A survey on cryptographic methods to secure communications for UAV traffic management

Ridwane Aissaoui, Jean-Christophe Deneuville, Christophe Guerber, Alain Pirovano

Version of Record: https://www.sciencedirect.com/science/article/pii/S2214209623000918
Manuscript_068e0dd9a1275b57d435e328ab2eb542

A survey on cryptographic methods to secure communications for UAV traffic management

Ridwane Aissaoui Jean-Christophe Deneuville

Christophe Guerber Alain Pirovano

ENAC, French Civil Aviation University, Toulouse, France

<first.last@enac.fr>

February 28, 2023

Abstract

Unmanned Aerial Systems (UAS) have a wide variety of applications, and their development in terms of capabilities is continuously evolving. Many missions performed by an Unmanned Aerial Vehicle (UAV) require flying in public airspace. This requires very high safety standards, similar to those mandatory in commercial civil aviation. A safe UAV Traffic Management (UTM) requires several communication links between aircraft, their pilots, and UTM systems. The integrity of these communication links is critical for the safety of operations. Several security requirements also have to be met on each of these links. Unfortunately, current cryptographic standards used over the internet are often unsuitable for UAS due to the limited resources and dynamic nature of UAVs. This survey discusses the security required for every communication link to enable safe traffic management. Research works focusing on the security of communication links using cryptographic primitives are then presented and discussed. Authentication protocols developed for UAVs or other constrained systems are compared and evaluated as solutions for UAS security. Symmetrical alternatives to the AES algorithm are also presented. Works to secure current UTM protocols such as ADS-B and RemoteID are discussed. The analysis reveals a need for the development of a complete security architecture able to provide authentication and integrity to external systems (other aircraft, UTM systems...).

Keywords: UAV, Drone, UAS, UTM, CNS, Information Security, Cryptography, Authentication, Safety, ADS-B, RemoteID, IoD

1 Introduction

1.1 Unmanned aerial systems applications and traffic management

The most common application for a civil UAV in 2022 is recreational use. However, they have proven to be critical in operations that humans cannot carry out in a safe and time-efficient manner [1]. The number of UAVs around the world grows by 13% each year, and a lot of research focuses on improving their operating capabilities. Their performance is continuously improving and they are the best solution for a growing number of applications. They are currently the most relevant and cost-efficient solution for infrastructure monitoring, area scanning, urgent delivery services, and other applications. They can also be used for agriculture by monitoring and spraying the fields, for transport to help limit the congestion in city centers, for the surveillance of areas where security cameras are unusable or more expensive, for telecommunication purposes, and for media and entertainment as cheap aerial cameras or to create new shows. They also can play a major role in smart cities and be used in Internet of Things (IoT) systems or Wireless Sensor Network (WSN) [2].

A UAS consists of all the components used to operate a UAV and its communication means. In its simplest form, a UAS comprises a UAV and a GCS, but advanced systems can include additional actors such as UTM systems and intermediate ground stations for managing communication between different UAVs and end users. Due to the characteristics of UAS, most communication links are wireless. As illustrated in Figure 2, a UAS has three main communication axes. First, there are links between any UAV and a Ground Control Station (GCS) through which command, telemetry, video, and other mission-specific data are transmitted. These links can be physically or logically separated as these different types of data are not always sent on the same channel. The second axis is between a UAS and the UTM systems when flying in controlled airspace. Telemetry information is sent from the UAV or the GCS to the UTM systems for monitoring traffic and organizing airspace. In turn, the UTM systems broadcast emergency geofencing zones and, depending on their level of authority, send trajectory suggestions or direct trajectory modifications to a specific UAV or GCS. Finally, the third type of communication occurs between two UAVs. They can exchange environmental information or be used as routers to transmit data to a remote GCS or the UTM. The security goals will vary depending on the sensitivity of the information transmitted. This document reviews the literature to secure the transport layer through different cryptographic techniques to reach those security goals.

1.2 UAS security issues

In Europe, the regulatory framework strongly limits UAS operations. Most UAV operations require or gain from Beyond the Visual Line Of Sight (BVLOS) flights. This type of flight requires a sustained communication link between the GCS and the UAV, as the pilot has to be able to take control of the UAV at any time during its flight. Depending on the category of UAV as defined by the European Aviation Safety Agency (EASA), flights are more or less restricted. The open, specific, and certified categories separate UAVs by their characteristics, and are allowed to perform different civil risk level operations [3]. Drones in the open category are not allowed to perform BVLOS flights. The specific category

allows BVLOS flights up to 1 km (2 with airspace observers) and only for UAVs under 25kg [4]. These numbers are more restricted when flying over densely populated areas. This severely limits the operations. The certified category should broaden the limits but as the certification process is slow and rigorous, it will take time to complete for manufacturers. As most applications need to break these limits, each UAV used will need to be certified or the specific category will need to be modified. For information security, no rules have been announced by the EASA, and the Federal Aviation Administration (FAA) has been advised by the Aviation Rukemaking Committee (ARC) [5] to build a working group to address the issue.

