, can be deployed to guarantee security of distributed data and information processing including in post cloud computing. Using BLISS_B library will enhance the integration with edge nodes in relation to their configuration, key management process, and signature verification. To address performance reliability when distributing data to edge or fog nodes due to the requirement of rigorous processing and offloading management, orchestration platforms like Open Horizon along with implementing quality of service (QoS) mechanisms can be utilised. Developing advanced resource orchestration tools that use machine learning algorithms for predictive resource allocation and optimization can enhance the efficiency of resource management of computational, storage, and energy resources across varied edge/fog nodes. Technologies like FogFlow can be used for context aware real time dynamic resource provisioning and workload management in FANETs. For instance, in use cases like drones as taxis where a drone taxying a human passenger detects flying birds in its path, FogFlow will allow the drone to process this data and change its path accordingly. These technologies are also not without their inherent challenges. BLISS weaknesses include vulnerability to side-channel attacks in addition to the fact it is highly sensitive to parameter selections, FogFlow suffers from limited standardisation and security and privacy threats.

C. Compliance and Regulatory Challenges

The immutability of blockchain conflicts with the GDPR's "right to be forgotten." Implementing off-chain storage solutions and using techniques like selective redaction and chameleon hashing can enable certain data to be altered or removed while preserving the integrity of the blockchain, ensuring compliance in FANETs.

D. Certificateless Free Pairing Authentication Challenges in FANETs

As for Certificateless Free Pairing Authentication, the key components of the solution to the challenges are key management and distribution, computational overhead, and interoperability and key revocation. Using hierarchical key management schemes and decentralized key distribution mechanisms, enhanced by blockchain can solve key distribution and management challenges by having fog nodes keys stored and managed by a blockchain platform. For instance, when a taxi drone needs to join a network the fog node generates a key pair and register the public key on the blockchain. For validation purpose other drones already in the network will have the storage and the processing capabilities to retrieve the public key before verifying and validating the transaction. The reduction of computational overhead can be achieved by implementing lightweight and energy efficient blockchain protocols like internet of things application (IoTA) or directed acyclic graph (DAG) based blockchain solutions. Developing standardized protocols for key revocation and interoperability, employing blockchain for revocation transparency, and automating key lifecycle management can enhance efficiency in FANETs and improve interoperability between different platforms, especially since drones from various manufacturers may utilize different blockchain technologies. Key revocation and key immutability will be enforced via blockchain by the irrevocability process of revoked. The immutability process of keys will permit new keys to be added and existing ones not altered. Transparency will be enforced as all nodes within the network have access to the information relating to the revoked keys. For more details visit [4]. These are just some of the theoretical as well as practical solutions to the challenges identified. But as any technology they are not without challenges as mentioned in the previous subsections.

VII. CONCLUSION & FUTURE WORKS

FANETs are a critical area of industrial, civil, military, and academic domains of research that requires ad infimum attention and innovation. This paper reviewed the current state of FANET security frameworks from different perspectives to identify key challenges in the context of the security and performance key paradigms. From there it then explored the potential to integrate emerging technologies of blockchain, edge and fog computing, and certificateless authentication mechanism as well as regulatory compliance tools. It proceeded to the challenges that relate not only to the architectural integration of the said technologies and tools but also the architectural implementation of each. By doing so, it provided a roadmap for future research directions, which future research directions must address the challenges examined above by focusing on the development of adaptive and smart security framework based on the technologies and the tools identified above. Expressed differently, the choice of technologies and tools is key to addressing the challenges identified above. If carried out properly then and only then would this novel framework guarantee the key performance, security, scalability, energy efficiency, and reliability metrics of FANETs networks.

