drones

MDPI

Review

A Review on Software-Based and Hardware-Based Authentication Mechanisms for the Internet of Drones

Emmanouel T. Michailidis [1,2,*] and Demosthenes Vouyioukas [2]

[1] Department of Electrical and Electronics Engineering, University of West Attica, Ancient Olive Grove Campus, 250 Thivon & P. Ralli Str., 12241 Egaleo, Greece
[2] Department of Information and Communication Systems Engineering, School of Engineering, University of the Aegean, 83200 Samos, Greece; dvouyiou@aegean.gr
* Correspondence: emichail@uniwa.gr

Abstract: During the last few years, a wide variety of Internet of Drones (IoD) applications have emerged with numerous heterogeneous aerial and ground network elements interconnected and equipped with advanced sensors, computation resources, and communication units. The evolution of IoD networks presupposes the mitigation of several security and privacy threats. Thus, robust authentication protocols should be implemented in order to attain secure operation within the IoD. However, owing to the inherent features of the IoD and the limitations of Unmanned Aerial Vehicles (UAVs) in terms of energy, computational, and memory resources, designing efficient and lightweight authentication solutions is a non-trivial and complicated process. Recently, the development of authentication mechanisms for the IoD has received unprecedented attention. In this paper, up-to-date research studies on authentication mechanisms for IoD networks are presented. To this end, the adoption of conventional technologies and methods, such as the widely used hash functions, Public Key Infrastructure (PKI), and Elliptic-Curve Cryptography (ECC), is discussed along with emerging technologies, including Mobile Edge Computing (MEC), Machine Learning (ML), and Blockchain. Additionally, this paper provides a review of effective hardware-based solutions for the identification and authentication of network nodes within the IoD that are based on Trusted Platform Modules (TPMs), Hardware Security Modules (HSMs), and Physically Unclonable Functions (PUFs). Finally, future directions in these relevant research topics are given, stimulating further work.

Keywords: authentication; Internet of Drones (IoD); Physically Unclonable Function (PUF); privacy; security; Unmanned Aerial Vehicle (UAV)

Citation: Michailidis, E.T.; Vouyioukas, D. A Review on Software-Based and Hardware-Based Authentication Mechanisms for the Internet of Drones. *Drones* **2022**, *6*, 41. https://doi.org/10.3390/drones6020041

Academic Editors: Mohammed H. Alsharif and Muhammad Asghar Khan

Received: 31 December 2021
Accepted: 6 February 2022
Published: 8 February 2022

1. Introduction

In the forthcoming Internet of Drones (IoD) era [1,2], various types of drones, formally referred to as Unmanned Aerial Vehicles (UAVs) or Remotely Piloted Aircrafts (RPAs), will act as flying smart "things" and collaborate with key enabling technologies, such as the Internet of Things (IoT) [3], cloud computing [4], Mobile Edge Computing (MEC) [5], Machine Learning (ML) [6], Blockchain [7], network slicing [8], Software-Defined Networking (SDN) [9], and Fifth Generation (5G) communications [10]. Drones are small, unmanned, fixed-wing or rotary-wing aircrafts that can be rapidly deployed at high elevation angles for short time periods, allowing for cost-effective, flexible, and ubiquitous wireless connections. Based on the IoD, innovative applications are envisioned in the civilian and military domains, including road traffic monitoring, area mapping, the monitoring of critical infrastructure and industrial facilities, surveillance and disaster management, public safety, entertainment, live streaming, and military services [1–3]. In this context, drones are expected to be deployed in various missions where human intervention is not feasible. Additionally, drones will incorporate communication, computation, energy, and control units, as well as actuators and advanced onboard sensors (e.g., cameras, accelerometers,

and gyroscopes) for data collection, the measurement of physical attributes (e.g., altitude, speed, and location), and the maintenance of a reference trajectory.

Nevertheless, there exist various challenges towards the establishment and evolution of the IoD, including the wide distribution of the network nodes in open and remote environments, the high mobility features, the dynamic network topology, and the weak, unencrypted, and insecure wireless communication links. In addition, the limited energy, computing, and storage resources of drones make them vulnerable to a wide range of invasive, non-invasive, and semi-invasive attacks [11]. Typical paradigms of these attacks are eavesdropping, man-in-the-middle attacks, spoofing, tampering, Denial-of-Service (DoS), impersonation/sybil attacks, replay attacks, and forgery attacks. These attacks intend to obtain sensitive collected data stored in drones, exploit non-authorized connections, and also extract cryptographic keys. Mitigating potential security and privacy threats and protecting the IoD against adversaries is vital and of utmost importance due to possible economic, societal, and environmental consequences. More importantly, IoD networks are volatile, since the nodes can dynamically join or leave the networks, whereas a vast number of heterogeneous nodes exist. In this respect, malicious entities may use unauthorized drones to destroy authorized ones through physical collisions. Hence, node authentication constitutes the prime requirement towards security for an IoD network. As authentication confirms the identity of the components involved in the IoD, only authorized and legitimate components should gain access to confidential information. In Figure 1, certain limitations of drones are demonstrated along with particular characteristics of IoD networks and types of attacks.

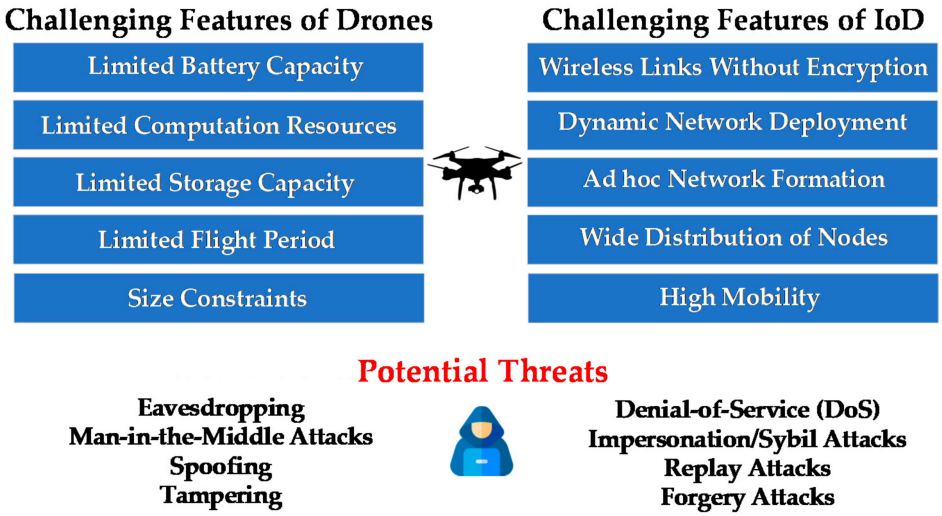

Figure 1. Challenges and threats within the Internet of Drones (IoD).

However, contrary to widely established conventional wireless networks, there are no identification and authentication mechanisms or unified security standards in the IoD. Another challenge associated with the utilization of typical security protocols is the heterogeneous nature of IoD networks and the diverse applications that necessitate specialized protection methods. As drones are typically resource-constrained, conventional and sophisticated security schemes based on complex cryptographic algorithms, such as the RSA (Rivest–Shamir–Adleman) public-key cryptosystem, cannot be directly applied. More specifically, designing authentication methods for the IoD is challenging, as a trade-off exists between lightweight features, efficiency, and adequate security. On the other hand, the limited flying period of drones necessitates their rapid authentication.

Motivated by the aforementioned observations, this review paper intends to shed light on a broad set of up-to-date, state-of-the-art authentication mechanisms for safeguarding the IoD. An overview of the key components of the IoD is initially given, and the authentication requirements are described. Then, an exhaustive investigation of recent advances in

software-based and hardware-based authentication schemes from all possible categories and their application in the IoD is carried out, and an insight into the latest trends in the field of the node authentication for the IoD is given. Fertile research areas and open issues are also identified for both the software-based and hardware-based authentication areas.

The rest of the paper is organized as follows. Section 2 provides a detailed investigation on relevant review and survey papers and describes their goals and shortcomings. Section 3 gives insights on the authentication procedure and discusses the current trends and emerging technologies for authentication within the IoD. In Section 4, recent authentication mechanisms for the IoD landscape that exploit software-based techniques are studied. Section 5 outlines hardware-based authentication solutions. Finally, conclusions and future research perspectives are drawn in Section 6.

2. Previous Review Papers

Previously, along with the growing number of proposed communication and networking solutions for the IoD, a wide range of relevant review papers investigating the interplay of the IoD and security aspects have been published. To the best of the authors' knowledge, the majority of previous relevant reviews, surveys, and tutorials investigated the security issues of the IoD without focusing on novel, hardware-based solutions. In [12], various features of the IoD were extensively reviewed from a layered and cross-layered network architecture perspective. In addition, the integration of UAVs in cellular networks was considered in [13], and the corresponding core technologies and challenges were surveyed. More specifically, the aforementioned work was dedicated to UAV types, the role of UAVs as flying relays, interference mitigation techniques, as well as standardization, regulation, and experimentation activities. Additionally, this work comprised an overview on the cyber security issues and indicative use cases. However, the security of the IoD was not the main research objective of [12,13]. In particular, authentication methods were partly and inadequately investigated in [12], and up-to-date research works were missing. From a cyber–physical security point of view, a well-structured review of UAV-based networks was provided in [14], and the requirements for cyber–physical security applications were discussed.

As the protection of heterogeneous, beyond 5G (B5G) air-to-ground deployments against attacks across network layers is necessary, a detailed review on research works that are related with ML techniques and UAV-based communications was provided in [6], and Physical Layer Security (PLS), as well as safety issues, were surveyed. Specifically, PLS was considered as a complementary security solution together with traditional encryption methods. In this regard, advanced ML-based information theoretic techniques were proposed to further improve the secrecy level of wireless transmissions. Since the implementation of Remotely Piloted Aircraft Systems (RPAS) with onboard intelligence that operate autonomously is highly desirable in real-world deployments, the role of Artificial Intelligence (AI) was explored in [15] without mentioning authentication issues concerning RPAs. Specifically, AI was considered as the key technology to avoid human intervention, reduce faults, and enhance the decision-making process in dynamic environments, thus ensuring accuracy, control system security, and safety. In [16], the security challenges at higher communication layers that are evoked in the context of UAV-based delivery systems, Intelligent Transportation Systems (ITS), and real-time multimedia streaming were reported. Additionally, Artificial Neural Network (ANN)-based schemes were introduced to mitigate potential threats. A classification on privacy and security issues in 5G-enabled, UAV-aided networks was provided in [7], and a Blockchain-based security countermeasure was presented. However, this survey paper is outdated, since recent research works were not included. Moreover, hardware security methods for the authentication of drones were not studied.

The existing security vulnerabilities of drones and the security issues that are associated with compromised drones in the military and civilian sector were comprehensively reviewed in [11], a realistic scenario of an attack life cycle was described, and countermea-

sures that can safeguard drone systems were suggested. In [17], a high-level UAV-based system architecture along with the key elements of civilian UAVs were presented. Additionally, security, privacy, and safety issues concerning deploying civilian drones in the national airspace were analyzed, a discussion about typical physical challenges and cyber threats was provided, and open problems were identified. To handle security issues and cyber-attacks that arise in the context of SDN-enabled UAV networks, solution schemes were foreseen in [9]. The benefits and drawbacks of security countermeasures against possible attacks in critical UAV-based applications (e.g., military and disaster scenarios) were highlighted in [18], and the role of Blockchain, ML, and watermarking was emphasized. An exhaustive literature review on the existing security protocols for UAVs together with the vulnerabilities of these protocols was provided in [19]. In this respect, several crucial topics were investigated, such as secure UAV-based communications, intrusion detection systems, the security of routing protocols, attacks on control systems, the detection of malicious UAVs, etc. As IoT and 5G communications will pave the way for novel applications and services, the role of drones as "flying" things was indicated in [20], and the security issues were synopsized. In this direction, a representative IoT architectural framework that ensures end-to-end protection against security and privacy threats in a collaborative and holistic manner was demonstrated. Furthermore, a thorough review of application scenarios for drone-based communications, security challenges, and advanced security solutions (i.e., Blockchain, SDN, ML, and fog/edge computing) was given in [21], and future research perspectives were discussed. Nevertheless, the hardware security issues regarding the IoD were not studied in [9,11,17–21].