UAS are highly susceptible to a variety of cyber threats, as they may contain sensitive or confidential data and transport high-value payloads such as medical supplies or high-end goods, which attackers could intercept if the UAS is compromised. In addition, the kinetic energy of UAS poses a significant physical threat to the public. As a result, it is crucial to safeguard UASs against cyber attacks, particularly those targeting their communication links, where most threats exist.

1.3 UTM safety and security

Operating UAS in populated areas requires compliance with a wide range of security standards, with communication security being critical. To enable safe operation in controlled airspace, UAS must be managed by UTM systems, which need to synchronize with existing Air Traffic Management (ATM) systems [6]. The exchange of sensitive and critical information between UAS and UTM systems necessitates secure communication. Numerous research works have addressed the importance of securing UAS communications. [7] details the importance of communication security in UAV networks. In [8], Shafique, Mehmood, and Elhadef show many UAV vulnerabilities that come from communications. Also, Sharma *et al.* investigate current methods of communications of UAVs and argue that their security features have to be improved in [9].

The International Civil Aviation Organization (ICAO) issued standard definitions for security and safety [10], as being:

> "*the state in which risks associated with aviation activities, related to, or in direct support of the operation of aircraft, are reduced and controlled to an acceptable level. Security aims to safeguard civil aviation against acts of unlawful interference. The objective is achieved by a combination of measures and human and material resources.*"

Despite being two separate notions in the regulatory framework, guaranteeing the safety of aerial operations is impossible without security measures. The "security for safety" concept has emerged to cover the security solutions involved in reaching safety objectives. In this paper, the term "safety" addresses this concept.

In [11], Barrado *et al.* emphasized that cybersecurity and encryption needs were issues to consider in the U-space architecture design. U-space is the UTM concept proposed in the Single European Sky ATM Research (SESAR) project roadmap. The main goal of the U-space design is to organize the safe integration of drones into all classes of European airspace.

Defending against cyber attacks requires significant computation power, memory space, bandwidth, sizeable software, or dedicated hardware. Such requirements are problematic for highly constrained systems like UAS, which pri-

oritize cost-efficiency. Defense mechanisms must be adapted and optimized for these systems. Information security in communication largely relies on cryptography, and specialized lightweight cryptographic primitives have been developed for constrained systems. These primitives aim to provide sufficient security properties while requiring lower performance.

1.4 Organization of the paper

The remainder of this survey is organized as follows: Section 2 provides an overview of the context of our study. Section 2.1 starts by presenting the types of UAVs concerned by our survey and explains the constraints existing in smaller devices. Next, Section 2.2 explores the different types of UAS networks. The section then discusses the organization of UAS traffic management in 2.3). It explains how communications play a crucial role in ensuring the safe operation of drones, particularly in beyond visual line of sight (BVLOS) operations. It also discusses the security requirements necessary for safe BVLOS operations. Next, the section explains the choice of cryptography and transport layer security in 2.4 and proposes other survey works that review physical layer security. Then, subsection 2.5 provides an overview of the main principles of cryptography, including symmetric and asymmetric encryption, signature and certificates, and authenticated key exchange. The section also details advanced topics in information security, including post-quantum cryptography and lightweight cryptography, which have important implications for securing communications in UAS. Finally, part 2.6 addresses the security threats, goals, and requirements for UAS systems. It highlights the importance of securing the UAV-GCS link, as it is a common point of attack for attackers seeking to compromise the drone's control. It also discusses the importance of securing the UAV-UTM system link, which is essential for safe and efficient drone operations, and the UAV-UAV link, which is critical for enabling cooperation and coordination among multiple drones. The section evaluates the required security level for each aforementioned link from a UTM perspective.

Section 3 discusses vulnerabilities that affect the safety of UTM communication links. For each vulnerability the section describes the main principles of a possible attacks, then proceeds to present common mitigation techniques and countermeasures. Regarding Global Navigation Satellite Systems (GNSS), vulnerabilities are considered outside the communication means included in UTM systems and therefore omitted from the discussion. GNSS vulnerabilities and solutions are studied by the GPS, Galileo, and other GNSS developer teams.

Section 4 presents cryptographic methods suitable for usage in a UAS environment for two-way communications. The section discusses lightweight encryption solutions relevant to the UAS domain, as well as proposals for IoT sensors and other constrained devices. It compares several asymmetric encryption schemes (Section 4.2) in terms of performance and security level. It then discusses symmetric encryption schemes (Section 4.3) to complete a potential hybrid encryption scheme.

Section 5 focuses on security solutions for broadcast communications, including signature schemes. The section explores several cryptographic security solutions researched to add security to ADS-B-like messages, cellular networks, or RemoteID. These solutions help ensure secure and authenticated communication.

Finally, Section 6 discusses open issues and future research directions in UTM

security. Key challenges include the development of secure and efficient post-quantum cryptography algorithms, the design of effective signature schemes for broadcast communications, and the creation of general security architectures.