REFERENCES

[1] F. Pasandideh, J. P. J. da Costa, R. Kunst, N. Islam, W. Hardjawana, and E. P. de Freitas, "A Review of Flying Ad Hoc Networks: Key Characteristics, Applications, and Wireless Technologies," CQUniversity, Journal contribution, 2022. Available: https://hdl.handle.net/10779/cqu.23584752.v1

[2] Y. Cui, Q. Zhang, Z. Feng, Z. Wei, C. Shi and H. Yang, "Topology-Aware Resilient Routing Protocol for FANETs: An Adaptive Q-Learning Approach," in *IEEE Internet of Things Journal*, vol. 9, no. 19, pp. 18632-18649, 1 Oct.1, 2022, doi: 10.1109/JIOT.2022.3162849.

[3] A. Yadav and S. Verma, "A Review of Nature-Inspired Routing Algorithms for Flying Ad Hoc Networks," in *Applications of Artificial Intelligence in Engineering*, Singapore: Springer, pp. 105-117, 2023. doi: 10.1007/978-981-99-1234-7_10.

[4] Ceviz, O., Sadioglu, P. "A Survey of Security in UAVs and FANETs: Issues, Threats, Analysis of Attacks, and Solutions" https://www.researchgate.net/publication/371871629_A_Survey_of_Security_in_UAVs_and_FANETs_Issues_Threats_Analysis_of_Attacks_and_Solutions accessed 12/4/24

[5] A. Mohamed et al., "Topology-Aware Resilient Routing Protocol for FANETs," *arXiv preprint arXiv:2306.17360*, 2023. [Online]. Available: https://arxiv.org/abs/2306.17360.

[6] Mahalle, A., Khandelwal, S., Dhore, A., Barbudhe, V., & Waghmare, V. (2024). Cyber attacks on UAV networks: A comprehensive survey. *Review of Computer Engineering Research*, *11*(1), 45-57. https://doi.org/10.18488/76.v11i1.3636

[7] A. Chriki, H. Touati, H. Snoussi, and F. Kamoun, "FANET: Communication, Mobility Models and Security Issues," *Ad Hoc Networks*, vol. 94, pp. 101935, Oct. 2019. doi: 10.1016/j.adhoc.2019.101935.

[8] M. Shafique et al., "Secure Routing in FANETs to Mitigate Wormhole Attacks," IEEE Access, vol. 8, pp. 53330-53340, 2020. doi: 10.1109/ACCESS.2020.2980895.

[9] M. Ahmed et al., "Machine Learning-Based Intrusion Detection in FANETs," *International Journal of Machine Learning and Cybernetics*, vol. 14, no. 1, pp. 98-110, 2023. doi: 10.1007/s13042-021-01456-8.

[10] A. Mohamed et al., "Topology-Aware Resilient Routing Protocol for FANETs," *arXiv preprint arXiv:2306.17360*, 2023. [Online]. Available: https://arxiv.org/abs/2306.17360

[11] X. Wang, Y. Liu, and T. Zhang, "Mitigating DoS Attacks in Drone-to-Drone Communication in FANETs," *IEEE Access*, vol. 7, pp. 48732-48745, 2019. doi: 10.1109/ACCESS.2019.2908324.

[12] R. Gupta, M. Khanna, and S. Kumar, "Ensuring Data Integrity in Drone-to-Drone Communication within FANETs," *Journal of Communications and Networks*, vol. 22, no. 4, pp. 310-318, 2020. doi: 10.1109/JCN.2020.000012.

[13] X. Wang, Y. Liu, and T. Zhang, "Mitigating DoS Attacks in Drone-to-Drone Communication in FANETs," *IEEE Access*, vol. 7, pp. 48732-48745, 2019. doi: 10.1109/ACCESS.2019.2908324.

[14] H. Li, Y. Zhang, and Z. Chen, "Blockchain-Based Non-Repudiation Framework for Drone-to-Drone Communication," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 3, pp. 1790-1800, 2021. doi: 10.1109/TII.2020.2998744

[15] H. Li, W. Zhang, and Z. Chen, "Frequency Hopping Techniques for Jamming Resistance in Drone-to-Ground Control Communication," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 9, pp. 9275-9284, 2020. doi: 10.1109/TVT.2020.3009898.