Although information security and network security have remained topics of paramount importance for both system designers and users, miscellaneous security vulnerabilities and attacks on hardware have recently been reported. In this direction, the security and privacy issues of UAVs were classified in [22] considering the hardware, the software, the communication, and the sensor levels. More importantly, the vulnerabilities, indicative threats, active and passive attacks, and potential mitigation methods against attacks were thoroughly investigated for each level. Although a useful framework for designing secure UAV-based systems was provided, the authentication of UAVs was not the prime target of this work, and relevant authentication mechanisms were not adequately reviewed. Beyond the IoD, the necessity of safeguarding the hardware of IoT devices in addition to software against Hardware Trojan (HT)-based attacks was pointed out in [23], and a taxonomy of HTs along with indicative countermeasures was given. Moreover, the benefits of using Physically Unclonable Functions (PUFs) for secret key generation and identification of network nodes in IoT applications was underlined in [24], relevant security techniques were comprehensively discussed, and a PUF implementation that relies on Resistive Random-Access Memory (ReRAM) was presented. The state-of-the-art mechanisms in the context of hardware security for the IoT devices were also outlined in [25], and emphasis on the ML solutions was given. Notwithstanding, the works in [24,25] did not invoke drones as IoT nodes towards the realization of IoD scenarios. Thus, relevant research activities were not included. In order to reconcile the shortcomings of previous work and investigate the ambiguous landscape regarding the available methods for the authentication of network entities within the IoD, newer review papers are indispensable. Table 1 briefly summarizes the aforementioned review and survey research works.

Table 1. Review and survey papers on security and privacy issues of the Internet of Things (IoT) and IoD.

References	Short Description	Security Issues and Methods for IoD	Authentication Methods
Bithas et al., 2019 [6]	Survey on Machine Learning (ML) methods for Unmanned Aerial Vehicle (UAV)-based communications	ML-based Physical Layer Security (PLS) methods	Software-based
Mehta et al., 2020 [7]	Survey on security issues in UAV networks	Blockchain-based security solutions	Software-based

Table 1. *Cont.*

References	Short Description	Security Issues and Methods for IoD	Authentication Methods
McCoy et al., 2019 [9]	Review on security solutions for Software-Defined Networking (SDN)-enabled UAV networks	Vulnerabilities, attacks, countermeasures, and open issues	Software-based
Yaacoub et al., 2020 [11]	Analysis of vulnerabilities of communication links of drone-based networks and application domains	Software-based security countermeasures	Software-based
Boccadoro et al., 2021 [12]	Review on research activities on IoD networking architectures	Cyber security issues and use cases	Software-based and hardware-based (partly studied)
Fotouhi et al., 2019 [13]	Survey on characteristics, interference issues, standardization activities, and testbed activities of UAV-assisted communications	Cyber–physical and physical security threats and use cases	Nothing in particular
Shakeri et al., 2019 [14]	Review on design challenges of multi-UAV systems for cyber–physical applications	Requirements for cyber–physical security applications	Nothing in particular
Aibin et al., 2021 [15]	Survey of Remotely Piloted Aircraft Systems (RPAS) Autonomous Control Systems that leverage Artificial Intelligence (AI) methods	Integration of AI-based strategies for increased control system security	Nothing in particular
Challita et al., 2019 [16]	Review on wireless and security challenges of UAV-based applications and ML-based solutions	ML-based security solutions	Software-based
Altawy et al., 2017 [17]	Survey on security, privacy, and safety aspects during the operation of civilian drones	Physical challenges and cyber threats	Software-based
Syed et al., 2021 [18]	Review on optimal techniques for securing UAVs	Blockchain-based, ML-based, and watermarking-based security methods	Nothing in particular
Shafique et al., 2021 [19]	Survey of existing security protocols and vulnerabilities in UAVs	Vulnerabilities in the security protocols and possible software-based solutions	Software-based
Lagkas et al., 2018 [20]	Review on UAV-enabled, IoT-enabled, and Fifth Generation (5G)-enabled applications	Security challenges and solutions for fleet management over aerial networking	Nothing in particular
Hassija et al., 2021 [21]	Review on security and reliability enhancements for existing and upcoming drone-enabled applications	Security challenges, emerging solutions, and open issues	Software-based
Mekdad et al., 2021 [22]	Survey on security and privacy issues of UAVs	Vulnerabilities, threats, attacks, and countermeasures at the hardware level, software level, communication level, and sensor level.	Software-based
Sidhu et al., 2019 [23]	Review on hardware security challenges of IoT devices and taxonomy of Hardware Trojans (HTs)	Nothing in particular	Hardware-based
Shamsoshoara et al., 2020 [24]	Survey on Physical Unclonable Function (PUF)-based security solutions for the authentication and identification of IoT devices	Nothing in particular	Hardware-based
Michailidis et al., 2020 [25]	Review on conventional, ML-based, and hardware-based security solutions for the IoT	Nothing in particular	Hardware-based
This paper	Review on up-to-date research works on software-based and hardware-based authentication mechanisms for IoD networks	Conventional and emerging technologies for the authentication of IoD network entities	Software-based and hardware-based

3. Overview of Authentication Principles and Potential Authentication Solutions

In IoD deployments, network architectures based on aerial and ground infrastructures or ad hoc configurations with only aerial nodes are typically considered [1]. The former involves flying drones that are usually configured in groups, the users, and a trusted Ground Control Station (GCS) with high computational capabilities and sufficient energy supply. The GCS remotely controls and monitors the drones during their operation. In addition, the latter includes aerial nodes that operate in a decentralized manner using drone-to-drone communication links. It is worth noting that drone-to-GCS communication

links are usually public, insecure, and susceptible to active attacks (e.g., man-in-the-middle attacks) and passive attacks (e.g., eavesdropping). On the other hand, drone-to-drone communication links can be modeled as Peer-to-Peer (P2P) links that are vulnerable to P2P attacks, such as sybil attacks and Distributed DoS (D-DoS) [11].

The authentication procedure is related not only with node authentication, but also with message authentication. Node authentication necessitates the verification of the identity of an IoD node, the provision of access to network resources, and the establishment of network connections between registered and trusted nodes. By successfully authenticating legitimate nodes, unauthorized ones are filtered out, and thus, security and privacy are maintained. Authentication schemes can be classified into several categories as follows:

- Mutual Authentication: Two network elements mutually confirm their identity using signatures and then exchange data via a secure drone-to-GCS, drone-to-user, or drone-to-drone channel [26].
- Authentication of Drones: An acoustic signal, a flight trajectory, a gyroscope, or a specialized PUF chip can be used to verify the identity of a drone within the IoD [27].
- Authentication of External Users: Passwords, smart cards, and personal biometrics can be exploited to validate a user and permit the exchange of secret keys via a key agreement protocol [28].
- Authentication of Operators: Behavioral biometrics can be used for the authentication of an operator [29].

On the other hand, checking the integrity of the data, verifying its source of origin, and detecting abnormalities in the data pattern is required in message authentication.

As depicted in Figure 2, authentication typically invokes multiple phases and the exchange of cryptographic keys between the network entities. The setup phase is the first step, where the GCS initializes and locally stores all the security parameters, including the protocol, the secret key, and the public–private key pairs. Then, the partially trusted users and drones, which aim to join the IoD network, register with the trusted GCS to achieve primal identification using secure channels. In addition, the corresponding records are stored in the database of GCS. In the next step, the authentication and key agreement take place, where a shared secret key is generated and agreed upon by the participants through an insecure channel. The final step involves the update phase, which dynamically determines whether a drone can be added or revoked.

Software-based authentication schemes solely rely on software, mathematical algorithmic approaches, secret keys to authorize the nodes, and encryption methods (e.g., RSA and Advanced Encryption Standard (AES)). Additionally, the one-way hash functions have been traditionally used in modern cryptography and information-security applications, such as Message Authentication Codes (MACs) and digital signatures, in order to quickly map message data of arbitrary sizes to bit arrays of fixed, compressed sizes [30]. Several cryptographic hash algorithms have been proposed over the last 30 years. Among them, some older algorithms (e.g., the Message Digest 5 (MD5), Secure Hash Algorithm-1 (SHA-1), RACE Integrity Primitives Evaluation Message Digest (RIPEMD), and Whirlpool) are vulnerable to collision attacks and length extension attacks. However, more recent implementations (e.g., truncated SHA-2, SHA-3, BLAKE2, and BLAKE3) can resist these types of attacks. In addition, the widely adopted public key cryptography schemes that are based on the Public Key Infrastructure (PKI) framework allow for the secure exchange of data using digital certificates that bind an entity to its public key [31]. Using PKI, the legitimacy of the IoD network entities can be verified, and information can be securely exchanged. Moreover, Elliptic-Curve Cryptography (ECC) has been used to offer an equivalent security level to RSA with abundant smaller key sizes [32]. ECC belongs to the family of asymmetric public-key cryptosystems and is related with the mathematics of elliptic curves and with the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP). Among the advantages of ECC are the rapid generation of the keys and the digital signature, as well as the minimal required computing resources. Additionally, ECC eliminates the need for mathematical co-processors. However, ECC can be potentially susceptible to side-channel

attacks and twist-security attacks that intend to leak information and invalidate security for the private keys. Identity (ID)-based security has been also used for the authentication process and is associated with an account login using a username and password, fingerprint biometric authentication, and facial recognition.

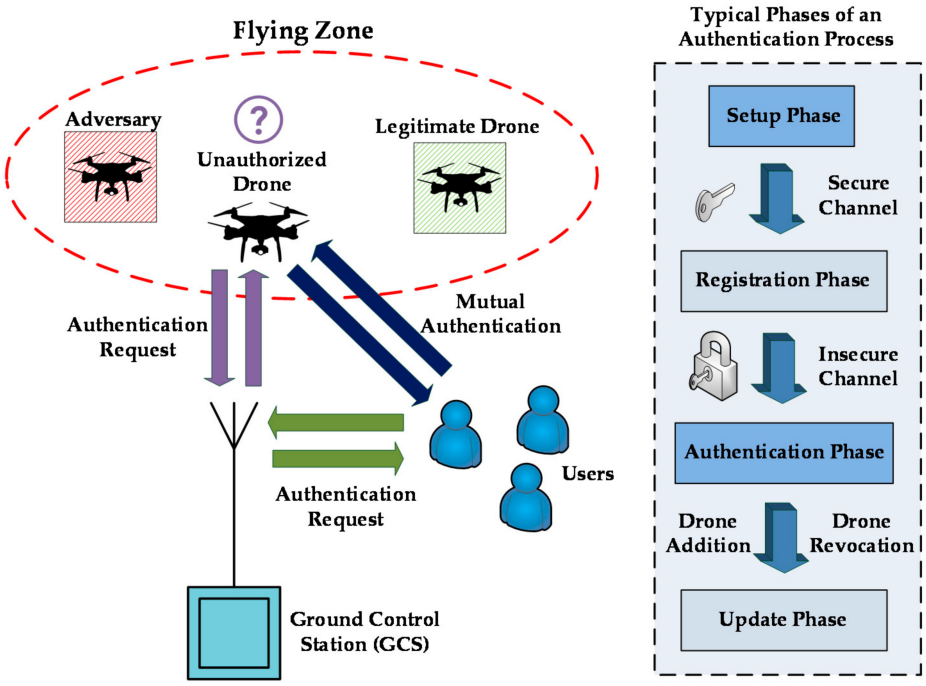

Figure 2. Simple representation of an authentication process in an IoD network.