2 Context

2.1 Types of UAVs

UAVs are generally categorized by weight. The physical threat they pose to the public is largely dependent on the kinetic energy they hold when flying over populated areas. Larger UAVs embark powerful hardware, as the energy consumption, weight, and price of Central Processing Unit (CPU)s is negligible compared to the advantages they bring. These larger UAVs are able to use internet protocols to provide information security to their users. For small UAVs the use of smaller computational units is preferred for their better cost and energy efficiency. However, their lower performance is insufficient to support all the computation required by the security features of internet protocols. Similarly, the bandwidth of the communication links is also a limiting factor.

Category	Weight	Altitude	Range	Payload
Nano	< 0.2 kg	< 90 m	< 90 m	< 0.2 kg
Micro	< 2 kg	< 90 m	< 5 km	< 0.5 kg
Mini	< 20 kg	< 900 m	< 25 km	< 10 kg
Small	< 150 kg	< 1500 m	< 100 km	< 50 kg
Tactical	> 150 kg	> 1500 m	> 100 km	> 50 kg

Table 1: Drone categories as proposed in [12].

Only UAVs in the categories Mini and smaller in Table 1 are considered to be limited in performance. This survey focuses on civil applications using these smaller UAVs. These characteristics correspond to the open and part of the specific UAV categories of EASA regulations. The improvement of information security (plus operational safety and other security issues) is needed for drones in the open category to operate in different areas. These improvements will allow A1, A2, and A3 UAVs (as defined in Table 2) to operate over populated areas and in BVLOS.

UAS	Operation		Drone Operator/Pilot		
Max Weight	Subcategory	Operational Restrictions	Drone Operator Registration	Remote Pilot Competence	Remote Pilot Minimum Age
<250g	A1 (can also fly in subcategory A3)	- No flight expected over uninvolved people (if it happens, overflight should be minimized) - No flight over assemblies of people	No unless camera / sensor on board and the drone is not a toy	- No training Required	No minimum age
<500g			Yes	- Read carefully the user manual - Complete the training and pass the exam defined by your national competent authority or have a 'Proof of completion for online training' for A1/A3 'open' subcategory	16+
<2kg	A2 (can also fly in subcategory A3)	- No flying over uninvolved people - Keep a horizontal distance of 50 m from uninvolved people	Yes	- Read carefully the user manual - Complete the training and pass the exam defined by your national competent authority or have a 'remote pilot certificate of competency' for A2 'open' subcategory	16+
<25kg	A3	- Do not fly near or over people - Fly at least 150m away from residential, commercial or industrial areas	Yes	- Read carefully the user manual - Complete the training and pass the exam defined by your national competent authority or have a 'Proof of completion for online training' for A1/A3 'open' subcategory	16+

Table 2: EASA open category [13].

2.2 UAS networks

A UAS with multiple UAVs is organized as either a cellular network or a Flying Ad-Hoc Network (FANET). Ad-Hoc networks have specific security solutions that are adapted to their unique properties. The specific security requirements and early security solutions of Ad-Hoc networks are detailed in

[14]. A FANET is a specific Mobile Ad-Hoc Network (MANET) with very high node mobility and speed, a lower node density, and a specific mobility model [15]. Several research works propose specific communication architectures for FANETs, with slight variations compared to MANET solutions. [16] surveys these architectures.

A different variant of MANET is the Vehicular Ad-Hoc Network (VANET) which is less specific than the FANET. This type of network has been researched for security. [17] discusses the security challenges and cryptographic solutions within VANETs and authentication schemes are presented in [18].

The Internet of Vehicles is a proposed VANET architecture. [19] surveys specific security issues and solutions that come with it. Similarly, a popular proposition of a UAS control architecture is the Internet of Drones (IoD) proposed by Gharibi, Boutaba, and Waslander [20]. Its design aims to coordinate UAVs into controlled airspace. The IoD includes an UTM system using UAVs as aerial relays, thus building a FANET within the system (see Figure 1). The IoD bases its structure around network concepts from the Air Traffic Control (ATC), the cellular network, and the Internet.

