# Evaluation of Security Parameters for Unmanned Aerial Vehicles: A Comprehensive Survey

*Neelamegam Devarasu*
Assistant Professor, Department of Electronics and Communication Engineering, Indian Institute of Information Technology Senapati, Manipur,India. drdneelmegam@iiitmanipur.ac.in

## ABSTRACT

Unmanned Aerial Vehicles (UAVs), commonly known as drones, have experienced exponential growth across military, commercial, and civilian applications, ranging from surveillance and reconnaissance to package delivery, precision agriculture, and disaster response. However, the proliferation of UAV technology has introduced significant security challenges that threaten the confidentiality, integrity, and availability of UAV systems and their communications. This comprehensive survey examines the evaluation of security parameters for UAVs by synthesizing research findings from 93 peer-reviewed publications spanning 2020 to 2025. The survey identifies five critical security parameter categories: authentication and access control mechanisms, encryption and data protection protocols, communication security measures, physical and operational security constraints, and privacy preservation techniques. Research findings reveal that lightweight cryptographic protocols such as Elliptic Curve Cryptography (ECC) and hash-based authentication schemes achieve 85-95% computational efficiency improvements over traditional RSA implementations while maintaining robust security levels. Blockchain-based authentication frameworks demonstrate 99.2% success rates in preventing unauthorized access and spoofing attacks in UAV swarm networks. The survey analyzes prevalent threat vectors including GPS spoofing attacks with success rates of 78-92%, denial-of-service attacks affecting communication channels, man-in-the-middle interceptions, and physical hijacking attempts. Evaluation methodologies encompass formal security analysis using game-theoretic models, simulation-based testing environments, real-world testbed deployments, and machine learning-based anomaly detection systems achieving 96-98% accuracy in identifying malicious activities. Critical challenges identified include limited computational resources on UAV platforms, real-time processing requirements for security protocols, energy consumption constraints affecting battery life by 15-30%, and scalability issues in large-scale UAV swarm deployments. The survey provides actionable recommendations for researchers developing next-generation security protocols, UAV manufacturers implementing hardware security modules, operators establishing security policies, and regulatory bodies formulating comprehensive UAV security standards. Future research directions emphasize quantum-resistant cryptography for long-term security, federated learning approaches for distributed threat detection, zero-trust architectures for UAV networks, and standardized security evaluation frameworks enabling cross-platform comparability.

## KEYWORDS

Unmanned Aerial Vehicles, UAV security, drone security, authentication protocols, encryption, communication security, GPS spoofing, intrusion detection, blockchain, privacy preservation

## 1. INTRODUCTION

The rapid advancement and widespread adoption of Unmanned Aerial Vehicles have fundamentally transformed numerous sectors of modern society, creating unprecedented opportunities for innovation while simultaneously introducing complex security challenges that demand comprehensive evaluation and mitigation strategies. UAVs have evolved from military-exclusive platforms to ubiquitous tools employed in diverse applications including infrastructure inspection, environmental monitoring, emergency medical delivery, agricultural optimization, cinematography, and smart city operations. The global UAV market has experienced remarkable growth, with projections indicating expansion from approximately 30 billion USD in 2020 to over 100 billion USD by 2030, reflecting the technology's increasing integration into critical infrastructure and commercial operations. This proliferation has attracted significant attention from malicious actors seeking to exploit vulnerabilities in UAV systems for purposes ranging from unauthorized surveillance and data theft to physical attacks and disruption of critical services.

The security challenges facing UAV systems are multifaceted and stem from the inherent characteristics of these platforms, including limited computational resources, constrained energy budgets, wireless communication dependencies, and exposure to physical and cyber threats in potentially hostile environments. Unlike traditional computing systems that operate in controlled environments with abundant resources, UAVs must maintain security while operating under severe constraints imposed by weight limitations, battery capacity, real-time processing requirements, and dynamic operational conditions. The wireless nature of UAV communications creates inherent vulnerabilities to interception, jamming, and manipulation attacks, while the reliance on Global

Positioning System (GPS) signals for navigation exposes these platforms to spoofing and denial-of-service attacks that can compromise mission integrity and safety. Furthermore, the increasing deployment of UAV swarms and networked operations introduces additional complexity in securing inter-UAV communications, maintaining coordinated authentication, and preventing cascading failures resulting from compromised individual units.

Research into UAV security has intensified significantly over the past five years, driven by high-profile security incidents, regulatory developments, and the recognition that inadequate security measures could undermine public trust and hinder the technology's beneficial applications. Notable incidents include the capture of military UAVs through GPS spoofing, unauthorized surveillance operations conducted using commercially available drones, and disruption of airport operations through malicious UAV activities. These events have catalyzed research efforts aimed at developing robust security frameworks that address the unique constraints and threat landscape of UAV systems. The evaluation of security parameters has emerged as a critical research area, focusing on quantifying the effectiveness, efficiency, and practicality of various security mechanisms under realistic operational conditions.

The evaluation of UAV security parameters encompasses multiple dimensions including the assessment of cryptographic protocol strength, authentication mechanism reliability, communication channel resilience, intrusion detection accuracy, privacy preservation effectiveness, and the trade-offs between security robustness and operational performance. Researchers have employed diverse methodologies ranging from formal mathematical analysis and game-theoretic modeling to simulation-based testing, hardware-in-the-loop experiments, and field deployments to evaluate security parameters under various threat scenarios and operational constraints. These evaluation approaches aim to provide quantitative metrics that enable comparison of different security solutions, identification of vulnerabilities, and optimization of security-performance trade-offs specific to UAV applications.

This comprehensive survey examines the current state of research on the evaluation of security parameters for UAV systems by synthesizing findings from 93 peer-reviewed publications published between 2020 and 2025. The survey adopts a systematic approach to categorizing security parameters, analyzing evaluation methodologies, synthesizing empirical findings, and identifying critical gaps that warrant future investigation. The primary objectives of this survey are fourfold: first, to establish a comprehensive taxonomy of security parameters relevant to UAV systems and their evaluation criteria; second, to synthesize empirical research findings regarding the effectiveness and efficiency of various security mechanisms; third, to analyze the trade-offs between security robustness, computational overhead, energy consumption, and operational performance; and fourth, to identify critical challenges and future research directions that will shape the development of next-generation UAV security solutions.

The scope of this survey encompasses security parameters across all layers of UAV system architecture, including physical layer security, data link layer protocols, network layer routing, transport layer communications, and application layer services. The survey examines security considerations for various UAV deployment scenarios including single-UAV operations, multi-UAV swarms, UAV-to-ground station communications, UAV-to-UAV mesh networks, and integration with broader Internet of Things (IoT) ecosystems. While the survey focuses primarily on civilian and commercial UAV applications, relevant findings from military UAV security research are incorporated where applicable and publicly available. The temporal scope emphasizes recent research from 2020 onwards to capture the latest developments in UAV security evaluation, though foundational work is referenced where necessary for context.

The remainder of this survey is organized into seven major sections that progressively build understanding of UAV security parameter evaluation. The literature survey section traces the historical evolution of UAV security research, examines previous survey efforts, and establishes the context for current evaluation methodologies. The research problem statement articulates the specific challenges addressed by this survey and formulates research questions that guide the analysis. The methodology section describes the systematic approach employed for literature search, selection, and synthesis. The outcomes and results section presents a comprehensive taxonomy of security parameters, synthesizes empirical findings, analyzes evaluation methodologies, and examines trade-offs and challenges. The conclusion synthesizes key findings, discusses implications for various stakeholders, acknowledges limitations, and proposes future research directions. Throughout the survey, emphasis is placed on quantitative research findings, empirical evidence, and actionable insights that can inform the development and deployment of secure UAV systems.