In recent years, there have been a wide range of works relating the authentication of IoD elements with emerging technologies, such as cloud/fog computing, MEC, ML, Blockchain, and SDN. Connecting the IoD with the cloud and storing sensitive information in the cloud enhances the network security and provides scalability [4], whereas MEC devices can support the mobility features of drones and reduce the computation cost [5]. Moreover, ML is an effective method to limit the security flaws in large-scale network deployments and dynamic environments by learning the behavior of network entities and predicting threats [6]. In addition, Blockchain has been suggested as a tamper-resistant and tamper-evident digital ledger that enables trustworthy and secure transactions in a decentralized fashion [7]. Additionally, the SDN-enabled IoD allows for a programmable network, in which various security functions are integrated and customized [9].

As secret keys represent sensitive information, various protection mechanisms have been developed. Although node authentication constitutes an essential precondition for secure operation over an IoD network, existing software-based security techniques utilize vulnerable, non-volatile, memory-based devices (e.g., flash memory and Electrically Erasable Programmable Read-Only Memory (EEPROM)) to store cryptographic keys, which may be exposed to physical attacks using a scanning electron microscope (SEM), tampering or probing. Additionally, as previously mentioned, drones generally have memory, storage, computation, and energy constraints, which hinder the application of modern, computationally intensive cryptographic techniques. To prevent the risk of unauthorized access, dedicated Integrated Circuits (ICs) and computing devices, such as Trusted Platform Modules (TPMs) and Hardware Security Modules (HSMs), can be used alongside software mechanisms (e.g., AES or PKI) [33] to carry out authentication operations. TPMs are special-purpose, secure hardware units that ensure hardware integrity and authentication by integrating unique and secret Endorsement Keys (EKs), which are accessible using software. Nevertheless, TPMs may be vulnerable to cold boot attacks, as long as the attacker has physical access to the devices. In addition, HSMs are standards-compliant

cryptographic devices with tamper-proof or tamper-resistant features that securely manage cryptographic keys and safeguard confidential data. However, HSMs may be prone to man-in-the-middle attacks, which aim to steal devices, clone devices, or apply reverse engineering. On the other hand, in large-scale IoD networks, key management is challenging owing to the large number of nodes.

To strengthen the identification, authentication, and access control, the implementation of PUFs has been recently suggested [24,25,27]. PUFs constitute a simple and cost-effective means of protecting hardware. More importantly, PUFs are non-reproducible, since they exploit the non-deterministic physical variation of the manufacturing process and have an inherently unpredictable behavior. Using PUFs as hardware security primitives, secret keys can be generated, digital fingerprints can be produced, and lightweight authentication protocols can be designed, without the need to store keys in memory units. Based on its uniqueness, an embedded PUF chip can generate a unique response (i.e., the output) for a particular challenge (i.e., the input) on demand, thus forming a unique challenge–response pair (CRP) [34]. PUFs can be classified into strong and weak PUFs depending on the level of security that they can support. In strong PUFs, the number of CRPs exponentially increases with the size of the chip area, whereas a significant number of CRPs is possessed by the weak PUFs. Nevertheless, PUFs are often highly sensitive to physical conditions and environmental changes, which influence their responses and prevent proper key generation. Although there is no unified framework for testing the responses of a PUF, certain performance metrics are usually used, including uniqueness, reproducibility (or reliability), and randomness (or uniformity) [34]. Aside from intrinsic PUFs, which protect devices without introducing any modifications, external components, or extra logic to explicitly introduce randomness, controlled PUFs (CPUFs) were also proposed to prevent man-in-the-middle attacks by exploiting control logic. As far as IoD networks are concerned, PUFs can be used to authenticate individual resource-constrained IoD nodes without using costly cryptographic methods. In Figure 3, several structuring elements of lightweight authentication solutions are illustrated.

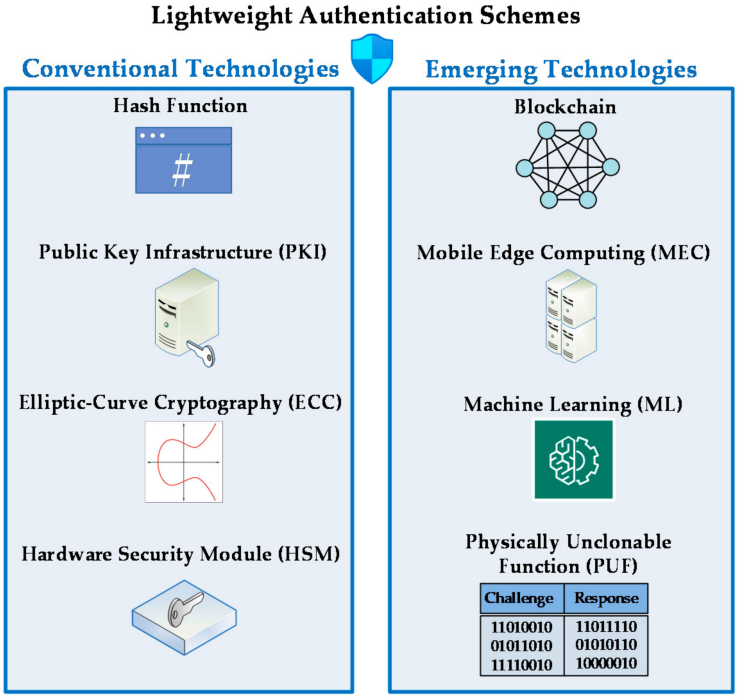

Figure 3. Key enablers for secure authentication within the IoD.

4. Software-Based Authentication Mechanisms for the IoD

In order to effectively perform the authentication of network nodes and reject the malicious ones, the IoD strives to pursue evolution in emerging technologies and trade on the significant achievements in this research field. To this end, several software-based methods have been employed to tackle authentication issues. In this section, recent research efforts on this sector are outlined and summarized in Table 2.

4.1. Hash-Based Authentication

Simple hash cryptographic functions were used in [30] to minimize the computation cost, and a resilient authentication protocol for IoD was proposed based on the Hash-based Message Authentication code Secure Hash Algorithmic (HMASHA1) function and randomized keys. To significantly reduce the computation effort and energy consumption during encryption and decryption operations, while retaining robustness against possible attacks, an efficient Lightweight Privacy-Preserving Scheme (L-PPS) for a smart IoD environment was proposed in [35]. The IoD network comprised clustered drone-nodes that gathered sensing information, intermediate cluster-heads, and a powerful server station. The proposed scheme exploited the Chebyshev Chaotic-Maps and avoided complicated cryptographic operations. More specifically, this scheme involved hash functions, Hash-based Message Authentication Code (HMAC), and bitwise exclusive-OR (XOR) operations to establish a secure channel, perform the mutual authentication between the network nodes, and thus enable the secure exchange of sensing data. As the IoD has certain dynamic characteristics owing to the inherent nature of drones, this scheme used a secret token exchange in each session and persistently and also rapidly authenticated the network nodes within a predefined time period. The performance of the L-PPS was tested using Scyther and the Random Oracle Model (ROM) [36]. Based on the results, the L-PPS can surpass other relevant existing schemes in terms of various metrics, such as end-to-end delay, packet delivery ratio, required time for connection for each drone, and throughput rate. In [37], a hash-based scheme based on random labels for the authentication of drones in large swarm deployments was proposed. Specifically, the lightweight hash functions SHA-256 and SPONGENT-128 were exploited to generate the random labels of the tasks, whereas military applications were considered. In order to construct a network simulation environment and test the delay and throughput of the aforementioned authentication scheme, the OMNeT++ framework was used and verified that the authentication scheme is accurate, cost-effective, and energy-efficient.

In [38], an Authenticated Key Exchange (AKE) protocol, the authenticated encryption mechanism AEGIS [39], SHA-256, and a bit-wise XOR operation were successfully combined to construct the LAKE-IoD (Lightweight AKE Protocol for IoD Environment) and authenticate mobile users. An IoD scenario, where multiple drones fly in specific fly zones and track the environment in their vicinity, was considered. In particular, the drones were employed to forward valuable data to the ground management server and also to external users. However, these users should be authenticated via the management server, in order to avoid man-in-the-middle and replay attacks. By following the principles of the Dolev and Yao (DY) [40] threat model, where an adversary is granted complete network control, the security of LAKE-IoD was initially tested using formal security analysis through the Burrows–Abadi–Needham (BAN) logic and the Scyther software tool. Additionally, an informal security analysis was realized. The simulation results underlined the effectiveness of LAKE-IoD regarding the communication, computing, and storage cost. As the authentication of single or multiple drones is prerequisite for becoming members of a swarm, CoMAD (Context-Aware Mutual Authentication Protocol for Drone Networks) was proposed in [41]. More importantly, CoMAD was the first protocol to introduce context information to carry out the information procedure and re-shape the swarm by adding or removing groups of swarm members, where context information represents secret-mission-based data that only the legitimate swarm members are aware of. An ad hoc drone network without secure channels and secure storage was assumed, where a master drone performed

the management operation of the swarm. As long as new nodes, for which there was no antecedent context information, requested authentication, the SHA version 2 or 3 with a minimum 256 bit output size was used to ensure resilience against collisions. The security performance of CoMAD was tested and verified informally by considering active and passive attacks and also formally using Scyther. Moreover, a military application of the IoD, where drones communicated with a Powerful Intelligence Computer System (PICS) or an Airborne Control and Command Platform (AC2P), was considered in [42]. The pairing cryptography was leveraged, which enables the generation of the public–private key pairs and the one-way hash functions. In addition, the key exchange was facilitated by the Computational Diffie–Hellman Problem (CDHP). In this regard, identity-based and aggregate signature-based authentication frameworks were developed to ensure confidentiality and data integrity.

4.2. PKI-Based Authentication

In [31], SENTINEL (Secure and Efficient autheNTIcation for uNmanned aErial vehicLes), a lightweight mechanism for the IoD that facilitates the authentication between drones and Ground Stations (GSs) was presented. SENTINEL was based on a PKI, used registered flight session keys to authenticate the resource-constrained drones in a particular flying zone, and prevented unauthorized drones that act as potential attackers from accessing the IoD infrastructure. In this respect, SENTINEL adopted a specially designed, lightweight binary certificate format instead of the typical X.509 certificate to reduce the size of the certificate. Using the Elliptic Curve Digital Signature Algorithm (ECDSA), Password-Based Key Derivation Function 2 (PBKDF2), and HMAC-SHA256, a prototype of SENTINEL was implemented, and its security was validated via ProVerif. The experimental results indicated that SENTINEL could execute the authentication process about 3.1 times faster than the "Transport Layer Security (TLS) for IoT" protocol. In [43], a PKI-based simple key agreement framework for the IoD was proposed, where a key exchange realized during encryption/decryption and the public–private key pair generated at the GCS was dynamically changed for each session. In this framework, a hash cryptographic operation was supported, and an authentication process between GCS, civilian drones, and users took place in six distinct phases, including: (i) the setup/initialization, (ii) the user's registration, (iii) the drones' registration, (iv) the key agreement, (v) the dynamic drone addition, and (vi) the drone revocation. The reliable ProVerif and Real-Or-Random (ROR) model [36] validated the security of the aforementioned authentication method, and indicative results were provided to demonstrate its efficiency with respect to computation, storage, and communication costs. Although PKI stands for a typical security method to authenticate network entities using certificates, potentially malicious drones may penetrate the network using valid certificates. To overcome this drawback, UAVouch was developed in [44]. In particular, UAVouch is a distributed authentication method with low computing requirements that enables the identification of drones before entering a specific group. This method can handle the authentication of drones by not only exploiting the PKI principle, but also examining the trajectory and the position of the drones, in order to detect abnormal mobility patterns. A military surveillance scenario with multiple cells consisting of an armored ground vehicle and a swarm of drones was considered, whereas both impersonation attacks within the cell and sybil attacks outside the cell were studied. In this respect, a network simulator setup based on INET and OMNetCC was established to assess UAVouch. Based on the results, UAVouch achieved a detection accuracy score of over 85%.