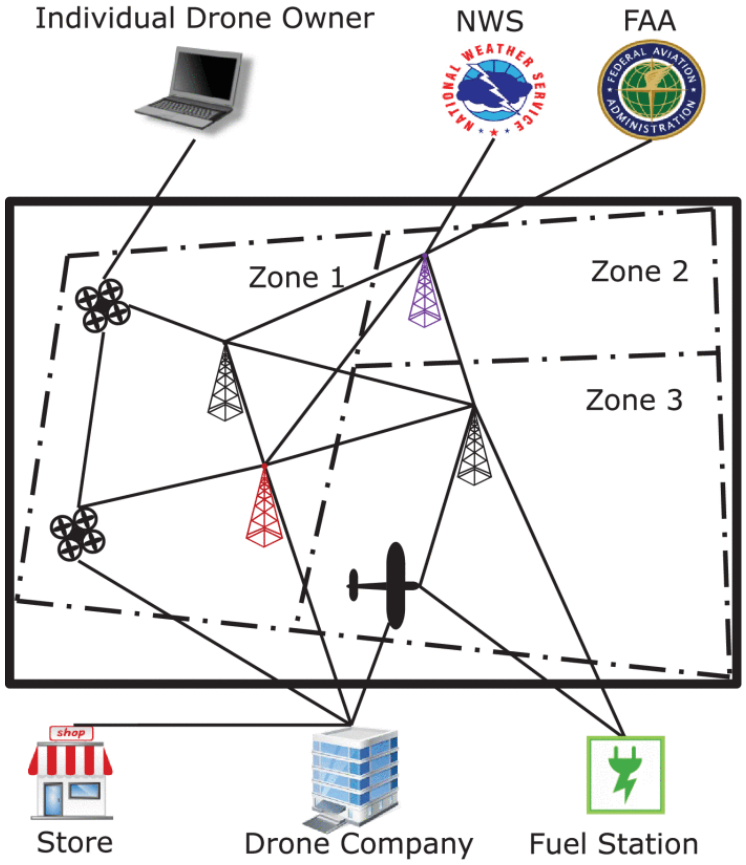

Figure 1: IoD architecture organization [20].

The IoD structure can support a large variety of applications such as smart city surveillance, WSN, business-to-business... [21]. However, the system lacks interoperability with ATM systems. In the IoD paradigm, UAS not in direct

communication with the ATC do not invade controlled airspace. ATC remains in charge of aircraft separation for both manned and unmanned systems [20].

2.3 UAS traffic management organization

In this survey, UTM is considered as defined by the ICAO framework [22]:

> "*UTM is a special aspect of air traffic management which manages UAS operations safely, economically and efficiently through the provision of facilities and a seamless set of services in collaboration with all parties and involving airborne and ground-based functions. The UTM system provides UTM through the collaborative integration of humans, information, technology, facilities and services, supported by air, ground or space-based Communications, Navigation and Surveillance (CNS).*"

In Figure 2, only the system providing the UTM flight control service is represented as it is the only part of the UTM system that communicates traffic management information with the UAS.

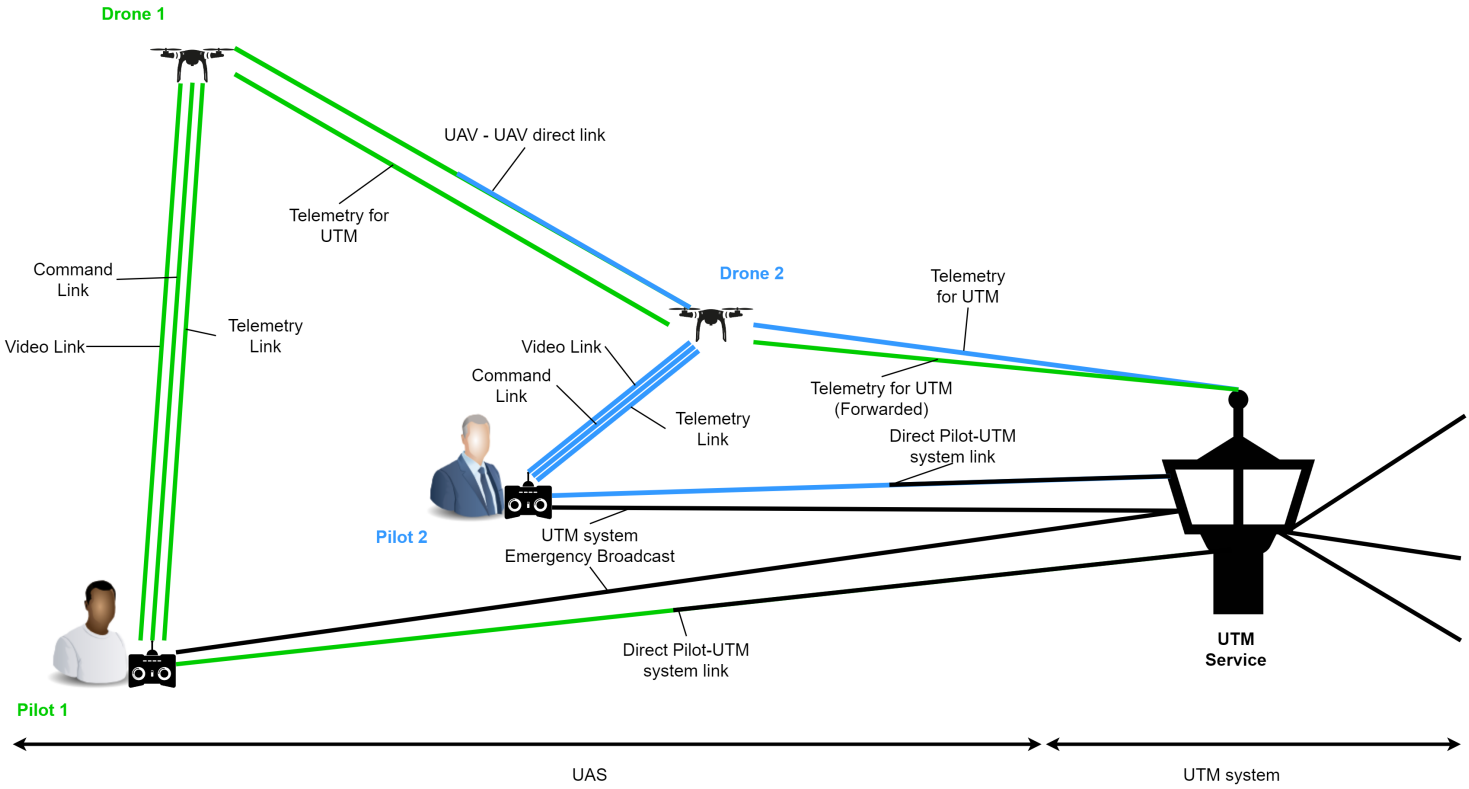

Figure 2: UAS with UTM system organization.