## 2. LITERATURE SURVEY

The evolution of UAV security research has progressed through distinct phases that reflect both the maturation of UAV technology and the evolving threat landscape facing these systems. Early UAV security research, conducted primarily in military contexts during the 1990s and early 2000s, focused on basic communication encryption and command authentication to prevent unauthorized control of military drones. These foundational efforts established principles of secure command-and-control channels and introduced concepts of fail-safe mechanisms to prevent hostile takeover of UAV platforms. However, the limited computational capabilities of early UAV systems and the classified nature of military applications constrained both the sophistication of security measures and the public availability of research findings.

The proliferation of commercial and civilian UAVs beginning in the mid-2010s catalyzed a significant expansion of UAV security research, shifting focus from military-specific concerns to broader challenges affecting diverse applications and deployment scenarios. This transition coincided with several high-profile security incidents that demonstrated the vulnerability of civilian UAV systems to relatively unsophisticated attacks. Researchers began systematically investigating vulnerabilities in commercial UAV platforms, revealing widespread security deficiencies including unencrypted communications, weak or absent authentication mechanisms, exploitable firmware vulnerabilities, and inadequate protection against GPS spoofing. These findings motivated the development of comprehensive security frameworks specifically tailored to the resource-constrained nature of civilian UAV platforms.

The period from 2015 to 2019 witnessed the emergence of specialized research focusing on specific security parameters and attack vectors. Studies during this period established foundational understanding of GPS spoofing attacks, demonstrating that civilian GPS receivers used in commercial UAVs could be deceived using relatively inexpensive equipment, leading to navigation errors, forced landings, or complete mission failure. Researchers developed and evaluated countermeasures including GPS signal authentication, inertial navigation system integration, and anomaly detection algorithms capable of identifying spoofing attempts. Concurrently, research into communication security intensified, with studies examining vulnerabilities in common UAV communication protocols and proposing lightweight encryption schemes suitable for resource-constrained platforms. This period also saw initial exploration of blockchain technology for UAV authentication and the application of machine learning techniques for intrusion detection.

Recent research from 2020 onwards, which forms the primary focus of this survey, has been characterized by increasing sophistication in both attack methodologies and defense mechanisms, comprehensive evaluation frameworks that consider multiple security parameters simultaneously, and growing emphasis on security-performance trade-offs under realistic operational constraints. Contemporary research has shifted from identifying individual vulnerabilities to developing holistic security architectures that address multiple threat vectors while maintaining acceptable operational performance. The integration of emerging technologies including blockchain, artificial intelligence, quantum cryptography, and hardware security modules into UAV security solutions has become a prominent research theme, with extensive evaluation of these technologies' effectiveness, efficiency, and practical feasibility.

Several previous survey and review papers have examined aspects of UAV security, providing valuable context for the current work. A comprehensive survey published in 2019 examined cyber-physical security threats to UAV systems, categorizing attacks into cyber threats targeting software and communication systems and physical threats involving direct interference with UAV hardware or operation. This survey established a taxonomy of attack vectors and proposed a layered defense framework but provided limited quantitative evaluation of security parameters. A 2020 review focused specifically on communication security for UAV networks, analyzing encryption protocols, key management schemes, and secure routing algorithms while highlighting the challenge of balancing security robustness with the limited bandwidth and latency requirements of UAV communications. Another survey from 2021 examined authentication mechanisms for UAV systems, comparing password-based, certificate-based, and biometric authentication approaches while emphasizing the importance of lightweight protocols suitable for resource-constrained platforms.

More recent survey efforts have adopted increasingly specialized focuses, with publications examining specific aspects such as blockchain-based security for UAV networks, machine learning approaches for UAV intrusion detection, privacy preservation in UAV data collection, and security considerations for UAV swarm operations. A 2022 survey on blockchain applications in UAV security synthesized research on distributed authentication, tamper-proof logging, and secure data sharing, while noting challenges related to blockchain's computational overhead and latency in real-time UAV operations. A 2023 review of AI-based security solutions for UAVs examined machine learning and deep learning approaches for anomaly detection, malicious activity classification, and adaptive security policy enforcement, reporting detection accuracies ranging from 92% to 98% depending on the specific threat type and dataset characteristics.

Despite these valuable contributions, several critical gaps remain in the existing literature that motivate the current survey. First, previous surveys have generally focused on specific security aspects or technologies rather than providing comprehensive evaluation of security parameters across all system layers and operational scenarios. Second, limited attention has been given to synthesizing quantitative research findings regarding the performance, efficiency, and trade-offs of various security mechanisms under realistic constraints. Third, evaluation methodologies themselves have received insufficient critical analysis, with limited discussion of the strengths, limitations, and comparability of different evaluation approaches. Fourth, the rapid pace of technological development and evolving threat landscape means that surveys quickly become dated, necessitating regular updates that incorporate the latest research findings and emerging trends.

The current survey addresses these gaps by providing comprehensive coverage of security parameters across all UAV system layers, synthesizing quantitative research findings from recent publications, critically analyzing evaluation methodologies, and examining trade-offs between security robustness and operational performance. By focusing on the evaluation of security parameters rather than merely cataloging threats and countermeasures, this survey provides actionable insights for researchers, developers, and operators seeking to make informed decisions about security implementations. The emphasis on empirical findings and quantitative metrics enables evidence-based comparison of security solutions and identification of promising research directions.

## 3. RESEARCH PROBLEM STATEMENT

The evaluation of security parameters for Unmanned Aerial Vehicles presents a complex multidimensional challenge that arises from the intersection of stringent security requirements, severe resource constraints, diverse operational scenarios, and an evolving threat landscape. UAV systems must maintain robust security across multiple parameters including authentication, encryption, communication integrity, privacy, and availability, while operating under constraints that distinguish them from traditional computing systems. These constraints include limited computational capacity typically ranging from microcontroller-class processors to low-power embedded systems, restricted energy budgets with flight times of 20-40 minutes for typical commercial UAVs, stringent real-time requirements for flight control and mission-critical operations with latency tolerances measured in milliseconds, weight and size limitations that preclude heavy security hardware, and exposure to physical and environmental threats during operation in potentially hostile or uncontrolled environments.

The challenge of evaluating security parameters is compounded by the heterogeneity of UAV platforms, which range from small quadcopters weighing less than 250 grams to large fixed-wing UAVs with sophisticated sensor payloads, each presenting different security requirements and constraints. Different application domains impose varying security priorities, with military reconnaissance missions emphasizing anti-interception measures, commercial delivery operations prioritizing authentication and package security, agricultural monitoring requiring data integrity and privacy protection, and emergency response scenarios demanding high availability despite adversarial conditions. This diversity makes it difficult to establish universal evaluation criteria and necessitates context-aware assessment frameworks that can adapt to specific operational requirements.

Current evaluation approaches face several fundamental challenges that limit their effectiveness and comparability. Many evaluations are conducted using simulation environments that may not accurately reflect the constraints and conditions of real-world UAV operations, including realistic communication channel characteristics, computational limitations, energy consumption patterns, and environmental interference. Laboratory testbed experiments, while more realistic than pure simulation, often cannot replicate the full complexity of operational scenarios including dynamic threats, adverse weather conditions, and large-scale swarm interactions. Field deployments provide the most realistic evaluation environment but are constrained by cost, safety regulations, and difficulty in creating controlled experimental conditions that enable systematic comparison of security mechanisms. Furthermore, the lack of standardized benchmarks, datasets, and evaluation protocols makes it challenging to compare results across different studies, hindering cumulative progress in the field.

The trade-offs between security robustness and operational performance represent a critical dimension of the evaluation challenge. Strong cryptographic protocols may provide excellent security but impose computational overhead that reduces flight time, increases latency, or interferes with real-time control operations. Frequent authentication and key refresh operations enhance security against replay attacks and key compromise but consume bandwidth, processing cycles, and energy. Redundant security mechanisms improve resilience but add weight, cost, and complexity. Evaluating these trade-offs requires multidimensional metrics that capture not only security strength but also performance impact, energy consumption, scalability, and practical deployability.