4.3. ECC-Based Authentication

In [45], ECC, symmetric keys, and biometrics were the key enablers for resultful authentication between drones and mobile devices on the ground via a public channel. As previously stated, ECC uses shorter keys and leads to minimum memory requirements and rapid arithmetic operations. Thus, ECC is ideal for devices with limited resources,

such as UAVs. After registering drones and devices with a central server, the drones were used for monitoring purposes of specific areas, whereas the users could acquire the data collected by the drones. An eCK adversary model [46] was adopted to simulate the potential threats. In addition, the performance of this method was formally tested using the ROM [43], and the results revealed that there was a balance between efficiency and security. Furthermore, the ECC with addition and multiplication operations was considered in [32] and an authentication scheme for Wireless Sensor Networks (WSNs), where the UAVs acted as mobile sinks, collecting data via sensors, was designed to mitigate security attacks (e.g., spoofing, key impersonation, replay, and password guessing). The performance evaluation underlined that this scheme decreased the time needed for system registration and also provided adequate protection against attacks with low computing costs. An authentication scheme for UAV-assisted ITS that leveraged Hyperelliptic Curve Cryptography (HECC) with an 80 bit key, a digital signature, and a hash function was presented in [47]. To implement and test this scheme, a 5G wireless backhaul network with multiaccess edge computing capabilities was considered, which consisted of UAVs equipped with sensors and onboard units (OBUs), multiple clustered roadside units (RSUs), as well as vehicles that forwarded event-driven messages to RSUs. Insecure communication links between network entities were assumed, and the DY model was exploited. First, formal security analysis was carried out, which was based on the ROR model, the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool, and the assumption of an active and a passive adversary. Informal and comparative security analysis was also conducted to highlight the superior performance of this scheme in terms of the computing and communication cost.

The certificateless-based and ECC-based SLPAKA (Secure Lightweight Proven Authenticated Key Agreement) authentication method, which can cope with the widely used Canetti–Krawczyk (CK) adversary model [48], was presented in [49]. In this model, a probabilistic polynomial adversary was considered that could totally affect the communication channel. Apart from the drones that were dynamically added, the IoD network consisted of the Trusted Authority Center (TAC) that facilitated the key generation, the MEC devices that assisted the drones during computation tasks, and the GCS. To implement SLPAKA and investigate its energy and computational efficiency, a python programming language was used. In this regard, the security was analyzed both informally and formally (via the ProVerif tool), and the advantages of SLPAKA were demonstrated. A certificateless pairing-free aggregate authentication scheme, called CLAS, with elliptic curves for the authentication between clusters of UAVs and the control center was proposed in [50]. In this scheme, the key escrow problem in key allocation could be avoided, while the certificate management could be overcome. It was assumed that the trusted Key Generation Center (KGC) was responsible for creating partial private keys for the UAVs, the aggregator, and the Command Center (CMC). The aggregator performed as a cluster head and aggregated the authentication responses, whereas the CMC verified these responses. In order to realistically model the malicious entities for this scheme, two types of threats were considered. The first extrinsic threat could only modify the public keys, whereas the second threat had the role of KGC and could acquire the master secret key. In [28], a network comprising a drone, a GCS, and a remote user was considered, and a user authentication protocol for IoD was presented. This protocol leveraged the ECC-based FourQ for better stability, enhanced efficiency, and lower required resources compared to conventional ECC schemes [51]. FourQ was collaboratively used with the Boyko–Peinado–Venkatesan (BPV) pre-calculation [52] for further performance improvement and a reduction in the number of elliptic curve group operations using discrete log and factoring. Using a Raspberry Pi 3B+, experimental results were obtained and depicted that this protocol improves the multiplication operation by about 4–5 times.

4.4. ML-Based Authentication

The authentication protocol proposed in [53] enabled the real-time identification of UAVs by studying their flying behavior and performing data processing. More specifically, this protocol modeled the behavior of trusted UAVs based on certain flying data (e.g., speed, latitude, and longitude) transmitted by the airborne black box to a big data management system server. In this regard, an online Bayesian learning method (i.e., Kalman filtering) was adopted to approve or decline the UAVs based on their legal or illegal behavior. Focusing on UAV-based IoT networks, the application of Federated Learning (FL) for UAV authentication was investigated in [54], where the UAVs locally and collaboratively trained the learning model. More specifically, an FL-based Deep Neural Network (DNN) architecture comprising four hidden layers was developed, capable of accepting or rejecting drones by learning the Radio Frequency (RF) features during signal transmission with Orthogonal Frequency-Division Multiplexing (OFDM) modulation. Among the various RF features, the symbol time, subcarrier spacing, Fast Fourier Transform (FFT) length, Cyclic Prefix (CP) length, detection, and signal power were included. In addition, the drones locally performed Stochastic Gradient Descent (SGD) optimization, whereas Homomorphic encryption ensured secured model parameters. The proposed authentication scheme was evaluated using an RF-based dataset from 3000 drones, and the results indicated that this scheme outperformed other ML-based schemes in terms of accuracy. In [55], an effective situational-aware authentication scheme for UAV swarm deployments was presented. It was considered that a legitimate cluster head (CH) should be selected among all candidate UAVs within a cluster. Since this selection procedure should be secure, the proposed scheme exploited edge intelligence and Linear Discriminant Analysis (LDA) to avert spoofing attacks. Application scenarios with unreliable communication links and a high degree of variability were considered in urban and rural environments, varying flying altitudes, and a different number of UAVs. Moreover, unique cross-layer attributes (e.g., Received Signal Strength Indication (RSSI), Packet Error Rate (PER), and latitude) were used to strengthen the authentication process and hinder possible attacks. In addition, results were provided to simulate the cross-layer attributes data and verify the accuracy and low computational overhead of this authentication scheme. In order to enhance intruder drone detection and optimize resource management, an ML-based Smart Drone Controller (SDC) framework was also proposed in [56]. By adaptively selecting the proper ML algorithm depending on the underlying scenario, this framework can facilitate the autonomous and collaborative operation of multiple Wi-Fi-connected commercial drones without requiring Visual Line-of-Sight (VLOS) connections. Overall, it is worth noting that the practical feasibility of ML solutions is directly based on the availability of an adequate number of sensor data and sufficient processing capabilities.

Table 2. Synopsis of recent research works on software-based authentication mechanisms for the IoD.

References	Key Technologies	Network Type	Threat Model	Security Analysis and Verification Tools	Benefits
Zhang et al., 2021 [28]	Elliptic-Curve Cryptography (ECC)-based FourQ	Typical IoD	Dolev-Yao (DY) model	Informal analysis	Low power consumption and execution efficiency
Jan et al., 2021 [30]	Hash functions	Flying Ad Hoc Network (FANET)	DY model	Random Oracle Model (ROM) and ProVerif	Low storage, computation and communication costs, and perfect forward secrecy
Cho et al., 2020 [31]	Public Key Infrastructure (PKI) and hash functions	Typical IoD	DY model	ProVerif	Execution efficiency, reduced traffic, and low computational overhead
Ever et al., 2020 [32]	ECC with addition and multiplication operations	Wireless Sensor Network (WSN)	Informal threat model	Informal analysis	Low computation cost

Table 2. *Cont.*

References	Key Technologies	Network Type	Threat Model	Security Analysis and Verification Tools	Benefits
Deebak et al., 2020 [35]	Chebyshev Chaotic-Maps and hash functions	UAV-based IoT	Informal threat model	Scyther and ROM	Robustness, low computation cost, and low energy consumption
Hu et al., 2021 [37]	Hash functions	Large-scale UAV swarm	Informal threat model	Informal analysis	Increased throughput and decreased delay
Tanveer et al., 2020 [38]	AEGIS, hash functions, and exclusive-OR (XOR) operations	Typical IoD	DY model	Informal analysis, Burrows–Abadi–Needham (BAN) logic and Scyther	Low computation and communication overhead, enhanced security functionalities
Cabuk et al., 2021 [41]	Context information and (conditionally) hash functions	FANET	Extended DY model	Informal analysis and Scyther	Extra layer of security and increased obscurity
Jan et al., 2021 [42]	Hash functions	IoD for military scenarios	Informal threat model	Informal analysis, ROM, Real-Or-Random (ROR), and ProVerif	Low complexity and low communication and computation costs
Jan et al., 2021 [43]	PKI and hash functions	Typical IoD	Informal threat model	ROR and ProVerif	Robustness and efficiency
de Melo et al., 2021 [44]	PKI and position verification	FANET	Informal threat model	Informal analysis	High detection accuracy and acceptable overhead
Hussain et al., 2021 [45]	ECC	Typical IoD	eCK adversary model	Informal analysis and ROM	Trade-off between security and efficiency
Khan et al., 2021 [47]	Hyperelliptic Curve Cryptography (HECC)	UAV-enabled Intelligent Transportation Systems (ITS)	DY model	Informal analysis, ROR, and AVISPA	Low computation and communication costs, small key size, and enhanced secrecy
Yahuza et al., 2021 [49]	ECC and Mobile Edge Computing (MEC)	Typical IoD	Canetti–Krawczyk (CK) model	Informal analysis and ProVerif	Low energy consumption, low computation and communication costs
Li et al., 2021 [50]	Certificateless ECC	UAV-based network	Informal threat model	Informal analysis	Unforgeability and practical efficiency
Jiang et al., 2020 [53]	Kalman filter	UAV-based network	-	Informal analysis	Good accuracy and low modeling complexity
Yazdinejad et al., 2021 [54]	Federated Learning (FL) and Deep Neural Network (DNN)	UAV-based IoT	Informal threat model	Informal analysis	High accuracy
Wang et al., 2021 [55]	Edge intelligence and Linear Discriminant Analysis (LDA)	UAV swarm	Informal threat model	Informal analysis	Accuracy and low computational overhead
Veerappan et al., 2022 [56]	ML	UAV swarm	-	-	Intruder drone detection
Gai et al., 2021 [57]	Blockchain	UAV-based network	Informal threat model	Informal analysis	Secure Peer-to-Peer (P2P) links and efficiency
Bera et al., 2021 [58]	ECC, hash functions, Blockchain, AI, big data analytics	Typical IoD	DY and CK models	Informal analysis, ROR, and AVISPA	Low communication and computation overhead, robustness

4.5. Blockchain-Based Authentication

The simultaneous authentication of multiple entities in UAV-based networks was addressed in [57], and a Blockchain-enabled Trustworthy UAV Network (BT-UAVN) was demonstrated that relied on attribute-based voting. In the BT-UAVN, the Blockchain could record and manage the transactions for the oncoming analysis of vulnerabilities. First, blocks were built to validate point-to-point data transfer between UAVs as well as between UAVs and the controller platform, and the required data was obtained using specialized

sensors. Then, the voter was hierarchically classified to obtain distinct attributes (i.e., properties) of the UAVs and verify the identity of each UAV. Apart from the simulations, real-world, hands-on experimentation evaluated the security of the BT-UAVN and two attack scenarios were studied, including those related with the facilities and those associated with the communication channel. Additionally, a Blockchain-based method, called ACSUD-IoD (Access Control Scheme for Unauthorized UAV Detection and mitigation in an IoD environment) was proposed in [58] to enable the detection of non-eligible UAVs. An IoD system was considered, where mutual authentication between the GCS and the UAVs was requisite and the decision-making process was aided by AI-inspired big data analytics. In this respect, a private Blockchain was used to record both the trusted and potentially untrusted data via the Practical Byzentine Fault Tolerance (PBFT) [59] by the following voting events. The Multiprecision Integer and Rational Arithmetic Cryptographic Library (MIRACL) [60], together with server and Raspberry PI 3 setups, were used to experimentally test and confirm the robustness of ACSUD-IoD against typical attacks.