The ICAO states that UTM system information protocols and interfaces play a key role in the safe integration of UASs into public airspace. [22] precises that it is necessary to develop minimum performance and interoperability standards for communications protocols for :

- C2 Link between GCS and UAVs

- UAV to UAV communications
- Communications link between UAVs and other airspace users (e.g. manned aircraft), as necessary
- Communications between remote pilots/GCSs and the UTM and ATM systems.

One of the pillars of traffic management systems is the CNS concept. It includes the development of communication systems. These systems enable safe navigation for aircraft. And the traffic is observed by surveillance systems, to ensure safe operations.

This survey focuses on the security requirements for UASs communications to enable safe traffic management. BVLOS operations are used for security evaluation as they represent the focus point of UTM [6] research. This means that the video link is critical for UAV control, alongside the command link. Safe traffic management requires different levels of information security in case of :

- UTM system broadcast for emergency geofencing or modification of airspace organization requires authentication of the UTM system and integrity while keeping a high availability level.
- UTM system direct link to UAS (GCS or UAV) is used for real-time traffic control and is critical for safety as it modifies UAV paths. Authentication and integrity are needed.
- Commands from the GCS to the UAV require authentication and integrity.
- Video from the UAV to the GCS is critical for safe UAV control from the pilot. It has the same requirements as the command link.
- Telemetry from the UAV is transmitted to the GCS in its entirety and is used for the safe operation of the UAS. For BVLOS flights, this information is critical for the safety of the operation as it is important for the surveillance of the flight. It requires authentication and integrity.
- A subpart of telemetry data is broadcast from the UAV to neighboring UAVs (for detect and avoid systems) and to the UTM system for real-time traffic surveillance. Authentication and integrity are needed.

For each one of these links, confidentiality is a privacy concern and does not directly impact safety. However, providing confidentiality is recommended to address privacy issues when designing a new system. Moreover, a lack of confidentiality can indirectly impact system safety (*i.e.* intercepting a drone by anticipating its trajectory). The same reasoning holds for non-repudiation, which is a traceability issue. As it allows authorities to investigate past incidents, this property is necessary even though it does not directly impact air traffic safety. Authentication is provided through encryption; which also provides confidentiality; or through signature, which also provides non-repudiation. Confidentiality and non-repudiation are discussed when addressed by research works but are not considered as a prominent issue regarding UTM safety.

2.4 Security on different OSI layers

Security can be provided to different layers of the OSI model. Literature has extensively researched the topic of physical layer security for UAVs. However, the focus of this survey is traffic management safety. Therefore the sensitivity of the information transmitted determines the security requirements, which means the security features have to be different depending on the type of information transmitted. As different types of information can go through the same physical link, physical layer security cannot be applied as required due to its incapacity to discriminate data. It is thus considered out of the scope of this survey. For similar reasons, this survey does not investigate research on 5G security beyond, which does not discriminate data, and forces cellular communications as the communication mean. Regarding the physical layer security of UAVs, Sun *et al.* survey the various means of securing UAVs against eavesdropping in [23]. In [24], Wu, Mei, and Zhang explore trajectory design, resource allocation, and cooperative UAVs to fight against passive or active eavesdropping in UAV wireless communication systems. Finally, Wang, Zhang, and Jiang proposed an overview focused on cooperative protection of communications in [25].

Securing UAS communications for UTM safety requires data discrimination. Adding security on the transport layer is optimal, as it allows data discrimination and is independent of the physical mean of communication. Providing security to information is the role of cryptography, which is the focus of this survey.

Cryptography can also provide security on the application layer for mission-specific applications. Mission-specific information sensitivity heavily varies and does not impact UTM safety. Thus, application layer security is out of the scope of this document.

Security solutions designed for specific drone applications, like UAV edge computing and cognitive UAV relays, cannot be applied to UAS that do not support these applications. Such solutions cannot be used to secure UTM safety communications, as a large portion of the traffic would be unable to use the security solutions. Therefore, security solutions designed for specific application scenarios are excluded from the scope of our survey.

2.5 Cryptography for information security

2.5.1 Main principles

Information security revolves around three main concepts :

- Confidentiality ensures that no illegitimate user can access the information
- Integrity verifies that the information has not been modified during the lifetime of the data
- Availability is the property allowing legitimate use of the information

There are several ways to add security to a communication link. As the links are wireless and the network topology is dynamic in a UAS, it excludes the possibility of physically protecting the links. Using cryptography is the best way to secure a communication link with those specifications.