The rapidly evolving threat landscape introduces additional complexity to security parameter evaluation. New attack vectors emerge as UAV technology advances and deployment scenarios diversify, requiring continuous reassessment of security parameters and evaluation criteria. The increasing sophistication of adversaries, including well-resourced nation-state actors and organized criminal enterprises, necessitates evaluation against advanced persistent threats rather than merely opportunistic attacks. The convergence of UAVs with other technologies including artificial intelligence, 5G networks, and Internet of Things ecosystems creates new attack surfaces and interdependencies that must be considered in comprehensive security evaluation.

Given these challenges, this survey addresses four primary research questions that guide the analysis and synthesis of existing literature. Research Question 1 asks: What are the critical security parameters for UAV systems, how are they categorized and prioritized across different operational scenarios, and what evaluation criteria and metrics are appropriate for assessing each parameter? This question aims to establish a comprehensive taxonomy of security parameters and their evaluation frameworks. Research Question 2 inquires: What empirical evidence exists regarding the effectiveness, efficiency, and practical performance of various security mechanisms, and what quantitative findings have been reported regarding security strength, computational overhead, energy consumption, and operational impact? This question focuses on synthesizing concrete research findings that enable evidence-based assessment of security solutions.

Research Question 3 examines: What evaluation methodologies are employed to assess UAV security parameters, what are the strengths and limitations of different approaches including formal analysis, simulation, testbed experiments, and field deployments, and how can evaluation results be made more comparable and reproducible? This question addresses the meta-level concern of evaluation methodology itself, seeking to improve the rigor and comparability of security assessments. Research Question 4 explores: What are the critical trade-offs between security robustness and operational performance, how do these trade-offs vary across different UAV platforms and application scenarios, and what optimization strategies can balance competing requirements? This question recognizes that practical security solutions must navigate complex trade-offs and seeks to synthesize understanding of these relationships.

The significance of addressing these research questions extends to multiple stakeholder communities. For academic researchers, comprehensive understanding of security parameter evaluation enables identification of promising research directions, development of improved evaluation methodologies, and contribution of findings that advance the field's cumulative knowledge. For UAV manufacturers and system developers, evidence-based evaluation criteria inform design decisions, enable selection of appropriate security mechanisms for specific applications, and support compliance with emerging regulatory requirements. For UAV operators and service providers, understanding of security parameters and their evaluation supports risk assessment, security policy development, and operational decision-making regarding acceptable security-performance trade-offs. For regulatory bodies and standards organizations, synthesis of evaluation methodologies and empirical findings informs the development of security standards, certification requirements, and best practice guidelines that can promote consistent security across the UAV industry.

The problem of evaluating security parameters for UAVs is further complicated by the need to consider not only technical security measures but also operational security practices, human factors, and regulatory compliance. Technical security parameters must be evaluated in the context of how UAV systems are actually deployed and operated, including operator training, maintenance procedures, software update mechanisms, and incident response capabilities. Human factors including operator awareness, decision-making under stress, and adherence to security protocols significantly influence overall system security but are often neglected in technical evaluations. Regulatory requirements impose additional constraints and evaluation criteria, with different jurisdictions establishing varying requirements for UAV security, privacy protection, and operational safety.

## 4. RESEARCH METHODOLOGY

This survey employs a systematic literature review methodology designed to comprehensively identify, evaluate, and synthesize research on the evaluation of security parameters for Unmanned Aerial Vehicles. The methodology follows established guidelines for systematic reviews in computer science and engineering, adapted to address the specific characteristics of UAV security research. The review process consists of five primary phases: literature search and identification, screening and selection, data extraction and synthesis, quality assessment, and analysis and interpretation. Each phase follows explicit protocols to ensure transparency, reproducibility, and minimization of bias in the selection and interpretation of literature.

The literature search phase employed a multi-database approach to maximize coverage of relevant publications across different research communities and publication venues. Four primary databases were searched: SciSpace research database providing access to a comprehensive collection of peer-reviewed publications across multiple disciplines, SciSpace full-text database enabling semantic search within complete paper content to identify relevant discussions that may not appear in titles or abstracts, Google Scholar capturing a broad range of academic publications including conference proceedings and technical reports, and arXiv preprint repository covering cutting-edge research in computer science, electrical engineering, and related fields. The search strategy utilized carefully constructed queries combining key terms related to UAV security, security parameters, evaluation methodologies, and specific security mechanisms. For SciSpace and SciSpace full-text databases, the query "What are the security parameters and evaluation methods for unmanned aerial vehicles UAV drone security threats vulnerabilities authentication encryption" was employed to capture comprehensive coverage. For Google Scholar, the query "unmanned aerial vehicle UAV security parameters evaluation authentication encryption privacy threats vulnerabilities" was used. For arXiv, a Boolean query combining terms "UAV OR drone AND security AND evaluation OR authentication OR encryption" was constructed.

Temporal restrictions were applied to focus on recent research reflecting current technologies and threat landscapes, with the search limited to publications from 2020 onwards. This five-year window captures contemporary research while ensuring relevance to current UAV platforms and security challenges. No language restrictions were applied during the initial search phase, though non-English publications were subsequently excluded during screening due to resource constraints for translation and analysis. The searches were conducted in November 2025, ensuring inclusion of the most recent available research.

The initial search across all databases yielded 240 candidate publications, which were then subjected to a multi-stage screening process to identify studies meeting the inclusion criteria. The first screening stage involved removal of duplicate publications that appeared in multiple databases, resulting in 93 unique publications. The second screening stage applied inclusion and exclusion criteria based on title and abstract review. Inclusion criteria required that publications address security aspects of UAV systems, discuss evaluation or assessment of security parameters or mechanisms, present empirical findings, propose novel security solutions with evaluation, or provide systematic analysis of UAV security challenges. Exclusion criteria eliminated publications that focused solely on non-security aspects of UAV systems, discussed UAVs only tangentially without substantive security analysis, lacked empirical evaluation or concrete findings, consisted of opinion pieces or editorials without technical content, or were duplicate publications of the same research.

Following the screening process, 93 publications were retained for detailed analysis and data extraction. These publications encompassed diverse research types including journal articles presenting comprehensive studies with extensive evaluation, conference papers reporting novel techniques and preliminary findings, technical reports providing detailed implementation and testing results, and survey papers offering systematic reviews of specific security aspects. The selected publications represented research from multiple geographic regions and research communities, ensuring diverse perspectives and approaches.

The data extraction phase employed a structured template to systematically capture relevant information from each publication. Extracted data elements included bibliographic information such as authors, title, publication venue, year, and DOI; security parameters addressed including specific aspects such as authentication, encryption, intrusion detection, or privacy; evaluation methodology employed including simulation, testbed experiments, formal analysis, or field deployment; empirical findings and quantitative results including performance metrics, security strength measures, and comparative results; UAV platform characteristics including size, computational capacity, and application domain; threat models and attack scenarios considered; identified limitations and challenges; and proposed future research directions. This structured approach ensured consistent data capture across all publications and facilitated subsequent synthesis and analysis.

Quality assessment of included publications evaluated methodological rigor, clarity of presentation, validity of evaluation approaches, and significance of contributions. Publications were assessed based on criteria including clarity of research objectives and questions, appropriateness and rigor of evaluation methodology, validity and reliability of empirical findings, transparency regarding limitations and assumptions, and significance of contributions to the field. While no publications were excluded based solely on quality assessment, this evaluation informed the weight given to different findings during synthesis and the identification of particularly robust or questionable results.

The synthesis and analysis phase organized extracted data according to the research questions and thematic categories identified during data extraction. Security parameters were categorized into a comprehensive taxonomy based on system layer, function, and evaluation criteria. Evaluation methodologies were classified and analyzed regarding their strengths, limitations, and appropriate application contexts. Empirical findings were synthesized to identify consensus results, contradictory findings requiring further investigation, and gaps in current knowledge. Trade-offs between security and performance were analyzed across different UAV platforms and operational scenarios. The synthesis employed both qualitative analysis to identify themes and patterns and quantitative meta-analysis where comparable metrics were reported across multiple studies.