5. Hardware-Based Authentication Mechanisms for the IoD

Beyond software-based authentication protocols for the IoD, recently, there have been various contributions towards hardware-based solutions, including TPM-based, HSM-based, and PUF-based implementations. Although TPMs and HSMs can create a secure and trusted environment to avoid unauthorized access, PUFs represent an alternative to key storage and software-generated bitstreams. In this section, relevant authentication schemes are discussed and synopsized in Table 3.

5.1. TPM-Based and HSM-Based Authentication

In [61], the ODOB (One Drone One Block) distributed network architecture was presented, which relies on a decoupled Blockchain-based framework. Compared with conventional Blockchain implementations, this framework intended to safeguard the network, minimize the computation and communication overhead of preserving the Blockchain, and also decrease the delay and storage requirements. An IoD scenario was considered that involved the aviation authority, the intermediate GSs acting as connection points, and the drones. Specifically, the aviation authority was charged with controlling the registration and access of drones to the permissioned blockchain. In addition, the drones were coupled with individual blocks and were equipped with TPM chips for secure identification. Each drone had a unique identity, which was assigned by combining the hash of the serial number and the onboard firmware. A Task-oriented Authentication Model (ToAM) for UAV-based networks which exploited Blockchain technology and PKI was also proposed in [62] to cope with weak connections and dynamic network topologies. In ToAM, TPM chips were embedded in the UAVs to provide protected data storage, and a chord ring was used to attain proper network operation under weak connections. In addition, the authentication procedure invoked two separate stages for group building authentication and intra-group authentication, while hash values stored in the Blockchain were used to represent the authentication information. The management of identity information and the registration of the network nodes was handled by the Certificate Authority (CA). Additionally, the Blockchain Authentication Server (BAS) acted as the master node that stored or queried the certificate information, while the Business Server published the task information. The performance analysis demonstrated that the ToAM provided sufficiently secure authentication of the UAVs with a notably low computation and communication cost.

By adopting PKI, HSMs, and the widely accepted TLS protocol, a reliable and globally operative cryptographic authentication system for commercial cellular-connected UAVs was presented in [63]. In this system, the UAV coordinates, which determined the placement of these UAVs in the airspace, were forwarded to a flight control server through a secure communication channel. The UAVs granted conditional permission to fly in the airspace, as soon as they were authenticated via X.509 certificates. This system ensured protected sensor

values, which were resilient against remote attacks and also achieved global availability and connectivity.

5.2. PUF-Based Authentication

In [26], a lightweight mutual authentication scheme for a software-defined UAV network (SDUAVN) was proposed, where the drones were equipped with PUF chips that generated CRPs. Specifically, the two-stage PUF-based Authentication for Remote Hovering Devices (PARTH) protocol was developed to establish two unique session keys, attain identity protection, and obtain mutual authentication in surveillance areas. In this direction, three layers with distinct network entities were considered, i.e., the GS, the mini drones with limited resources, and the powerful intermediate leader drones acting as relay network nodes. Since the mini drones were not able to directly communicate with the GS, which was the only trusted entity, the authentication process between the GS and the leader drone took place in the first stage. In addition, the second stage was related with the authentication between the leader drone and a mini drone. The performance of the PARTH protocol was investigated with regard to the computing cost, latency, and resilience against known threats. A performance comparison between this protocol and previously proposed advanced protocols was also included. Although there were no keys stored onboard the drones, the results indicated that the PARTH protocol is capable of countering drone tampering, replay, man-in-the-middle, and impersonation attacks. Moreover, an efficient two-stage authentication and key agreement protocol for three-layer, UAV-enabled networks was introduced in [27], where each of the network layers was associated with a specific entity, i.e., the member drones, the head drones, or the trusted GS. The member drones were employed to gather critical data and forward the required data to GSs via the intermediate head drones. PUF chips were embedded into UAVs to protect their privacy against adversaries and produce two session keys in one session. However, only hash and XOR operations were considered to reduce computation overhead and energy consumption. On the other hand, the key agreement between member drones and head drones, as well as the key agreement between head drones and GS, provided confidentiality and integrity. In order to ascertain the security of this protocol against various attack types (e.g., eavesdropping, tampering, replay, masquerading, and man-in-the-middle attacks), the DY threat model was exploited, and relevant simulation tools were used, including BAN logic, the ROR model, and the AVISPA tool. The simulation results underlined the feasibility and efficacy of this protocol in terms of the function properties, computing cost, and communication cost. To efficiently preserve privacy and handle the authentication process in the MEC-enabled IoD, while avoiding the use of volatile memory units to store cryptographic keys, a simple key agreement scheme was proposed in [64]. In this scheme, invasive and non-invasive attacks could be prevented, while minimum computing resources were required by exploiting PUFs and hash functions. In particular, an IoD consisting of multiple UAVs was considered. These UAVs used third-party edge devices susceptible to various threats (e.g., authentication, privacy, location, session-key security, and physical security threats). In this regard, the MEC operators could validate the legitimacy of a particular UAV owing to a double-PUF-based configuration at each UAV, where the first PUF was located in the memory unit and the second PUF was placed in the main control circuit. The results verified the superior performance of this authentication scheme in terms of the total authentication time for a varying number of UAVs.

Recently, the combination of the radio frequency identification (RFID) technology and PUFs was suggested for efficient real-time recognition and tracking of UAVs that embody RFID tags [65]. More specifically, a military application was considered, where the authentication of the UAVs was essential for secure operation in a certain airspace. In this respect, an interrogator or reader located on the ground scanned the tags to verify the credentials of the UAVs, whereas these UAVs employed a weak Static Random-Access Memory (SRAM) PUF capable of performing device-intrinsic fingerprint generation. In order to attain a minimum computational complexity while avoiding man-in-the-middle

attacks and eavesdropping, a SRAM PUF-based authentication protocol was proposed. In this protocol, the analysis of the security and privacy was based on Ouafi and Phan's security model [66]. The performance evaluation results showed that this protocol outperforms other RFID-based and PUF-based authentication protocols, whereas it is a viable security solution for UAV-enabled scenarios. In addition, a WSN with multiple dispersed nodes with sensors in specific locations of a remote and inaccessible area (e.g., a battlefield or a dense forest area) was considered in [67]. In this WSN, a UAV was employed to gather data from the nodes. In order to generate unique responses for specific challenges, the nodes took advantage of delay-based arbiter PUF circuits that traded on the intrinsic properties of hardware and the delay difference of signal propagation paths. In this regard, CoMSeC++, a lightweight, PUF-based authentication protocol with hash functions was presented. This protocol enabled secure wireless connectivity between the sensors and the cloud via the UAV and included five separate phases: (a) pre-deployment of sensor nodes, (b) drone registration, (c) authentication and key-agreement, (d) user registration with cloud server, and (e) user login and authentication. The Scyther simulator was used to obtain indicative results and confirmed that this authentication protocol can prevent the impersonation and manipulation of private/sensitive information in the WSN by malicious attackers.

Although energy efficiency is a critical factor for practical IoD deployments, the majority of the authentication protocols reported in the literature have not considered the energy consumption of the network nodes. On the contrary, a lightweight identity security authentication protocol, namely Optimized Identity Authentication Protocol (ODIAP), for the IoD was presented in [68] and aimed to mitigate several security threats (e.g., impersonation and replay attacks) in an energy-efficient manner. This protocol included three separate operation phases (i.e., the initialization phase, the registration phase, and the authentication phase) and considered four network entities (i.e., the sensors, the drones, the access point, and the servers). Additionally, this protocol relied on the Chinese residual theorem to optimize the computing resources at the UAV nodes and convey complex computation tasks to powerful server nodes. Using the widely adopted ProVerif-based automated analysis tools for protocol verification, performance analysis results were provided and showed that ODIAP ensured adequate security. Furthermore, an authentication protocol that relies on PUFs was developed in [69], aiming to handle influential physical security challenges in monitoring, surveillance, and disaster management applications with UAV swarms and multiple stationary and trusted base stations (BSs). Based on this protocol, confidentiality was attained, whereas protection against DoS, replay attacks, man-in-the-middle attacks, impersonation attacks, and node-tampering attacks was obtained. Unlike other similar protocols, this protocol can enable the simultaneous authentication of multiple UAVs endowed with unique PUFs at the lowest possible computation time and communication cost by exploiting a spanning tree algorithm, while having a running time in order of $O(n)$, where n is the number of UAVs. In particular, this protocol facilitated authentication in dynamic multi-hop propagation scenarios with varying mobility and topology, including multi-UAV and UAV-to-BS communication links. Depending on the number of iterations of the execution of the algorithm, single or multiple attacks could be opposed.

Table 3. Synopsis of recent research works on hardware-based authentication mechanisms for the IoD.

References	Key Technologies	Network Type	Threat Model	Security Analysis and Verification Tools	Benefits
Alladi et al., 2020 [26]	PUF, SDN, and XOR operations	Multi-UAV surveillance network	Informal threat model	Mao and Boyd logic	Low computation latency and resiliency against known security attacks
Zhang et al., 2021 [27]	PUF, hash functions, and XOR operations	UAV-based network	DY model	Informal analysis, BAN logic, ROR, and AVISPA	Low computational complexity, efficiency, and resiliency against known security attacks

Table 3. *Cont.*

References	Key Technologies	Network Type	Threat Model	Security Analysis and Verification Tools	Benefits
Singh et al., 2020 [61]	Trusted Platform Module (TPM), Blockchain, hash functions, and XOR operations	Typical IoD	Informal threat model	Informal analysis	Flexibility, sufficient security, and low computation and communication overhead
Chen et al., 2020 [62]	TPM, Blockchain, PKI, and hash functions	UAV-based network	Informal threat model	Informal analysis	Flexibility, sufficient security, and low computation and communication costs
Pirker et al., 2021 [63]	Hardware Security Module (HSM), PKI, and Transport Layer Security (TLS)	UAV-based network	Informal threat model	Informal analysis	Sufficient security and standardized protocols
Gope et al., 2020 [64]	PUF, MEC, and hash functions	Typical IoD	Informal threat model	ROR	Low power consumption, low storage and communication costs, and execution efficiency
Gope et al., 2021 [65]	Static Random-Access Memory (SRAM) PUF and hash functions	Radio Frequency Identification (RFID)-enabled UAV network	Ouafi and Phan's model	Informal analysis	Efficiency and low computation overhead
Mall et al., 2021 [67]	Arbiter PUF, hash functions, and XOR operations	WSN	Informal threat model	Informal analysis and Scyther	Low computation and communication costs and energy efficiency
Lei et al., 2021 [68]	PUF, hash functions, and XOR operations	Typical IoD	DY model	Informal analysis and ProVerif	Sufficient security and optimized utilization of computing resources
Bansal et al., 2021 [69]	PUF and spanning tree algorithm	UAV swarm	DY model	Mao and Boyd logic	Low computation time and low communication cost
Alladi et al., 2020 [70]	PUF, hash functions, and XOR operations	UAV-to-ground and UAV-to-UAV networks	Informal threat model	Informal analysis and Mao and Boyd logic	Sufficient security and efficiency and satisfactory computation, communication, and storage costs
Alladi et al., 2021 [71]	PUF, hash functions, and XOR operations	UAV-based 5G mobile backhaul network	Informal threat model	Informal analysis	Sufficient security and low computation time
Pu et al., 2020 [72]	PUF and chaotic system	UAV-based network	Informal threat model	Informal analysis	Low computation cost and low energy consumption
Pal et al., 2020 [73]	ARM's TrustZone technology and Ring Oscillator (RO) PUF	UAV-based network	Informal threat model	Informal analysis	Sufficient security and scalability
Ionescu et al., 2020 [74]	Memristor-based PUF	UAV-based network	-	-	Affordable production cost and high performance
Bansal et al., 2021 [75]	PUF and K-Means clustering algorithm	UAV swarm	DY model	Mao and Boyd logic	Sufficient security, scalability, low computational cost, and low authentication time