To ensure information security, cryptographic techniques have been researched since antiquity. The long history of cryptography has produced many proven solutions for information security. In cryptography, four properties ensure data security :

- Confidentiality ensures that only a legitimate user can access the information
- Integrity verifies that the information has not been modified during the lifetime of the data
- Authentication provides trust in the identity of the parties sharing information
- Non-Repudiation prevents the source of the information from denying being the source

If good practices and standards are correctly applied in the implementation of cryptographic methods, information can be theoretically confidential, authenticated, non-repudiable, and its integrity ensured. The Kerckhoff principle states that the security of a scheme should only rely on the secrecy of a randomly chosen parameter (called a key) rather than on the secrecy of the algorithm. Actually, all the algorithms of the scheme should be public, and only the knowledge of the secret key should allow the legitimate user to correctly use these algorithms.

There exists only one scheme that has been proven perfectly secure: the so-called One-Time-Pad (OTP). In that scheme, it is of paramount importance to use a randomly chosen secret key, as long as the plaintext to encrypt, and this key should be used only once. By doing so, a given ciphertext can correspond to any plaintext, and there is no way to decrypt the message without knowing the key. However, the OTP is not used in practice due to the complexity of the key transmission and its length. For schemes that cannot be proved perfectly secure, their security level is given by the complexity of the best-known attack against them. For instance, if the best-known attack against an encryption algorithm requires 2^{80} computing cycles, the security level of this scheme is considered to be 80 bits (it's the equivalent of a scheme where the bruteforce of an 80-bit long key is the best attack). The downside of this approach is that it does not account for the memory space complexity: some attacks might perform more efficiently in time than others, but their memory complexity makes them completely intractable in practice (*e.g.* enumeration attacks). In 2022, it is generally admitted that a cryptographic primitive providing 80 bits of security or less can be efficiently broken (within months using modern computers).

Three main primitives exist in modern cryptography :

- Encryption, symmetric or asymmetric ensures confidentiality and authentication
- Hash functions ensure integrity
- Signature ensures authentication and non-repudiation

Combining these primitives allows for ensuring every property needed for any specific information. A Hash-based Message Authentication Code (HMAC) for instance ensures both authentication and integrity, adding a hash product to an encrypted message ensures integrity, etc...

A widely used construction that provides every security property available is hybrid encryption. It uses an asymmetrical encryption algorithm to agree on a key known only by two entities, providing authentication, then uses that temporary session key to communicate with symmetric encryption. The first

step is called an Authenticated Key Exchange (AKE) or Authenticated Key Agreement (AKA) and is the most critical part of the scheme. If it is compromised the entire security provided by the scheme is lost. The transition to symmetrical encryption has two major advantages. Firstly the leak of a session key does not compromise the other sessions, meaning only the leak of a secret key can impact previous and further communications. And secondly, symmetrical encryption is more efficient, quicker, and has less bandwidth overhead. The Transport Layer Protocol (TLS) protocol that uses this architecture is the basis of internet security.

2.5.2 Symmetric encryption

Symmetric encryption algorithms are based on a shared secret between the communicating parties. When only these two parties know the secret key, and this key has been shared in an authenticated manner, it is considered that the encrypted exchange is authenticated. There exist authenticated symmetrical encryption algorithms that add an authentication mechanism beyond the simple encryption of a message, and Authenticated Encryption with Associated Data (AEAD) that authenticate the non-encrypted associated information in a packet.

The current standard for symmetrical encryption is the Advanced Encryption Standard (AES) algorithm. It won the standardization contest in 2000 but only became widely used after the triple Data Encryption Standard (DES) lost its popularity a few years later. AES can be used with 128, 192, or 256-bit keys and encrypts blocks of 128 bits.

2.5.3 Asymmetric encryption

Asymmetric encryption uses a pair of keys for each entity. The secret (or private) key is never shared with anyone, while the public key is, as its name suggests, shared with everyone. If someone wants to send a message to an entity, the message is encrypted with the public key of the recipient, and can only be decrypted with the corresponding secret key. This provides confidentiality to the encrypted message, as the secret key is never shared.

Asymmetrical encryption is based on hard mathematical problems, such as the integer factorization for Rivest Shamir Adelman (RSA) [26], or the discrete logarithm for ElGamal encryption scheme [27]. Even if the aforementioned problems are not generically proven NP-hard, the best-known algorithms solving these problems have at least sub-exponential complexity, making them hard to solve in a reasonable time for cryptographic-size parameters.

2.5.4 Signature and certificates

Digital signatures are based on asymmetrical algorithms. They are used to validate the authenticity of a message. The signing algorithm takes a message and the secret key and outputs a signature. To verify it, the signature is put through a verification algorithm with the public key as the other entry. The signature is verified if the output of the verification algorithm corresponds to the original message. This adds authentication and non-repudiation without encrypting the message. This is particularly useful for broadcast (or any message with multiple recipients), where the source of the data only has to sign once and everyone can verify without sustained communication with the source. In practice, a hash of the message is computed and is the only part signed. This

provides integrity and strongly reduces the computation time for the signature and verification processes.