[16] J. Park, H. Lee, and J. Kim, "Obfuscation Techniques to Protect Drone-to-Satellite Communication from Traffic Analysis Attacks," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 57, no. 2, pp. 1234-1246, 2021. doi: 10.1109/TAES.2020.2982347.

[17] L. Zheng, X. Chen, and Y. Wang, "Ensuring Data Integrity in Drone-to-Satellite Communication," *IEEE Communications Letters*, vol. 24, no. 8, pp. 1824-1827, 2020. doi: 10.1109/LCOMM.2020.2990912.

[18] Y. Huang, J. Zhao, and W. Yang, "Resilience Techniques for Drone-to-Satellite Communication under DoS Attacks," *IEEE Access*, vol. 9, pp. 1824-1835, 2021. doi: 10.1109/ACCESS.2021.3052489

[19] H. Kim, S. Park, and Y. Lee, "Blockchain-Based Non-Repudiation Framework for Drone-to-Satellite Communication," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 56, no. 4, pp. 2841-2852, 2020. doi: 10.1109/TAES.2020.2988762.

[20] M. K. Khan, R. Amin, and M. Atiquzzaman, "Securing Passenger and Third-Party Communications in Drone Taxis Using Advanced Encryption Protocols," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 2, pp. 1123-113

[21] M. Ammar et al., "Adaptive Filtering Techniques to Mitigate Jamming Attacks in FANETs," *IEEE Communications Magazine*, vol. 58, no. 6, pp. 61-67, 2020. doi: 10.1109/MCOM.2020.9146152.

[22] N. Kumar et al., "Physical Layer Security in UAV Communications: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2252-2280, 2021. doi: 10.1109/COMST.2021.3059381

[23] A. Mahmood et al., "Secure MAC Protocol for FANETs," IEEE Transactions on Vehicular Technology, vol. 70, no. 3, pp. 2520-2531, 2021. doi: 10.1109/TVT.2021.3058742.

[24] S. Khan et al., "Lightweight Cryptographic Techniques to Prevent Replay Attacks in FANETs," IEEE Communications Letters, vol. 26, no. 2, pp. 356-359, 2022. doi: 10.1109/LCOMM.2022.3140172

[25] M. Alshahrani et al., "Enhanced MAC Protocol for Security in FANETs," Ad Hoc Networks, vol. 108, pp. 102287, 2021. doi: 10.1016/j.adhoc.2020.102287.

[26] P. Goyal et al., "Trust Management for Mitigating Sybil Attacks in FANETs," IEEE Systems Journal, vol. 15, no. 4, pp. 5463-5473, 2021. doi: 10.1109/JSYST.2020.3033614.

[27] M. Iqbal et al., "Secure Routing in FANETs: Challenges and Countermeasures," IEEE Transactions on Vehicular Technology, vol. 70, no. 2, pp. 1203-1214, 2021. doi: 10.1109/TVT.2020.3048371.

[28] M. Rizwan et al., "Secure Session Management in FANETs," IEEE Transactions on Network and Service Management, vol. 19, no. 1, pp. 45-56, 2022. doi: 10.1109/TNSM.2021.3134867

[29] F. Bashir et al., "Transport Layer Security in FANETs: A Comprehensive Survey," IEEE Communications Surveys & Tutorials, vol. 24, no. 2, pp. 812-835, 2022. doi: 10.1109/COMST.2022.3149175.

[30] T. Alam et al., "Anomaly Detection Systems for Preventing Malware Injection in FANETs," IEEE Access, vol. 9, pp. 39864-39875, 2021. doi: 10.1109/ACCESS.2021.3059548.