In [70], PUFs were used to strengthen the mutual authentication procedure in UAV-to-GS and inter-UAV connections, while keeping this procedure less demanding in terms of communication, computation, and storage requirements. In this regard, a lightweight protocol, entitled SecAuthUAV, was presented, and a wireless network was considered that consisted of a GS as well as legitimate and resource-constrained UAVs equipped with PUFs. By applying a 32 bit challenge, these PUFs could give a response of 320 bit with a

response time of 0.4 µs. In each session, this protocol aimed to generate unique secret keys and maintain mutual authentication, anonymity, and forward secrecy. Additionally, this protocol was resilient against typical security threats (e.g., masquerade, man-in-the-middle, replay attacks, cloning attacks, and physical attacks) and was able to trace any tampering attempt. A typical security analysis based on Mao and Boyd logic along with a traditional cryptanalysis were used to validate the powerful security features of SecAuthUAV. In addition, simulation results were provided to ascertain the performance of this authentication protocol in NodeMCUv3.0 and Raspberry Pi 3B simulation environments, when several mathematical and cryptographic operations (e.g., XOR, pseudo-random number generation (PRNG), and hash functions) were carried out. In [71], Drone-MAP, a mutual authentication protocol for 5G UAV-aided backhaul networks, was proposed to avoid common security attacks (e.g., eavesdropping, impersonation, and replay attacks). The goal of this protocol was to establish secure sessions and meet the confidentiality and untraceability requirements in communication scenarios with a single BS and multiple UAVs. This protocol could also avert unauthorized access without exploiting PKI or ECC encryption. In this respect, this protocol generated unique secret keys via PUFs with 32 bit responses and 32 bit challenges. Thus, no typical memory units were necessary to store sensitive data. A Raspberry Pi 3B was used to implement Drone-MAP, and a security analysis was provided along with performance results to reveal the benefits of this protocol with regard to computation time. Moreover, PCAP, an energy-efficient and computation-efficient mutual authentication protocol for secure UAV-to-GS communication links, was proposed in [72]. PCAP was related with a PUF unit and a chaotic system with non-linear behavior. More importantly, the CRP of the PUF initialized the chaotic system that was highly sensitive to initial conditions and could be used as a PRNG to facilitate the generation of the secret session key. In this regard, a series of event driven simulations based on OMNeT++ were conducted in a 150×150 m^2 square network region and demonstrated that PCAP could effectively distinguish legitimate and malicious UAVs and clearly outperformed traditional cryptographic methods without high computational and energy demands. In addition, a Trusted Execution Environment (TEE) was developed in [73] using ARM's TrustZone technology and drones with built-in field-programmable gate array (FPGA)-based Ring Oscillator (RO) PUFs as digital fingerprints of an onboard companion computer, LIght Detection and Ranging (LiDAR) sensors, and a flight controller. In order to demonstrate the two-phase (i.e., the enrollment phase and the device authentication phase) authentication procedure, a RaspberryPi, a Pixhawk2, and a LiDAR Lite V3 by Garmin were used as companion computer, flight controller, and LiDAR sensor, respectively. Additionally, a Cmod A7 FPGA board was selected to implement the RO PUFs, which supported 8 bit challenges and 8 bit responses.

In the context of PUFs, memristors have recently been proposed as effective entropy sources for IoD scenarios. Memristors represent non-volatile electronic memory devices that hold a memory in the form of programmable resistance and ensure more compact cell size than typical Complementary Metal–Oxide–Semiconductor (CMOS) implementations. Memristor-based PUFs maintain an internal resistive state that relies on previously applied current and voltage values and exploit not only the process variations, but also the intrinsic randomness. Although this type of PUF is less susceptible to several physical attacks, e.g., microprobing and photoelectric attacks, it suffers from certain reliability issues (e.g., stability, retention loss, and thermal variation). In [74], a cost-effective and non-intrusive hardware-based authentication mechanism for drones was proposed, where PUF units based on a "twins" memristors deployment were placed on the UAV and the GS. In this direction, the current or the resistance of the memristors was used as the response of the PUFs. Beyond one-to-one authentication, a scalable authentication protocol for UAV-to-BS communications that leverages the *K*-Means clustering algorithm and the efficacy of PUF chips was introduced in [75]. Since the position of the UAVs dynamically changes, multiple clusters for different distances between UAVs and BSs could be formed using the clustering algorithm. By transmitting the messages to proximate UAVs in a specific cluster, the flow of

protocol messages was designated, whereas the entire propagation time and propagation distance decreased. As the UAVs were vulnerable to security attacks, an onboard computer that integrated PUF-based digital fingerprints was installed on each UAV to realize the identification procedure via a CRP check. In the simulation setup, the BS was placed at the center of the region. In addition, 100 randomly deployed UAVs were considered, and their operations were performed using a Raspberry Pi 3B device. The simulation results indicated that the proposed authentication protocol could surpass other protocols with respect to the total authentication time. Overall, based on the existing authentication schemes described in Sections 4 and 5, a classification of these schemes can be defined in the IoD. This classification is illustrated in Figure 4.

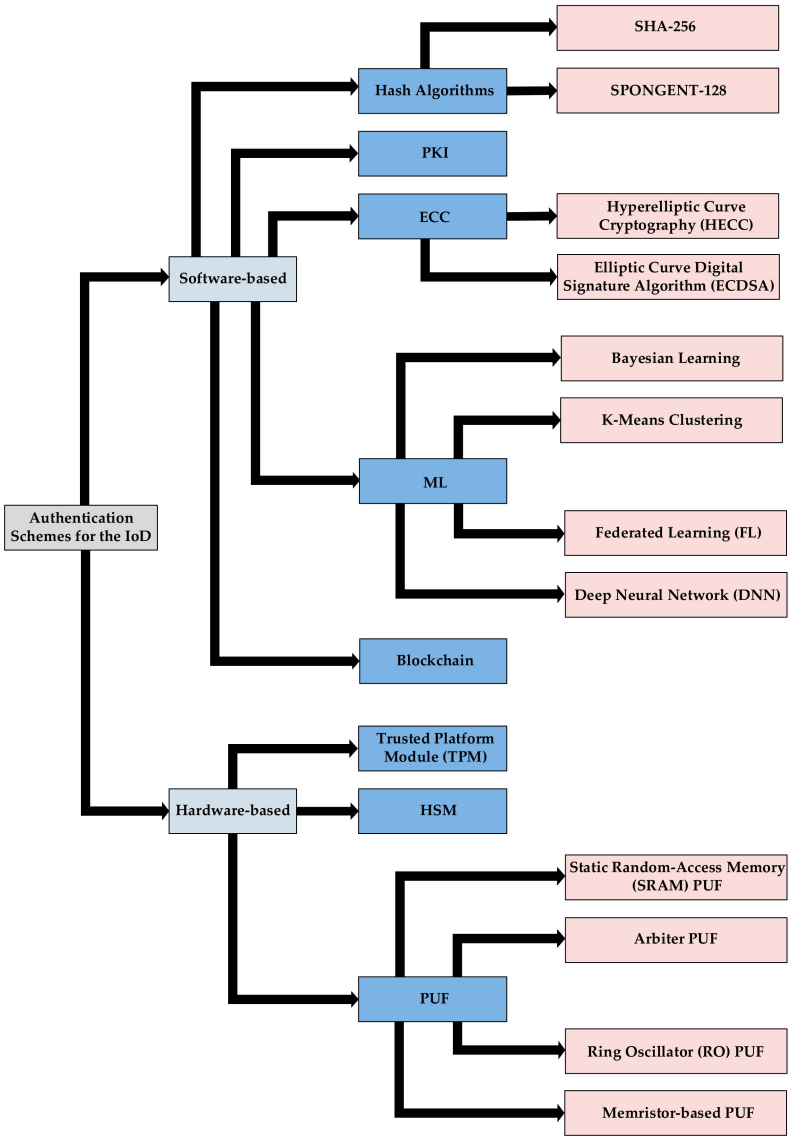

Figure 4. Classification of the recently proposed authentication schemes for the IoD.

6. Conclusions and Future Research Directions

6.1. Conclusions

As drones will be integrated as flying things in IoD networks, several possibilities for novel applications and services are envisioned in the forthcoming years. However, numerous security challenges and barriers exist that may prevent the IoD from maximizing its impact on industry and society. Although the authentication of network nodes is a

cornerstone for future IoD deployments, the use of complex cryptographic methods may be severely restricted in scenarios where drones have limited onboard processing resources and limited battery capacity or where dedicated cloud/fog/edge computing infrastructures do not exist to facilitate the processing of large amounts of data. In this regard, the development of lightweight, software-based or hardware-based authentication mechanisms entailing lower complexity is expected to give great impetus to the establishment and evolution of the IoD ecosystem.

This paper aimed to provide a convenient framework for the successful authentication of network nodes through the IoD. In this direction, this paper initially provided a discussion and comparison of relevant review and survey papers. Then, this paper outlined current trends on node authentication for the IoD. Moreover, this paper presented an extensive overview and classification of recently proposed software-based authentication methods with low computing requirements. In addition, this paper reviewed hardware-based implementations of authentication solutions that leverage TPMs, HSMs, or PUFs. To this end, the major outcomes of this paper can be summarized as follows:

- A trade-off between security and performance should be obtained in practical IoD implementations.
- The communication, computation, and storage costs, as well as the energy consumption represent primal performance metrics for various authentication schemes.
- Traditional cryptographic techniques, such as hash functions, PKI, and ECC, can be used to mitigate malicious attacks.
- ML-based methods have opened up new opportunities for safeguarding security and distinguishing legitimate and malicious nodes under dynamic and complex IoD scenarios. Although ML algorithms usually require significant computing power, running these algorithms on the cloud drastically increases the response and efficiency of the IoD system.
- Blockchain technology can provide an extra layer of security in a distributed manner.
- Although the performance of conventional hardware-based authentication solutions based on TPMs or HSMs is satisfactory, the role of PUFs in providing robust, cost-effective, and feasible authentication solutions for the IoV is significant.
- Hybrid authentication strategies that combine diverse techniques can enhance the security level and build scalable IoV network architectures.

6.2. Future Research Directions

Aiming to foster further developments in this research field, several critical aspects of IoD should be taken into account in future work as follows:

- Newer authentication strategies for decentralized scenarios should be proposed. Additionally, the dynamic distribution of IoD nodes and the mobility of drones during secure data exchange should be considered in upcoming authentication schemes.
- As far as vast amounts of data from multiple sources are available for training, the implementation of smart IoD authentication models with more complex ML approaches is suggested, such as Convolutional Neural Networks (CNNs) that facilitate vision-based object detection and the tracking of a target drone by analyzing visual imagery.
- Future work could be devoted to the upcoming field of quantum-based cryptography that intends to replace the public key cryptosystems.
- The development of more sophisticated hybrid authentication schemes (e.g., Blockchain-based and SDN-based hybrid schemes for robustness and scalability or chaos-based and quantum-based hybrid schemes for enhanced security) along with traditional cryptography schemes is another upcoming research topic in the IoD, which needs critical attention.
- The CRP behavior of different types of PUFs in various environmental and physical conditions should be more extensively studied to minimize possible faults during authentication.

- Finally, small-scale, realistic experimental testbeds that use different types of drones and adversaries for the same experiments are necessary to validate the hitherto theoretical results.

Author Contributions: Conceptualization, E.T.M.; investigation, E.T.M.; methodology, E.T.M. and D.V.; supervision, D.V.; visualization, E.T.M.; writing—original draft, E.T.M.; writing—review and editing, E.T.M. and D.V. All authors have read and agreed to the published version of the manuscript.