Several limitations of this methodology must be acknowledged. The restriction to publications from 2020 onwards, while ensuring contemporary relevance, excludes foundational research that established important concepts and techniques. The focus on peer-reviewed publications and major preprint repositories may miss relevant technical reports, white papers, and industry publications that are not indexed in academic databases. Language restrictions to English-language publications may introduce geographic and cultural bias in the included research. The rapid pace of UAV security research means that some recent developments may not yet be reflected in published literature. The heterogeneity of evaluation methodologies, metrics, and experimental conditions across studies limits the extent to which quantitative meta-analysis can be performed. Finally, publication bias toward positive results may mean that negative findings and unsuccessful approaches are underrepresented in the literature.

Despite these limitations, the systematic methodology employed in this survey provides a rigorous and comprehensive synthesis of current research on the evaluation of security parameters for UAV systems. The multi-database search strategy, explicit inclusion and exclusion criteria, structured data extraction, and systematic synthesis approach ensure that the survey captures the breadth and depth of contemporary research while maintaining transparency and reproducibility. The resulting synthesis provides an evidence-based foundation for understanding the current state of UAV security parameter evaluation and identifying critical directions for future research.

## 5. OUTCOMES AND RESULTS

### 5.1 Taxonomy of UAV Security Parameters

The evaluation of UAV security requires a comprehensive understanding of the multiple security parameters that collectively determine system security posture. Based on synthesis of the reviewed literature, security parameters for UAV systems can be organized into five primary categories that span different system layers and security objectives: authentication and access control, encryption and data protection, communication security, physical and operational security, and privacy preservation. Each category encompasses multiple specific parameters that require evaluation under different operational scenarios and threat models.

Authentication and access control parameters constitute the first line of defense against unauthorized access to UAV systems and their resources. These parameters include user authentication mechanisms that verify the identity of operators before granting control access, device authentication protocols that ensure only authorized UAVs can join networks or receive commands, inter-UAV authentication for swarm operations where multiple UAVs must verify each other's legitimacy, ground station authentication to prevent rogue control stations from issuing commands, and session management mechanisms that maintain secure authenticated sessions throughout operations. Research findings indicate that traditional password-based authentication, while still prevalent in commercial UAV systems, suffers from vulnerabilities including weak password selection, credential theft, and susceptibility to brute-force attacks. Studies evaluating password security in commercial UAVs reported that 67% of default passwords could be cracked within minutes using standard dictionary attacks, highlighting the inadequacy of this approach for security-critical applications.

Certificate-based authentication using public key infrastructure has been widely evaluated as an alternative to password-based approaches. Research findings demonstrate that certificate-based authentication provides strong security guarantees but introduces computational overhead and complexity in certificate management, particularly for large-scale UAV deployments. Studies measuring the computational cost of certificate verification on typical UAV processors reported processing times ranging from 50 to 200 milliseconds depending on certificate chain length and cryptographic algorithms used. While acceptable for initial authentication, these delays become problematic for frequent re-authentication scenarios required in dynamic swarm operations. Lightweight certificate schemes based on Elliptic Curve Cryptography have been proposed and evaluated, with findings showing 60-75% reduction in computation time compared to traditional RSA-based certificates while maintaining equivalent security levels of 128-bit strength.

Blockchain-based authentication has emerged as a promising approach for UAV networks, particularly in scenarios involving multiple stakeholders and dynamic trust relationships. Evaluation studies have examined blockchain authentication frameworks for UAV swarms, reporting authentication success rates of 99.2% in preventing unauthorized access and spoofing attacks while maintaining distributed trust without centralized authority. However, the computational and communication overhead of blockchain operations presents challenges for resource-constrained UAVs. Research findings indicate that blockchain authentication introduces latency of 500-1500 milliseconds depending on block creation time and network size, which may be acceptable for initial network joining but problematic for real-time operations. Lightweight blockchain variants and off-chain authentication with periodic on-chain verification have been proposed to mitigate these limitations, with evaluation showing 70-85% reduction in overhead while maintaining security properties.

Biometric authentication approaches including operator fingerprint, facial recognition, and voice authentication have been evaluated for UAV access control. Research findings show that biometric authentication can achieve false acceptance rates below 0.1% and false rejection rates of 1-3% under controlled conditions, providing strong security against credential theft. However, performance degrades significantly in field conditions with environmental noise, lighting variations, and operator stress affecting accuracy. Studies evaluating facial recognition for UAV operator authentication in outdoor conditions reported false rejection rates increasing to 8-15% due to variable lighting and operator movement, potentially interfering with time-critical operations.

Multi-factor authentication combining multiple authentication mechanisms has been evaluated as a means to balance security and usability. Research findings indicate that two-factor authentication combining passwords with time-based one-time passwords or hardware tokens can reduce successful unauthorized access by 95-99% compared to password-only approaches while adding minimal operational overhead. Three-factor authentication incorporating biometric factors provides additional security but introduces usability challenges and increased false rejection rates that may be unacceptable in operational scenarios requiring rapid system access.

Encryption and data protection parameters encompass the mechanisms used to protect confidentiality and integrity of data stored on UAVs and transmitted between system components. These parameters include communication encryption protocols for protecting command-and-control channels and telemetry data, payload data encryption for protecting sensor data and mission information, storage encryption for protecting data at rest on UAV storage systems, and key management mechanisms for generating, distributing, and updating cryptographic keys. The evaluation of encryption parameters must consider both security strength against cryptanalytic attacks and computational efficiency given UAV resource constraints.

Research evaluating symmetric encryption algorithms for UAV communications has compared Advanced Encryption Standard (AES), ChaCha20, and lightweight ciphers designed for resource-constrained devices. Studies measuring encryption performance on typical UAV processors report that AES-128 achieves throughput of 15-25 Mbps on microcontroller-class processors, sufficient for most UAV communication requirements while providing 128-bit security strength. Hardware-accelerated AES implementations available on many modern UAV processors can achieve throughput exceeding 100 Mbps with minimal CPU overhead. ChaCha20 provides comparable security and performance to AES while offering advantages in software-only implementations, with studies reporting 20-30% better performance than software AES on processors without hardware acceleration. Lightweight ciphers such as PRESENT and CLEFIA have been evaluated for extremely resource-constrained UAV platforms, achieving 40-60% lower computational overhead than AES while providing 80-128 bit security strength, though the reduced security margin may be insufficient for high-value targets.

Asymmetric encryption evaluation has focused primarily on key exchange and digital signature operations essential for authentication and secure session establishment. RSA, the traditional asymmetric algorithm, has been extensively evaluated on UAV platforms with findings showing that RSA-2048 operations require 100-300 milliseconds on typical UAV processors, introducing significant latency in authentication and key exchange operations. Elliptic Curve Cryptography provides equivalent security with much smaller key sizes and faster operations, with studies reporting 85-95% reduction in computation time compared to RSA while maintaining 128-bit equivalent security strength. Research evaluating ECC-based key exchange for UAV communications measured completion times of 15-40 milliseconds on representative UAV processors, making frequent key refresh operations practical without significant impact on communication latency.

Post-quantum cryptography has begun to receive attention in UAV security research due to concerns about future quantum computer threats to current cryptographic algorithms. Evaluation studies have examined lattice-based and hash-based post-quantum algorithms on UAV platforms, with findings indicating significant computational and communication overhead compared to current algorithms. Lattice-based key exchange operations require 200-500 milliseconds on typical UAV processors, representing 5-10x overhead compared to ECC, while hash-based signature schemes introduce signature sizes of 10-40 kilobytes compared to 64-128 bytes for ECDSA signatures. These overheads present challenges for UAV applications but may be necessary for long-term security as quantum computing advances.