[31] F. Siddiqui et al., "Encryption Strategies to Prevent Data Theft in FANETs," IEEE Transactions on Information Forensics and Security, vol. 17, pp. 67-78, 2022. doi: 10.1109/TIFS.2021.3115679

[32] A. Mirza et al., "Application Layer Security Protocols for FANETs," IEEE Transactions on Wireless Communications, vol. 19, no. 10, pp. 6773-6782, 2020. doi: 10.1109/TWC.2020.3007816.

[33] R. Sharma, A. Kaul, and S. Joshi, "Resolving Hidden Node Problem in FANETs: A Collision Avoidance Mechanism," *Journal of Network and Computer Applications*, vol. 199, pp. 103-117, 2022. doi: 10.1016/j.jnca.2021.102945

[34] Spiceworks. "What is a Security Vulnerability?" Spiceworks, https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-a-security-vulnerability/. Accessed Jul. 11, 2024

[35] M. Alomari, A. Mahmood, and N. Kumar, "Security in UAV Communication Networks: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 2282-2317, 2020. doi: 10.1109/COMST.2020.2966015.

[36] M. U. Hassan, M. H. Rehmani, and J. Chen, "A Certificateless Pairing-Free Authentication Scheme for Unmanned Aerial Vehicle Networks," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 9463606, 2021. [Online]. Available: https://onlinelibrary.wiley.com/doi/epdf/10.1155/2021/9463606. [Accessed: June. 1, 2024].

[37] R. Aldossri, A. Aljughaiman, and A. Albuali, "Advancing Drone Operations through Lightweight Blockchain and Fog Computing Integration: A Systematic Review," *Drones*, vol. 8, no. 4, p. 153, Apr. 2024. doi: 10.3390/drones8040153

[38] D. Yang, C. Long, H. Xu, and S. Peng, "A Review on Scalability of Blockchain," [Online]. Available: https://chatgpt.com/c/16357833-988c-4e39-b8a1-8d824e771263. Accessed: June 1, 2024.

[39] Ai, Y., Peng, M., & Zhang, K. (2018). Edge computing technologies for Internet of Things: A primer. *Digital Communications and Networks*, *4*(2), 77-86. https://doi.org/10.1016/j.dcan.2017.07.001

[40] Habibi, P., Farhoudi, M., Kazemian, S., Khorsandi, S., & Leon-Garcia, A. (2020). Fog Computing: A Comprehensive Architectural Survey. *IEEE Access*, 8, 69105-69120. doi: 10.1109/ACCESS.2020.2983253.

[41] M. Ndiaye and K. Konate, "Security Strengths and Weaknesses of Blockchain Smart Contract System: A Survey," *World Academy of Science, Engineering and Technology, International Journal of Information and Communication Engineering*, vol. 16, no. 5, pp. 134-143, 2022.

[42] S. Dustdar, C. Avasalcai, and I. Murturi, "Edge and Fog Computing: Vision and Research Challenges," *IEEE Internet Computing*, vol. 23, no. 2, pp. 17-26, Mar./Apr. 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8705869. Accessed: July 1, 2024

[43] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential Privacy in Blockchain Technology: A Futuristic Approach," arXiv, 2019. [Online]. Available: https://arxiv.org/pdf/1910.04316. [Accessed: June. 1, 2024].

[44] S. D. Kotey, E. T. Tchao, A.-R. Ahmed, A. S. Agbemenu, H. Nunoo-Mensah, A. Sikora, D. Welte, and E. Keelson, "Blockchain interoperability: The state of heterogeneous blockchain-to-blockchain communication," *IET Communications*, vol. 17, no. 8, pp. 891-914, 2023.

[45] Ducas, L., Durmus, A., Lepoint, T., & Lyubashevsky, V. (2013). BLISS: Bimodal Lattice Signature Schemes. In *Proceedings of the 20th ACM Conference on Computer and Communications Security (CCS '13)* (pp. 305-316). New York, NY, USA: Association for Computing Machinery. doi:10.1145/2508859.2516700.