Funding: This research is funded in the context of the research project "SafeIT: Wearable systems for the safety and wellbeing applied in security guards" co-financed by the European Regional Development Fund of the European Union and Greek national funds through the Operational Program "Competitiveness, Entrepreneurship and Innovation (EPAnEK) 2014–2020", under the call RESEARCH–CREATE–INNOVATE.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

5G	Fifth Generation
ACSUD-IoD	Access Control Scheme for Unauthorized UAV Detection and Mitigation in an IoD Environment
AES	Advanced Encryption Standard
AI	Artificial Intelligence
AKE	Authenticated Key Exchange
ANN	Artificial Neural Network
AVISPA	Automated Validation of Internet Security Protocols and Applications
BAN	Burrows–Abadi–Needham
BAS	Blockchain Authentication Server
BPV	Boyko–Peinado–Venkatesan
BS	Base Station
BT-UAVN	Blockchain-Enabled Trustworthy UAV Network
CA	Certificate Authority
CDHP	Computational Diffie–Hellman Problem
CH	Cluster Head
CK	Canetti–Krawczyk
CLAS	Certificateless Pairing-Free Aggregate Authentication Scheme
CMC	Command Center
CMOS	Complementary Metal–Oxide–Semiconductor
CNN	Convolutional Neural Networks
CoMAD	Context-Aware Mutual Authentication Protocol for Drone Networks
CP	Cyclic Prefix
CPUF	Controlled Physically Unclonable Function
CRP	Challenge–Response Pair
D-DoS	Distributed Denial of Service
DNN	Deep Neural Network
DoS	Denial-of-Service
DY	Dolev and Yao
ECC	Elliptic-Curve Cryptography
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECDSA	Elliptic Curve Digital Signature Algorithm
EEPROM	Electrically Erasable Programmable Read-only Memory
EK	Endorsement Key
FFT	Fast Fourier Transform
FL	Federated Learning
FPGA	Field-Programmable Gate Array
GCS	Ground Control Station
GS	Ground Station

HECC	Hyperelliptic Curve Cryptography
HMAC	Hash-based Message Authentication Code
HMASHA	Hash-based Message Authentication Code Secure Hash Algorithmic
HSM	Hardware Security Module
HT	Hardware Trojan
IC	Integrated Circuit
ID	Identity
IoD	Internet of Drones
IoT	Internet of Things
ITS	Intelligent Transportation Systems
KGC	Key Generation Center
LAKE-IoD	Lightweight AKE Protocol for IoD Environment
LDA	Linear Discriminant Analysis
LiDAR	LIght Detection And Ranging
L-PPS	Lightweight Privacy-Preserving Scheme
MAC	Message Authentication Code
MD	Message Digest
MEC	Mobile Edge Computing
MIRACL	Multiprecision Integer and Rational Arithmetic Cryptographic Library
ML	Machine Learning
OBU	Onboard Unit
ODIAP	Optimized Identity Authentication Protocol
ODOB	One Drone One Block
OFDM	Orthogonal Frequency-Division Multiplexing
P2P	Peer-to-Peer
PARTH	PUF based Authentication for Remote Hovering Devices
PBFT	Practical Byzentine Fault Tolerance
PBKDF2	Password-Based Key Derivation Function 2
PER	Packet Error Rate
PICS	Powerful Intelligence Computer System
PKI	Public Key Infrastructure
PLS	Physical Layer Security
PRNG	Pseudo-Random Number Generation
PUF	Physically Unclonable Function
ReRAM	Resistive Random-Access Memory
RF	Radio Frequency
RFID	Radio Frequency Identification
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
RO	Ring Oscillator
ROM	Random Oracle Model
ROR	Real-Or-Random
RPA	Remotely Piloted Aircraft
RPAS	Remotely Piloted Aircraft System
RSA	Rivest–Shamir–Adleman
RSSI	Received Signal Strength Indication
RSU	Roadside Unit
SDC	Smart Drone Controller
SDN	Software-Defined Networking
SDUAVN	Software-Defined UAV network
SENTINEL	Secure and Efficient autheNTIcation for uNmanned aErial vehicLes
SGD	Stochastic Gradient Descent
SHA	Secure Hash Algorithm
SLPAKA	Secure Lightweight Proven Authenticated Key Agreement
SRAM	Static Random-Access Memory
TAC	Trusted Authority Center
TEE	Trusted Execution Environment
TLS	Transport Layer Security

ToAM	Task-oriented Authentication Model
TPM	Trusted Platform Module
UAV	Unmanned Aerial Vehicle
VLOS	Visual Line-of-Sight
WSN	Wireless Sensor Network
XOR	Exclusive-OR

References

1. Abualigah, L.; Diabat, A.; Sumari, P.; Gandomi, A.H. Applications, Deployments, and Integration of Internet of Drones (IoD): A Review. *IEEE Sens. J.* **2021**, *21*, 25532–25546. [CrossRef]
2. Abdelmaboud, A. The Internet of Drones: Requirements, Taxonomy, Recent Advances, and Challenges of Research Trends. *Sensors* **2021**, *21*, 5718. [CrossRef] [PubMed]
3. Michailidis, E.T.; Potirakis, S.M.; Kanatas, A.G. AI-Inspired Non-Terrestrial Networks for IIoT: Review on Enabling Technologies and Applications. *IoT* **2020**, *1*, 21–48. [CrossRef]
4. Tan, Z.; Qu, H.; Zhao, J.; Zhou, S.; Wang, W. UAV-Aided Edge/Fog Computing in Smart IoT Community for Social Augmented Reality. *IEEE Internet Things J.* **2020**, *7*, 4872–4884. [CrossRef]
5. Michailidis, E.T.; Miridakis, N.I.; Michalas, A.; Skondras, E.; Vergados, D.J. Energy Optimization in Dual-RIS UAV-Aided MEC-Enabled Internet of Vehicles. *Sensors* **2021**, *21*, 4392. [CrossRef] [PubMed]
6. Bithas, P.S.; Michailidis, E.T.; Nomikos, N.; Vouyioukas, D.; Kanatas, A.G. A Survey on Machine-Learning Techniques for UAV-Based Communications. *Sensors* **2019**, *19*, 5170. [CrossRef]
7. Mehta, P.; Gupta, R.; Tanwar, S. Blockchain envisioned UAV networks: Challenges, solutions, and comparisons. *Comput. Commun.* **2020**, *151*, 518–538. [CrossRef]
8. Skondras, E.; Michailidis, E.T.; Michalas, A.; Vergados, D.J.; Miridakis, N.I.; Vergados, D.D. A Network Slicing Framework for UAV-Aided Vehicular Networks. *Drones* **2021**, *5*, 70. [CrossRef]
9. McCoy, J.; Rawat, D.B. Software-Defined Networking for Unmanned Aerial Vehicular Networking and Security: A Survey. *Electronics* **2019**, *8*, 1468. [CrossRef]
10. Nomikos, N.; Michailidis, E.T.; Trakadas, P.; Vouyioukas, D.; Karl, H.; Martrat, J.; Zahariadis, T.; Papadopoulos, K.; Voliotis, S. A UAV-based moving 5G RAN for massive connectivity of mobile users and IoT devices. *Veh. Commun.* **2020**, *25*, 100250. [CrossRef]
11. Yaacoub, J.-P.; Noura, H.; Salman, O.; Chehab, A. Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet Things* **2020**, *11*, 100218. [CrossRef]
12. Boccadoro, P.; Striccoli, D.; Grieco, L.A. An extensive survey on the Internet of Drones. *Ad Hoc Netw.* **2021**, *122*, 102600. [CrossRef]
13. Fotouhi, A.; Qiang, H.; Ding, M.; Hassan, M.; Giordano, L.G.; Garcia-Rodriguez, A.; Yuan, J. Survey on UAV Cellular Communications: Practical Aspects, Standardization Advancements, Regulation, and Security Challenges. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3417–3442. [CrossRef]
14. Shakeri, R.; Al-Garadi, M.A.; Badawy, A.; Mohamed, A.; Khattab, T.; Al-Ali, A.; Harras, K.A.; Guizani, M. Design challenges of multi-UAV systems in cyber-physical applications: A comprehensive survey, and future directions. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3340–3385. [CrossRef]
15. Aibin, M.; Aldiab, M.; Bhavsar, R.; Lodhra, J.; Reyes, M.; Rezaeian, F.; Saczuk, E.; Taer, M.; Taer, M. Survey of RPAS Autonomous Control Systems Using Artificial Intelligence. *IEEE Access* **2021**, *9*, 167580–167591. [CrossRef]
16. Challita, U.; Ferdowsi, A.; Chen, M.; Saad, W. Machine learning for wireless connectivity and security of cellular-connected UAVs. *IEEE Wirel. Commun.* **2019**, *26*, 28–35. [CrossRef]
17. Altawy, R.; Youssef, A.M. Security, Privacy, and Safety Aspects of Civilian Drones: A Survey. *ACM Trans. Cyber-Phys. Syst.* **2017**, *1*, 1–25. [CrossRef]
18. Syed, F.; Gupta, S.K.; Hamood Alsamhi, S.; Rashid, M.; Liu, X. A survey on recent optimal techniques for securing unmanned aerial vehicles applications. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4133. [CrossRef]
19. Shafique, A.; Mehmood, A.; Elhadef, M. Survey of Security Protocols and Vulnerabilities in Unmanned Aerial Vehicles. *IEEE Access* **2021**, *9*, 46927–46948. [CrossRef]
20. Lagkas, T.; Argyriou, V.; Bibi, S.; Sarigiannidis, P. UAV IoT Framework Views and Challenges: Towards Protecting Drones as "Things". *Sensors* **2018**, *18*, 4015. [CrossRef]
21. Hassija, V.; Chamola, V.; Agrawal, A.; Goyal, A.; Luong, N.C.; Niyato, D.; Yu, F.R.; Guizani, M. Fast, Reliable, and Secure Drone Communication: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2802–2832. [CrossRef]
22. Mekdad, Y.; Aris, A.; Babun, L.; Fergougui, A.E.; Conti, M.; Lazzeretti, R.; Uluagac, A.S. A Survey on Security and Privacy Issues of UAVs. *arXiv* **2021**, arXiv:2109.14442v2.
23. Sidhu, S.; Mohd, B.J.; Hayajneh, T. Hardware Security in IoT Devices with Emphasis on Hardware Trojans. *J. Sens. Actuator Netw.* **2019**, *8*, 42. [CrossRef]
24. Shamsoshoara, A.; Korenda, A.; Afghah, F.; Zeadally, S. A survey on physical unclonable function (PUF)-based security solutions for Internet of Things. *Comput. Netw.* **2020**, *183*, 107593. [CrossRef]