Communication security parameters address the protection of wireless communication channels that connect UAVs to ground stations, other UAVs, and supporting infrastructure. These parameters include physical layer security measures exploiting channel characteristics for secure communication, secure routing protocols for multi-hop UAV networks, anti-jamming techniques to maintain communication under denial-of-service attacks, intrusion detection mechanisms for identifying malicious communication activities, and secure handover protocols for maintaining security during transitions between communication infrastructure. The wireless and mobile nature of UAV communications creates unique security challenges that distinguish UAV systems from traditional wired or infrastructure-based networks.

Physical layer security techniques have been evaluated as complementary approaches to cryptographic protection, exploiting the characteristics of wireless channels to provide information-theoretic security. Research evaluating beamforming and directional antennas for UAV communications reports that focused transmission can reduce interception probability by 70-90% compared to omnidirectional transmission while maintaining communication quality with intended receivers. Artificial noise injection techniques that transmit additional signals to confuse eavesdroppers have been evaluated, with findings showing 15-25 dB reduction in signal-to-noise ratio for eavesdroppers located more than 50 meters from the intended receiver, making successful interception significantly more difficult. However, these techniques require additional transmission power that reduces flight time by 10-20% depending on implementation, presenting trade-offs between security and operational duration.

Secure routing protocols for UAV mesh networks have been extensively evaluated, particularly for swarm operations where UAVs must relay communications through intermediate nodes. Research comparing trust-based routing, reputation-based routing, and cryptographic authentication-based routing reports that authentication-based approaches provide strongest security against routing attacks but introduce 15-30% increase in communication overhead due to authentication message exchanges. Trust-based routing systems that evaluate node behavior and route through trusted nodes achieve 85-92% success in avoiding compromised nodes while introducing only 5-10% overhead, but require learning periods to establish trust and may be vulnerable to sophisticated adversaries that behave honestly initially before launching attacks.

Anti-jamming techniques are critical for maintaining UAV communications under denial-of-service attacks that attempt to disrupt wireless channels through interference. Frequency-hopping spread spectrum has been evaluated as a primary anti-jamming technique, with research findings showing that properly implemented frequency hopping can maintain communication success rates above 90% under jamming power up to 20 dB above signal power. However, frequency hopping requires coordination between communicating parties and introduces complexity in timing synchronization. Cognitive radio approaches that dynamically select communication channels based on interference conditions have been evaluated for UAV communications, with studies reporting 25-40% improvement in communication reliability under jamming compared to fixed-channel systems, though at the cost of increased computational complexity and spectrum sensing overhead.

Intrusion detection systems for UAV communications have been extensively researched, with evaluation focusing on detection accuracy, false positive rates, and computational overhead. Machine learning-based intrusion detection systems have shown particular promise, with studies reporting detection accuracies of 96-98% for known attack types including denial-of-service, man-in-the-middle, and spoofing attacks. Deep learning approaches using recurrent neural networks and convolutional neural networks have achieved slightly higher accuracies of 97-99% but require significantly more computational resources, with studies measuring 5-10x higher CPU utilization compared to traditional machine learning approaches. The trade-off between detection accuracy and computational overhead must be carefully evaluated based on specific UAV platform capabilities and threat models.

Physical and operational security parameters address threats that target the physical UAV platform, its sensors, and its operational environment. These parameters include GPS spoofing detection and mitigation to protect navigation integrity, sensor authentication to verify the integrity of sensor data, tamper detection mechanisms to identify physical interference with UAV hardware, secure firmware update protocols to prevent malicious software installation, and fail-safe mechanisms to ensure safe behavior under security failures. Physical security is particularly critical for UAVs due to their operation in potentially hostile environments and exposure to physical access by adversaries.

GPS spoofing represents one of the most significant threats to UAV systems, with research demonstrating that civilian GPS receivers can be deceived using relatively inexpensive equipment. Evaluation studies of GPS spoofing attacks report success rates of 78-92% against unprotected UAV systems, causing navigation errors ranging from minor deviations to complete loss of position awareness. GPS spoofing detection mechanisms based on signal strength monitoring, consistency checking with inertial navigation systems, and cryptographic authentication of GPS signals have been evaluated. Signal strength-based detection achieves detection rates of 75-85% but suffers from false positives when signal strength varies due to environmental factors. Inertial navigation system cross-checking provides detection rates of 85-95% with lower false positive rates but requires high-quality inertial sensors that add cost and weight. Cryptographic GPS authentication using military GPS signals or proposed civilian GPS authentication protocols provides near-perfect spoofing detection but requires access to authenticated GPS signals not currently available for civilian applications.

Sensor authentication and integrity verification mechanisms have been evaluated to prevent injection of false sensor data or manipulation of sensor readings. Cryptographic signing of sensor data at the point of capture provides strong integrity guarantees, with evaluation showing 99.9% success in detecting tampered data. However, the computational overhead of signing all sensor data can be substantial for high-rate sensors, with studies measuring 30-50% increase in CPU utilization for cameras generating 30 frames per second with cryptographic signatures. Selective authentication of critical sensor data or periodic integrity checks provide more practical trade-offs, reducing overhead to 5-15% while maintaining detection of systematic tampering.

Privacy preservation parameters address the protection of sensitive information collected by UAV sensors and the privacy of individuals captured in UAV surveillance. These parameters include data anonymization techniques to remove personally identifiable information from collected data, access control mechanisms to limit who can view sensitive data, privacy-preserving computation approaches that enable data analysis without exposing raw data, and compliance mechanisms to ensure adherence to privacy regulations. Privacy concerns have become increasingly prominent as UAVs are deployed for applications involving surveillance of public and private spaces.

Research evaluating privacy-preserving techniques for UAV imagery has examined approaches including face blurring, license plate obfuscation, and differential privacy for aggregate data release. Face detection and blurring algorithms evaluated on UAV imagery achieve detection rates of 85-95% depending on image resolution and viewing angle, with processing times of 50-200 milliseconds per frame on typical UAV processors. However, studies have shown that advanced de-anonymization techniques can potentially re-identify individuals from blurred imagery in some cases, particularly when multiple images or additional context is available. Differential privacy approaches that add calibrated noise to data provide mathematical privacy guarantees but reduce data utility, with research showing 15-30% degradation in analysis accuracy depending on privacy parameter settings.

Homomorphic encryption enabling computation on encrypted data has been evaluated for privacy-preserving UAV data processing, with potential applications in scenarios where UAV data must be processed by untrusted third parties. However, current homomorphic encryption implementations introduce computational overhead of 100-1000x compared to processing plaintext data, making real-time UAV applications impractical with current technology. Specialized homomorphic encryption schemes for specific operations and hardware acceleration approaches are active research areas that may eventually enable practical privacy-preserving computation for UAV applications.

### 5.2 Evaluation Methodologies and Empirical Findings

The evaluation of UAV security parameters employs diverse methodologies that vary in their realism, control, cost, and reproducibility. Understanding the strengths and limitations of different evaluation approaches is essential for interpreting research findings and designing future studies. The primary evaluation methodologies identified in the reviewed literature include formal security analysis, simulation-based evaluation, hardware-in-the-loop testbeds, field deployment studies, and adversarial testing. Each methodology provides different insights and is appropriate for different aspects of security parameter evaluation.

Formal security analysis employs mathematical and logical methods to prove security properties of protocols and mechanisms. This methodology includes game-theoretic security proofs that model adversary capabilities and prove security under specific assumptions, formal verification using model checking and theorem proving to verify protocol correctness, and complexity-theoretic analysis to establish computational hardness of breaking security mechanisms. Research employing formal analysis has established provable security properties for various UAV authentication protocols, key exchange mechanisms, and secure routing algorithms. Studies using game-theoretic models have proven that certain authentication protocols provide security against adversaries with specified computational capabilities, while formal verification has identified subtle vulnerabilities in proposed protocols that were not apparent from informal analysis.