The standard signature schemes used in TLS are RSA with Probabilistic Signature Scheme (RSA-PSS), Elliptic Curve Digital Signature Algorithm (ECDSA), and Edwards Curve Digital Signature Algorithm (EdDSA).

Depending on the signature scheme, the size of the keys and the signature varies. The complexity of the signature process and the verification are also different. By choosing the correct algorithm, it is possible to minimize the workload of the signature process or validation (usually at the cost of the other).

To ensure the legitimacy of public keys, a public-key certificate can be used. This is a document attesting to the validity of a public key. It includes information about the identity of the owner, as well as the authority that issued the certificate of the key. The authority signs the certificate with its own private key, and the corresponding public key is either directly known by the hardware or is itself certified by a higher certification authority. This chain will continue up to a certificate authority that is publicly known by the hardware. Currently, the most common certificates are x509. This format can use the three signature schemes allowed by TLS.

2.5.5 Authenticated key exchange/agreement and hybrid encryption

An AKE is based on asymmetric encryption. The public key is available to everyone, and the secret key is known only by its proprietary. A random secret is generated by the entity that wishes to communicate and is then encrypted with the public key of the recipient. The ciphertext can then be transmitted through an unsecured channel. This process is called a Key Encapsulation Mechanism (KEM). The secret is known only by the two parties because the knowledge of the private key is needed to decrypt the ciphertext and recover the secret. In practice during the KEM process, the source also signs a hash of the key in order to provide mutual authentication, integrity, and non-repudiation to the key exchange.

An AKA has a similar process, but the secret is not fully generated by one side, it is computed with one's secret key and the other's public key (plus a random number). This process allows for both entities to compute the same secret, which is impossible to obtain without the knowledge of one of the two secret keys. This allows for mutual authentication if the public keys are certified.

The TLS protocol uses Diffie-Hellman Ephemeral (DHE), Elliptic Curve Diffie-Hellman Ephemeral (ECDHE), and RSA (but not in the latest version) for authenticated key exchange.

Once a secret key is shared between two parties, it is derived into a symmetrical session key, used to encrypt communications. This symmetric encryption process is called the Data Encapsulation Mechanism (DEM). The combination of KEM and DEM is called hybrid encryption and allows for secure communication. As symmetric encryption is a lot more efficient than asymmetric encryption, the hybrid encryption scheme optimizes the data expansion and computation power required to check all the security requirements.

2.5.6 Post-quantum cryptography

With the development of quantum computing, certain current standards are potentially compromised. For instance, Shor's quantum algorithm [28] provides a polynomial time solution to the factorization problem, which allows breaking

any RSA key in a reasonable time. It can also be used to quantumly compute discrete logarithms in quasi-polynomial time, compromising the security of Diffie-Hellman (DH) like primitives (including those involving elliptic curves). With the simplification of the cryptanalysis of current standards, there is a need for the development of post-quantum solutions.[1]

For symmetric algorithms, the new possibilities of quantum computing simplify the cryptanalysis but the solutions remain exponential. AES in particular is vulnerable to cryptanalysis by Grover's search algorithm [29], which essentially square roots the complexity of an attack (hence halving its security level). Therefore AES would only remain relevant for 256-bit keys. The same problem appears for hash functions, where finding collisions is made easier with the Grover algorithm. The countermeasure is similar to AES, where SHA-256 is potentially vulnerable, SHA-512 will remain secure.

The quantum threat exists mainly for key exchange and signature schemes. RSA-based, Elliptic Curve Cryptography (ECC)-based and DH schemes will not be secure. The development of quantum-resistant applications has been a field of research since the discovery of the Shor algorithm. There are 5 main (public-key) primitives for post-quantum cryptography:

- (Euclidean) Lattices for encryption and signature;
- (Error Correcting) Codes for encryption and possibly signature;
- Hash functions for signature;
- Multivariate polynomials for signature and possibly encryption;
- (Elliptic curves) Isogeny for encryption and possibly signature.[2]

In 2016 the National Institute of Standards and Technology (NIST) launched a standardization process for post-quantum cryptography [30]. The standards have been announced in July 2022. These standards have been thoroughly investigated for vulnerabilities, dismissed, or modified during the selection process. However, they will take some time to be widely adopted, as the trust in their security by the general public comes with experience.

2.5.7 Lightweight cryptography

Each cryptographic scheme has requirements for its usage on hardware. For an encryption algorithm, these requirements are the number of computation cycles and the memory space they use. These numbers are relative to the size of the encrypted message and the level of security. They also depend on the CPU architecture (The number of cycles and memory usage varies between an ARM and an x86 CPU, or between 32bit and 64bit CPUs). The comparison must be made at a similar level of security and on the same hardware to properly evaluate the performance of these algorithms. Characteristics such as ciphertext size overhead compared to the cleartext, and key sizes are also important in the performance evaluation of cryptographic techniques.

Lightweight Cryptography (LWC) represents the schemes that have a smaller computation complexity and/or memory consumption. The goal is to extend the

[1] Post-quantum algorithms are sometimes referred to as quantum-resistant or quantum-safe in the literature.