25. Michailidis, E.T.; Kogias, D.G.; Voyiatzis, I. A Review on Hardware Security Countermeasures for IoT: Emerging Mechanisms and Machine Learning Solutions. In Proceedings of the 24th Pan-Hellenic Conference on Informatics (PCI), Athens, Greece, 20–22 November 2020; pp. 268–271. [CrossRef]
26. Alladi, T.; Chamola, V.; Naren; Kumar, N. PARTH: A two-stage lightweight mutual authentication protocol for UAV surveillance networks. *Comput. Commun.* **2020**, *160*, 81–90. [CrossRef]
27. Zhang, L.; Xu, J.; Obaidat, M.S.; Li, X.; Vijayakumar, P. A PUF-based lightweight authentication and key agreement protocol for smart UAV networks. *IET Commun.* **2021**, 1–18. [CrossRef]
28. Zhang, N.; Jiang, Q.; Li, L.; Ma, X.; Ma, J. An efficient three-factor remote user authentication protocol based on BPV-FourQ for internet of drones. *Peer-to-Peer Netw. Appl.* **2021**, *14*, 3319–3332. [CrossRef]
29. Shoufan, A. Continuous authentication of UAV flight command data using behaviometrics. In Proceedings of the IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC), Abu Dhabi, United Arab Emirates, 23–25 October 2017; pp. 1–6. [CrossRef]
30. Jan, S.U.; Qayum, F.; Khan, H.U. Design and Analysis of Lightweight Authentication Protocol for Securing IoD. *IEEE Access* **2021**, *9*, 69287–69306. [CrossRef]
31. Cho, G.; Cho, J.; Hyun, S.; Kim, H. SENTINEL: A Secure and Efficient Authentication Framework for Unmanned Aerial Vehicles. *Appl. Sci.* **2020**, *10*, 3149. [CrossRef]
32. Ever, Y.K. A secure authentication scheme framework for mobile-sinks used in the Internet of Drones applications. *Comput. Commun.* **2020**, *155*, 143–149. [CrossRef]
33. Barker, E.; Roginsky, A. *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*; Special Publication (NIST SP) 2015; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2015.
34. Bhunia, S.; Tehranipoor, M. *Hardware Security: A Hands-on Learning Approach*; Elsevier/Morgan Kaufmann: Cambridge, MA, USA, 2019. [CrossRef]
35. Deebak, B.D.; Al-Turjman, F. A smart lightweight privacy preservation scheme for IoT-based UAV communication systems. *Comput. Commun.* **2020**, *162*, 102–117. [CrossRef]
36. Abdalla, M.; Fouque, P.A.; Pointcheval, D. Password-based authenticated key exchange in the three-party setting. In Proceedings of the 8th International Workshop on Public Key Cryptography, Les Diablerets, Switzerland, 23–26 January 2005; Volume 3386, pp. 65–84. [CrossRef]
37. Hu, F.; Qian, H.; Liu, L. A Random Label and Lightweight Hash-Based Security Authentication Mechanism for a UAV Swarm. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 6653883. [CrossRef]
38. Tanveer, M.; Zahid, A.H.; Ahmad, M.; Baz, A.; Alhakami, H. LAKE-IoD: Lightweight Authenticated Key Exchange Protocol for the Internet of Drone Environment. *IEEE Access* **2020**, *8*, 155645–155659. [CrossRef]
39. Wu, H.; Preneel, B. AEGIS: A Fast Authenticated Encryption Algorithm. In *Selected Areas in Cryptography—SAC 2013, Proceedings of the International Conference on Selected Areas in Cryptography, Burnaby, BC, Canada, 14–16 August 2013*; Lange, T., Lauter, K., Lisoněk, P., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2013; Volume 8282. [CrossRef]
40. Dolev, D.; Yao, A.C.-C. On the security of public key protocols. *IEEE Trans. Inf. Theory* **1983**, *29*, 198–207. [CrossRef]
41. Cabuk, U.C.; Dalkilic, G.; Dagdeviren, O. CoMAD: Context-Aware Mutual Authentication Protocol for Drone Networks. *IEEE Access* **2021**, *9*, 78400–78414. [CrossRef]
42. Jan, S.U.; Khan, H.U. Identity and Aggregate Signature-Based Authentication Protocol for IoD Deployment Military Drone. *IEEE Access* **2021**, *9*, 130247–130263. [CrossRef]
43. Jan, S.U.; Abbasi, I.A.; Algarni, F. A Key Agreement Scheme for IoD Deployment Civilian Drone. *IEEE Access* **2021**, *9*, 149311–149321. [CrossRef]
44. De Melo, C.F.E.; e Silva, T.D.; Boeira, F.; Stocchero, J.M.; Vinel, A.; Asplund, M.; de Freitas, E.P. UAVouch: A Secure Identity and Location Validation Scheme for UAV-Networks. *IEEE Access* **2021**, *9*, 82930–82946. [CrossRef]
45. Hussain, S.; Chaudhry, S.A.; Alomari, O.A.; Alsharif, M.H.; Khan, M.K.; Kumar, N. Amassing the Security: An ECC-Based Authentication Scheme for Internet of Drones. *IEEE Syst. J.* **2021**, *15*, 4431–4438. [CrossRef]
46. LaMacchia, B.; Lauter, K.; Mityagin, A. Stronger Security of Authenticated Key Exchange. In *ProvSec 2007: Provable Security, Proceedings of the International Conference on Provable Security, Wollongong, NSW, Australia, 1–2 November 2007*; Susilo, W., Liu, J.K., Mu, Y., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2007; Volume 4784. [CrossRef]
47. Khan, M.A.; Ullah, I.; Alkhalifah, A.; Rehman, S.U.; Shah, J.A.; Uddin, I.I.; Alsharif, M.H.; Algarni, F. A Provable and Privacy-Preserving Authentication Scheme for UAV-Enabled Intelligent Transportation Systems. *IEEE Trans. Ind. Inform.* **2021**, *18*, 3416–3425. [CrossRef]
48. Canetti, R.; Krawczyk, H. Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels. In *EUROCRYPT 2001: Advances in Cryptology, Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, 15–19 May 2001*; Pfitzmann, B., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2001; Volume 2045. [CrossRef]
49. Yahuza, M.; Idris, M.Y.I.; Wahab, A.W.A.; Nandy, T.; Ahmedy, I.B.; Ramli, R. An Edge Assisted Secure Lightweight Authentication Technique for Safe Communication on the Internet of Drones Network. *IEEE Access* **2021**, *9*, 31420–31440. [CrossRef]
50. Li, J.; Wang, J.; Ding, Y.; Wu, W.; Li, C.; Wang, H. A Certificateless Pairing-Free Authentication Scheme for Unmanned Aerial Vehicle Networks. *Secur. Commun. Netw.* **2021**, *2021*, 9463606. [CrossRef]

51. Costello, C.; Longa, P. FourQ: Four-dimensional decompositions on a Q-curve over theMersenne prime. In *ASIACRYPT 2015: Advances in Cryptology, Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, 29 November–3 December 2015*; Iwata, T., Cheon, J.H., Eds.; Springer: Berlin/Heidelberg, Germany, 2015; pp. 214–235. [CrossRef]
52. Boyko, V.; Peinado, M.; Venkatesan, R. Speeding up discrete log and factoring based schemes via precomputations. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Espoo, Finland, 31 May–4 June 1998; Springer: Berlin/Heidelberg, Germany, 1998; pp. 221–235. [CrossRef]
53. Jiang, C.; Fang, Y.; Zhao, P.; Panneerselvam, J. Intelligent UAV Identity Authentication and Safety Supervision Based on Behavior Modeling and Prediction. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6652–6662. [CrossRef]
54. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Karimipour, H. Federated learning for drone authentication. *Ad Hoc Netw.* **2021**, *120*, 102574. [CrossRef]
55. Wang, H.; Fang, H.; Wang, X. Safeguarding Cluster Heads in UAV Swarm Using Edge Intelligence: Linear Discriminant Analysis-Based Cross-Layer Authentication. *IEEE Open J. Commun. Soc.* **2021**, *2*, 1298–1309. [CrossRef]
56. Veerappan, C.S.; Loh, P.K.K.; Chennattu, R.J. Smart Drone Controller Framework—Toward an Internet of Drones. In *AI and IoT for Smart City Applications*; Piuri, V., Shaw, R.N., Ghosh, A., Islam, R., Eds.; Studies in Computational Intelligence; Springer: Singapore, 2022; Volume 1002. [CrossRef]
57. Gai, K.; Wu, Y.; Zhu, L.; Choo, K.-K.R.; Xiao, B. Blockchain-Enabled Trustworthy Group Communications in UAV Networks. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 4118–4130. [CrossRef]
58. Bera, B.; Das, A.K.; Sutrala, A.K. Private blockchain-based access control mechanism for unauthorized UAV detection and mitigation in Internet of Drones environment. *Comput. Commun.* **2021**, *166*, 91–109. [CrossRef]
59. Castro, M.; Liskov, B. Practical byzantine fault tolerance and proactive recovery. *ACM Trans. Comput. Syst.* **2002**, *20*, 398–461. [CrossRef]
60. MIRACL Cryptographic SDK: Multiprecision Integer and Rational Arithmetic Cryptographic Library. 2020. Available online: https://github.com/miracl/MIRACL (accessed on 7 February 2021).
61. Pirker, D.; Fischer, T.; Lesjak, C.; Steger, C. Global and Secured UAV Authentication System based on Hardware-Security. In Proceedings of the 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), Oxford, UK, 13–16 April 2020; pp. 84–89. [CrossRef]
62. Singh, M.; Aujla, G.S.; Bali, R.S. ODOB: One Drone One Block-based Lightweight Blockchain Architecture for Internet of Drones. In Proceedings of the IEEE INFOCOM 2020—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 6–9 July 2020; pp. 249–254. [CrossRef]
63. Chen, A.; Peng, K.; Sha, Z.; Zhou, X.; Yang, Z.; Lu, G. ToAM: A task-oriented authentication model for UAVs based on blockchain. *EURASIP J. Wirel. Commun. Netw.* **2021**, *2021*, 166. [CrossRef]
64. Gope, P.; Sikdar, B. An Efficient Privacy-Preserving Authenticated Key Agreement Scheme for Edge-Assisted Internet of Drones. *IEEE Trans. Veh. Technol.* **2020**, *69*, 13621–13630. [CrossRef]
65. Gope, P.; Millwood, O.; Saxena, N. A provably secure authentication scheme for RFID-enabled UAV applications. *Comput. Commun.* **2021**, *166*, 19–25. [CrossRef]
66. Ouafi, K.; Phan, R.C.-W. Privacy of Recent RFID Authentication Protocols. In *ISPEC 2008: Information Security Practice and Experience, Proceedings of the International Conference on Information Security Practice and Experience, Sydney, NSW, Australia, 21–23 April 2008*; Chen, L., Mu, Y., Susilo, W., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2008; Volume 4991. [CrossRef]
67. Mall, P.; Amin, R.; Obaidat, M.S.; Hsiao, K.-F. CoMSeC++: PUF-based secured light-weight mutual authentication protocol for Drone-enabled WSN. *Comput. Netw.* **2021**, *199*, 108476. [CrossRef]
68. Lei, Y.; Zeng, L.; Li, Y.-X.; Wang, M.-X.; Qin, H. A Lightweight Authentication Protocol for UAV Networks Based on Security and Computational Resource Optimization. *IEEE Access* **2021**, *9*, 53769–53785. [CrossRef]
69. Bansal, G.; Sikdar, B. S-MAPS: Scalable Mutual Authentication Protocol for Dynamic UAV Swarms. *IEEE Trans. Veh. Technol.* **2021**, *70*, 12008–12100. [CrossRef]
70. Alladi, T.; Bansal, G.; Chamola, V.; Guizani, M. SecAuthUAV: A Novel Authentication Scheme for UAV-Ground Station and UAV-UAV Communication. *IEEE Trans. Veh. Technol.* **2020**, *69*, 15068–15077. [CrossRef]
71. Alladi, T.; Venkatesh, V.; Chamola, V.; Chaturvedi, N. Drone-MAP: A Novel Authentication Scheme for Drone-Assisted 5G Networks. In Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Vancouver, BC, Canada, 10–13 May 2021; pp. 1–6. [CrossRef]
72. Pu, C.; Li, Y. Lightweight Authentication Protocol for Unmanned Aerial Vehicles Using Physical Unclonable Function and Chaotic System. In Proceedings of the 2020 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN), Orlando, FL, USA, 13–15 July 2020; pp. 1–6. [CrossRef]
73. Pal, V.; Acharya, B.S.; Shrivastav, S.; Saha, S.; Joglekar, A.; Amrutur, B. PUF Based Secure Framework for Hardware and Software Security of Drones. In Proceedings of the 2020 Asian Hardware Oriented Security and Trust Symposium (AsianHOST), Kolkata, India, 15–17 December 2020; pp. 1–6. [CrossRef]

74. Ionescu, O.; Besleaga, C.; Dumitru, V.; Pricop, E. UAV identification system based on memristor physical unclonable functions. In Proceedings of the 12th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Bucharest, Romania, 25–27 June 2020; pp. 1–4. [CrossRef]
75. Bansal, G.; Sikdar, B. Location Aware Clustering: Scalable Authentication Protocol for UAV Swarms. *IEEE Netw. Lett.* **2021**, *3*, 177–180. [CrossRef]