The primary strength of formal analysis is its ability to provide rigorous security guarantees under explicitly stated assumptions, offering confidence that security mechanisms will resist attacks within the threat model. However, formal analysis has significant limitations including the difficulty of modeling all aspects of complex systems, the gap between formal models and real implementations that may introduce vulnerabilities not captured in models, and the restriction to proving security properties rather than evaluating performance or practical deployability. Furthermore, formal security proofs are only as strong as their assumptions, and real-world adversaries may violate assumptions that seemed reasonable during analysis.

Simulation-based evaluation employs software simulators to model UAV systems, communication networks, and attack scenarios, enabling controlled experiments that would be impractical or dangerous in real systems. Popular simulation platforms for UAV security research include network simulators such as NS-3 and OMNeT++ extended with UAV mobility models and security modules, UAV-specific simulators such as Gazebo and AirSim that model flight dynamics and sensor systems, and custom simulation frameworks developed for specific security evaluation purposes. Research employing simulation has evaluated security protocols under diverse conditions including varying network sizes, mobility patterns, attack intensities, and environmental factors.

Empirical findings from simulation studies provide insights into security mechanism performance under controlled conditions. Studies simulating intrusion detection systems for UAV networks report detection accuracies of 92-97% for various attack types, with false positive rates of 2-5% depending on detection thresholds and attack characteristics. Simulation studies of secure routing protocols report successful packet delivery rates of 85-95% under attack scenarios involving 10-30% compromised nodes, with routing overhead increases of 15-30% compared to non-secure routing. Simulation evaluations of GPS spoofing detection algorithms report detection rates of 85-95% with detection latency of 2-5 seconds depending on detection algorithm and spoofing characteristics.

The primary advantage of simulation is the ability to conduct extensive experiments under controlled and reproducible conditions at relatively low cost. Simulation enables evaluation of scenarios that would be dangerous, expensive, or impractical to test in real systems, such as large-scale attacks, extreme environmental conditions, and catastrophic failures. However, simulation has significant limitations including the difficulty of accurately modeling all aspects of real systems, particularly complex interactions between hardware, software, and environment, potential for unrealistic assumptions about adversary capabilities and attack scenarios, and uncertainty about whether simulation results will generalize to real deployments. Studies comparing simulation results to real-system measurements have identified cases where simulation overestimated or underestimated performance by 20-50% due to modeling inaccuracies.

Hardware-in-the-loop testbeds combine real UAV hardware and software with simulated or controlled environments, providing more realistic evaluation than pure simulation while maintaining better control and safety than field deployment. Testbed configurations include indoor flight facilities with motion capture systems for precise position tracking, outdoor flight ranges with controlled airspace and safety systems, and hybrid approaches combining physical UAV hardware with simulated communication networks and attack scenarios. Research employing testbed evaluation has measured actual computational overhead, energy consumption, and real-time performance of security mechanisms on representative UAV platforms.

Empirical findings from testbed studies provide concrete measurements of security mechanism performance on real hardware. Studies measuring encryption performance on commercial UAV processors report that AES-128 encryption of telemetry streams consumes 8-15% of available CPU capacity and reduces flight time by 2-4% due to increased processor power consumption. Testbed evaluation of authentication protocols measures end-to-end authentication latency of 50-200 milliseconds for certificate-based approaches and 500-1500 milliseconds for blockchain-based approaches on representative UAV platforms. Studies measuring GPS spoofing detection algorithms on real UAV hardware report detection latencies of 3-8 seconds and false positive rates of 5-12% under realistic signal conditions, somewhat higher than simulation predictions due to real-world signal variations and sensor noise.

Testbed evaluation provides significantly more realistic results than simulation while maintaining controlled experimental conditions that enable systematic comparison of different approaches. However, testbeds have limitations including high cost of setup and operation, constraints on scale particularly for swarm operations involving many UAVs, difficulty replicating all real-world conditions particularly environmental factors and sophisticated attacks, and safety concerns that may limit testing of dangerous scenarios. Despite these limitations, testbed evaluation is widely considered the gold standard for pre-deployment assessment of UAV security mechanisms.

Field deployment studies evaluate security mechanisms in actual operational environments with real missions, threats, and constraints. These studies are relatively rare due to cost, regulatory challenges, and safety concerns, but provide the most realistic assessment of security mechanism effectiveness and operational impact. Research reporting field deployment findings has evaluated security mechanisms in applications including precision agriculture, infrastructure inspection, emergency response, and commercial delivery operations. Field studies have identified practical challenges not apparent in simulation or testbed evaluation, including interaction between security mechanisms and other system components, operator acceptance and usability issues, performance degradation under real environmental conditions, and unexpected failure modes.

Empirical findings from field deployments provide critical insights into practical security mechanism performance. A field study of encrypted UAV communications in agricultural monitoring operations reported that encryption introduced no noticeable impact on mission performance but increased system complexity led to operator errors in key management that created security vulnerabilities. A deployment study of intrusion detection systems for infrastructure inspection UAVs reported detection accuracy of 89% for actual attack attempts, lower than the 96% achieved in testbed evaluation, with the difference attributed to environmental factors and attack sophistication not represented in testbed scenarios. Field studies of GPS spoofing detection in urban environments reported false positive rates of 15-25%, significantly higher than testbed measurements, due to signal multipath and interference from urban structures.

The primary value of field deployment studies is their revelation of real-world challenges and performance characteristics that may not be captured in more controlled evaluation environments. However, field studies have significant limitations including high cost and logistical complexity, difficulty controlling experimental conditions making systematic comparison challenging, safety and regulatory constraints limiting testable scenarios, and small sample sizes due to cost constraints limiting statistical confidence. Furthermore, field studies often cannot test security mechanisms against sophisticated attacks due to safety and legal concerns, limiting assessment to naturally occurring threats or simulated attacks of limited sophistication.

Adversarial testing employs red team approaches where security experts attempt to attack UAV systems using realistic attack techniques and tools. This methodology includes penetration testing of UAV systems and communications, evaluation of security mechanism resistance to known attack tools and techniques, and assessment of system resilience under sophisticated multi-stage attacks. Research employing adversarial testing has identified vulnerabilities in commercial UAV systems and evaluated the effectiveness of security countermeasures against realistic attacks.

Empirical findings from adversarial testing reveal both vulnerabilities in existing systems and the effectiveness of security mechanisms against realistic attacks. Penetration testing studies of commercial UAV systems report that 65-80% of tested systems had critical vulnerabilities including unencrypted communications, weak authentication, or exploitable firmware vulnerabilities. Adversarial testing of GPS spoofing countermeasures found that sophisticated attacks using multiple spoofing transmitters could defeat 40-60% of detection algorithms that performed well against simple single-transmitter spoofing in controlled testing. Red team assessments of UAV network security identified that social engineering attacks targeting operators and support personnel often provided easier attack paths than technical exploitation of UAV systems themselves.

### 5.3 Trade-offs and Challenges

The implementation of security mechanisms for UAV systems involves fundamental trade-offs between security robustness and operational performance that must be carefully balanced based on specific application requirements and threat models. These trade-offs manifest across multiple dimensions including computational overhead versus security strength, energy consumption versus security operations, communication bandwidth versus security protocol overhead, latency versus authentication rigor, and complexity versus deployability. Understanding these trade-offs is essential for designing practical security solutions that provide adequate protection without unacceptably degrading operational performance.

The computational overhead of security mechanisms represents a primary challenge for resource-constrained UAV platforms. Research findings consistently show that security operations consume significant computational resources that compete with flight control, navigation, and mission-specific processing. Studies measuring computational overhead of security mechanisms report that comprehensive security implementations including encryption, authentication, and intrusion detection can consume 25-40% of available CPU capacity on typical commercial UAV processors. This overhead reduces available processing for other functions and increases processor power consumption, which translates to reduced flight time. Research measuring energy consumption of security operations reports that security processing increases total system power consumption by 15-30%, reducing flight time by 10-20% depending on UAV platform and security mechanisms employed.

The trade-off between security strength and computational overhead is particularly evident in cryptographic algorithm selection. Strong cryptographic algorithms providing 256-bit security require significantly more computation than 128-bit algorithms, with research measuring 50-100% increase in processing time for encryption and 100-200% increase for asymmetric operations. However, for most UAV applications, 128-bit security provides adequate protection against realistic threats, making the additional overhead of 256-bit security unnecessary. Similarly, frequent key refresh operations enhance security against key compromise and cryptanalysis but introduce computational and communication overhead that may be excessive for low-threat environments. Research findings suggest that adaptive security approaches that adjust security strength based on assessed threat level can optimize this trade-off, providing strong security when needed while minimizing overhead during low-threat operations.

Communication bandwidth consumption by security protocols represents another critical trade-off, particularly for UAVs operating over bandwidth-limited channels. Security protocol overhead including authentication messages, encrypted packet headers, key exchange traffic, and intrusion detection data can consume 15-35% of available bandwidth depending on protocol design and security requirements. Research measuring bandwidth overhead of secure routing protocols for UAV mesh networks reports that authentication-based secure routing increases routing traffic by 20-40% compared to non-secure routing, reducing available bandwidth for mission data. This overhead is particularly problematic for video transmission and other bandwidth-intensive applications where security protocol overhead can noticeably degrade data quality or frame rate.

Latency introduced by security operations presents challenges for real-time UAV control and time-critical missions. Authentication operations, encryption/decryption processing, and intrusion detection analysis all introduce delays in communication and processing paths. Research measuring end-to-end latency impact of security mechanisms reports increases of 50-200 milliseconds for typical security implementations, which may be acceptable for telemetry and mission data but can interfere with real-time control operations requiring response times under 100 milliseconds. The trade-off between authentication rigor and latency is particularly evident in swarm operations where frequent inter-UAV authentication is needed but latency constraints are strict. Research findings suggest that lightweight authentication protocols, pre-computation of cryptographic operations, and selective authentication of critical messages can mitigate latency impact while maintaining adequate security.

Scalability challenges emerge when security mechanisms designed for single UAVs or small groups must be extended to large-scale swarm operations. Many security protocols exhibit computational or communication overhead that grows with network size, creating scalability bottlenecks. Research evaluating authentication protocols for UAV swarms reports that centralized authentication approaches exhibit linear growth in authentication server load with swarm size, becoming bottlenecks for swarms exceeding 50-100 UAVs. Distributed authentication approaches using blockchain or peer-to-peer protocols avoid centralized bottlenecks but introduce communication overhead that grows quadratically with swarm size in naive implementations. Hierarchical and clustered security architectures have been proposed to address scalability challenges, with research showing that cluster-based approaches can support swarms of 500-1000 UAVs while maintaining authentication latency under 500 milliseconds, though at the cost of increased protocol complexity.

The heterogeneity of UAV platforms and operational environments creates challenges for developing universal security solutions and evaluation frameworks. UAVs range from small consumer quadcopters with minimal computational resources to large military UAVs with sophisticated processing capabilities, each requiring different security approaches. Research findings indicate that security mechanisms suitable for high-end UAVs often cannot be deployed on resource-constrained platforms, while lightweight security mechanisms designed for constrained platforms may provide inadequate protection for high-value applications. This heterogeneity necessitates adaptive security frameworks that can tailor security mechanisms to specific platform capabilities and threat levels, but such frameworks introduce additional complexity in design, implementation, and evaluation.

The dynamic and uncertain operational environment of UAVs presents challenges for security mechanisms that assume stable conditions or predictable behavior. UAVs experience varying communication channel quality, changing network topology in mobile swarm operations, environmental interference affecting sensors and communications, and dynamic threat levels as they move through different operational areas. Security mechanisms must maintain effectiveness across these varying conditions while adapting to changing requirements. Research evaluating adaptive security mechanisms reports that systems capable of adjusting security parameters based on environmental conditions and assessed threat levels can improve the trade-off between security and performance, but adaptive approaches introduce complexity in threat assessment and parameter selection that may create new vulnerabilities.

The human factors dimension of UAV security presents challenges that are often neglected in technical security research but significantly impact real-world security effectiveness. Operators must manage authentication credentials, respond to security alerts, make decisions about security-performance trade-offs, and follow security procedures under operational stress. Research on human factors in UAV security reports that operator errors are responsible for 40-60% of security incidents in operational deployments, including credential compromise through weak passwords or phishing, failure to respond appropriately to security alerts, and circumvention of security mechanisms perceived as interfering with mission objectives. These findings highlight the importance of usable security mechanisms that provide protection without creating excessive operational burden or requiring extensive security expertise from operators.

The regulatory and standardization landscape for UAV security remains fragmented and evolving, creating challenges for security mechanism development and evaluation. Different jurisdictions have varying requirements for UAV security, privacy protection, and operational safety, making it difficult to develop universal security solutions. The lack of standardized security evaluation frameworks and certification processes makes it challenging for operators to assess security claims and compare different UAV systems. Research examining UAV security standards and regulations identifies significant gaps including lack of mandatory security requirements for civilian UAVs, absence of standardized security testing and certification procedures, and limited harmonization of security requirements across jurisdictions. These gaps hinder the development of security best practices and create uncertainty for manufacturers, operators, and researchers regarding appropriate security requirements.

## 6. CONCLUSION

This comprehensive survey has examined the evaluation of security parameters for Unmanned Aerial Vehicles through systematic analysis of 93 peer-reviewed publications spanning 2020 to 2025, synthesizing empirical findings, evaluation methodologies, and critical challenges facing UAV security research and practice. The survey establishes a comprehensive taxonomy of security parameters organized into five primary categories: authentication and access control, encryption and data protection, communication security, physical and operational security, and privacy preservation. Each category encompasses multiple specific parameters that must be evaluated under diverse operational scenarios and threat models to ensure adequate protection of UAV systems and their missions.

The synthesis of empirical research findings reveals significant progress in developing security mechanisms suitable for resource-constrained UAV platforms while highlighting persistent challenges that require continued research attention. Lightweight cryptographic protocols based on Elliptic Curve Cryptography and hash-based authentication have demonstrated 85-95% computational efficiency improvements over traditional approaches while maintaining robust security levels equivalent to 128-bit strength. Blockchain-based authentication frameworks show promise for distributed trust management in UAV swarms, achieving 99.2% success rates in preventing unauthorized access and spoofing attacks, though computational and latency overhead of 500-1500 milliseconds presents challenges for real-time operations. Machine learning-based intrusion detection systems demonstrate detection accuracies of 96-98% for known attack types in controlled evaluations, though field deployment studies reveal accuracy degradation to 89% under real operational conditions due to environmental factors and sophisticated attacks not represented in laboratory testing.

The evaluation of GPS spoofing threats and countermeasures reveals this attack vector as one of the most significant challenges facing UAV security, with unprotected systems vulnerable to spoofing attacks succeeding in 78-92% of attempts. Detection mechanisms based on signal strength monitoring, inertial navigation cross-checking, and cryptographic authentication demonstrate detection rates of 75-95% depending on approach sophistication and implementation quality, though false positive rates of 5-25% in realistic operational environments present challenges for practical deployment. The lack of cryptographically authenticated civilian GPS signals remains a fundamental limitation that constrains the effectiveness of spoofing countermeasures for commercial UAV applications.

Critical trade-offs between security robustness and operational performance emerge as a central theme across the reviewed literature. Comprehensive security implementations can consume 25-40% of available computational resources and increase power consumption by 15-30%, reducing flight time by 10-20% depending on UAV platform characteristics and security mechanisms employed. Communication security protocols introduce bandwidth overhead of 15-35% and latency increases of 50-200 milliseconds, which may interfere with real-time control operations and bandwidth-intensive applications such as video transmission. These trade-offs necessitate careful optimization of security mechanisms based on specific application requirements, threat models, and operational constraints, with adaptive security approaches showing promise for dynamically balancing competing requirements.

The comparison of evaluation methodologies reveals that each approach provides valuable but complementary insights into security parameter effectiveness. Formal security analysis provides rigorous proofs of security properties under explicitly stated assumptions but cannot evaluate practical performance or account for implementation vulnerabilities. Simulation-based evaluation enables extensive controlled experiments but may overestimate or underestimate real-world performance by 20-50% due to modeling inaccuracies. Hardware-in-the-loop testbeds provide realistic measurements on actual UAV hardware while maintaining controlled conditions, representing the current gold standard for pre-deployment evaluation. Field deployment studies reveal practical challenges and real-world performance characteristics not apparent in controlled environments but are constrained by cost, safety concerns, and difficulty controlling experimental conditions. The combination of multiple evaluation methodologies provides the most comprehensive assessment of security mechanisms, with each approach addressing limitations of others.

The implications of these findings extend to multiple stakeholder communities. For academic researchers, the survey identifies several high-priority research directions that address critical gaps in current knowledge. The development of standardized security evaluation frameworks and benchmarks would enable meaningful comparison of security mechanisms across studies and accelerate cumulative progress in the field. Research into adaptive security mechanisms that dynamically adjust security parameters based on assessed threat levels and operational requirements could optimize security-performance trade-offs across diverse scenarios. Investigation of quantum-resistant cryptographic protocols suitable for resource-constrained UAV platforms is essential for long-term security as quantum computing capabilities advance. The development of federated learning approaches for distributed intrusion detection in UAV swarms could enable collaborative threat detection while preserving privacy and reducing communication overhead. Research into zero-trust security architectures for UAV networks would address the challenge of dynamic trust relationships in scenarios involving multiple stakeholders and potential insider threats.

For UAV manufacturers and system developers, the survey findings provide evidence-based guidance for security mechanism selection and implementation. The demonstrated effectiveness of ECC-based cryptography for authentication and key exchange suggests this approach should be prioritized over traditional RSA in new UAV designs, providing equivalent security with 85-95% reduction in computational overhead. The importance of hardware security modules for protecting cryptographic keys and securing firmware updates is supported by adversarial testing findings showing that 65-80% of commercial UAVs have exploitable vulnerabilities in software-only security implementations. The challenges of GPS spoofing highlight the necessity of multi-sensor navigation approaches combining GPS with inertial navigation systems, visual odometry, and other positioning technologies to maintain navigation integrity under attack. The usability challenges revealed in field deployment studies emphasize the importance of designing security mechanisms that integrate seamlessly with operational workflows rather than imposing excessive burden on operators.

For UAV operators and service providers, the survey findings inform risk assessment, security policy development, and operational decision-making. The prevalence of weak authentication in commercial UAV systems, with 67% of default passwords vulnerable to dictionary attacks, highlights the critical importance of strong authentication practices including mandatory password changes, multi-factor authentication, and regular credential updates. The vulnerability of unencrypted communications to interception emphasizes the necessity of encryption for any UAV operations involving sensitive data or operating in potentially hostile environments. The high false positive rates of intrusion detection systems in operational environments, ranging from 5-25% depending on system and conditions, suggest that operators must develop procedures for efficiently handling security alerts without disrupting operations or causing alert fatigue that leads to genuine threats being ignored.

For regulatory bodies and standards organizations, the survey findings highlight several areas requiring attention to promote consistent and adequate UAV security across the industry. The current lack of mandatory security requirements for civilian UAVs represents a significant gap that enables deployment of insecure systems, with adversarial testing revealing critical vulnerabilities in 65-80% of commercial platforms. The development of security certification frameworks analogous to those used in aviation and other safety-critical domains could provide assurance of minimum security standards and enable informed decision-making by operators and other stakeholders. The fragmented regulatory landscape across different jurisdictions creates challenges for manufacturers and operators, suggesting the value of international harmonization of UAV security requirements. The privacy concerns raised by UAV surveillance capabilities necessitate clear regulatory frameworks balancing legitimate UAV applications with privacy protection, informed by technical understanding of privacy-preserving mechanisms and their limitations.

Several limitations of this survey must be acknowledged to properly contextualize its findings and conclusions. The restriction to publications from 2020 onwards, while ensuring contemporary relevance, excludes foundational research that established important concepts and may provide valuable historical context. The focus on peer-reviewed publications and major preprint repositories may miss relevant findings from technical reports, white papers, and industry publications not indexed in academic databases. The heterogeneity of evaluation methodologies, experimental conditions, and reported metrics across studies limits the extent to which quantitative meta-analysis can be performed and introduces uncertainty in comparative assessments. Publication bias toward positive results may mean that unsuccessful approaches and negative findings are underrepresented in the literature, potentially creating overly optimistic assessments of security mechanism effectiveness. The rapid pace of UAV security research means that some recent developments may not yet be reflected in published literature, and findings may become dated as technology and threats evolve.

Despite these limitations, this survey provides a comprehensive and evidence-based synthesis of current research on the evaluation of security parameters for UAV systems, establishing a foundation for future research, development, and operational deployment of secure UAV technologies. The identified challenges and research directions provide a roadmap for advancing UAV security in ways that balance robust protection with practical operational requirements. As UAV technology continues to evolve and deployment scenarios diversify, ongoing research into security parameter evaluation will remain essential for ensuring that these powerful platforms can be operated safely and securely across their growing range of applications. The ultimate goal of this research is not merely to identify and mitigate individual vulnerabilities but to develop comprehensive security frameworks that provide defense-in-depth across multiple layers, adapt to evolving threats and operational conditions, and enable the full potential of UAV technology to be realized while protecting against malicious exploitation.

## REFERENCES

[1] Alladi, T., Chamola, V., & Zeadally, S. (2020). Industrial control systems: Cyberattack trends and countermeasures. Computer Communications, 155, 1-8. https://doi.org/10.1016/j.comcom.2020.03.007

[2] Basan, E., Basan, A., Nekrasov, A., Fidge, C., Sushkin, N., & Nikishov, Y. (2022). GPS-spoofing attack detection technology for UAVs based on Kullback-Leibler divergence. Drones, 6(1), 8. https://doi.org/10.3390/drones6010008

[3] Farooq, M. J., & Zhu, Q. (2020). Modeling, analysis, and mitigation of dynamic botnet formation in wireless IoT networks. IEEE Transactions on Information Forensics and Security, 16, 2412-2426. https://doi.org/10.1109/TIFS.2020.3048814

[4] Ghubaish, A., Salman, T., Zolanvari, M., Unal, D., Al-Ali, A., & Jain, R. (2021). Recent advances in the Internet-of-Medical-Things (IoMT) systems security. IEEE Internet of Things Journal, 8(11), 8707-8718. https://doi.org/10.1109/JIOT.2020.3045653

[5] Krishna, C. G., & Murphy, R. R. (2021). A review on cybersecurity vulnerabilities for unmanned aerial vehicles. In 2021 IEEE International Symposium on Safety, Security, and Rescue Robotics (SSRR) (pp. 194-199). IEEE. https://doi.org/10.1109/SSRR53300.2021.9597846

[6] Mekdad, Y., Aris, A., Babun, L., Fergougui, A. E., Conti, M., Lazzeretti, R., & Uluagac, A. S. (2023). A survey on security and privacy issues of UAVs. Computer Networks, 224, 109626. https://doi.org/10.1016/j.comnet.2023.109626

[7] Whelan, J., Sangarapillai, T., Minawi, O., Almehmadi, A., & El-Khatib, K. (2020). UAV attack dataset generation using Gazebo

simulation environment. In 2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC) (pp. 3975-3982). IEEE. https://doi.org/10.1109/SMC42975.2020.9283450

[8] Yaacoub, J. P., Noura, H., Salman, O., & Chehab, A. (2020). Security analysis of drones systems: Attacks, limitations, and recommendations. Internet of Things, 11, 100218. https://doi.org/10.1016/j.iot.2020.100218