[2] By possibly, the authors mean that there exist propositions in this sense in the literature. However, a substantial fraction of them has proved to be unsecured.

use of cryptography to more constrained devices that are not powerful enough to compute standard algorithms in an acceptable amount of time.

Lightweight primitives exist for encryption (symmetric and asymmetric), hashes, and signatures. Asymmetric encryption and signature schemes can have uneven performance requirements, so they are very lightweight on a constrained side but require a lot more computation on the other side. This is helpful for systems with uneven performance capabilities (WSN or UAS for example). The powerful central/ground unit of these systems is able to compute more than the outer nodes.

The NIST has started a standardization contest for lightweight primitives [31]. This process should finish in late 2022 and will define standard lightweight primitives for symmetric and asymmetric encryption, signature, and hashes. They will have been thoroughly tested and modified accordingly during the selection process, and therefore will be considered secure enough to be used on a larger scale. This, however, does not mean that they do not have any vulnerability and a new powerful zero-day attack could be able to breach the security they provide. But the extensive testing guarantees that no existing method is able to compromise these solutions.

2.6 Security threats, goals and requirements for UAS communication links

Information security on UAS communication links has several goals. It enables a secured operation and safe traffic management for UAVs. As safety is this paper's focus, the properties required for privacy are considered secondary. The protection of mission-specific information is delegated to the responsibility of the operator, as the high disparity in data sensitivity discourages a common security approach. The links and their security requirements are presented in Table 3. The impact column represents the level of importance. The temporary loss of an important link can be acceptable but any loss of a critical link can impact the safety of the operation and induce physical and material damage. The requirements in parenthesis do not directly impact operation safety but are relevant from a privacy and traceability point of view. The security requirements are then discussed and justified in Sections 2.6.1, 2.6.2, and 2.6.3.

Type of Communication	Data	Impact	Security Requirements
UAV-GCS	command	critical	(C), I, A, (NR)
	video	critical	(C), A, I
	telemetry	important	(C), A, I
	mission data	specific	Non Applicable
UTM-UAV	emergency	critical	I, A, (NR)
	direct	critical	(C), I, A, (NR)
	telemetry	critical	I, A, (NR)
UAV-UAV	relay	important	(C), I, A, (NR)
	routing	important	I, A, (NR)
	environmental	important	I, A, (NR)

Table 3: UAS links and their security requirements (Confidentiality, Integrity, Authentication, Non-Repudiation).

2.6.1 UAV-GCS link security

The link between a UAV and its GCS is the only link that is technically mandatory to fly. Aside from mission-specific data, it can be separated into 3 different links. They are sometimes physically separated but are usually sent through the same communication means.

First is the command link that transmits all command inputs or trajectory adjustments from the GCS to the UAV. The UAV can respond with acknowledgment messages. This link is critical for the safe operation of a UAS. If the command link is compromised, the direct control of the UAV is in danger. For safe UTM, this link has very important needs of authentication and integrity. The GCS has to be authenticated as it has overriding authority on the UAVs decisions. To avoid being fed false information, the GCS needs to trust the UAV as well. However, this link needs sustained availability, especially when the UAV has no or limited automation. The mission is compromised if the communication with the GCS is lost. There are confidentiality needs as well, especially if the system uses the IoD architecture presented in Figure 1. An outside observer should not be able to determine which end-user controls which UAV. Confidentiality is not required to enable a safe UTM and is only a privacy concern.

The video feed is sent from the UAV to the GCS and is mandatory in any BVLOS flight. The pilot cannot safely control the UAV without visual input and it is mandatory that a human pilot can take direct control of a UAV. The visual information also helps to check the progression of the mission and verify that the UAV follows the correct course. Video is also often part of the mission (surveillance, infrastructure monitoring, and others). However, even if mission-specific data is left to the discretion of the operator, its critical use for safety makes it a critical link for safe traffic management. This means that authentication and integrity of the video are required. Moreover, video is very sensitive

regarding privacy requirements. The link can contain private information which is why confidentiality needs are important for privacy.

The UAV sends all the telemetry data it collects back to the GCS. This link contains a lot of information on the flight, and the data can be used by the GCS to modify the flight plan. Compromising this link can indirectly modify the UAV's trajectory. Authentication and integrity are then important to secure the airspace. As a lot of information gets sent through this link, confidentiality is needed for privacy. The temporary loss of this link is not as critical as it is for the command and video links.

Mission-specific data that is not the video used for UAV control does not impact the safety of UTM. Each operator is responsible for the level of security required for such information. If privacy concerns are raised the data will have to remain confidential.

2.6.2 UAV-UTM system link security

UTM solutions are still in development, and the technical specifications of the links between the UTM system and the UAS are still not determined. It is known that three types of communications will be required (see Section 2.3). The UTM system can broadcast emergency messages for real-time airspace organization modifications. It will also be able to contact a specific UAS via its GCS and eventually the UAV. And the UAV will need to transmit telemetry information to the UTM services.

The emergency broadcast from the UTM system is used for last-minute modifications in the organization of the airspace. As needed for ensuring the safety of the traffic, new geofences can be enabled and changes in flight authorizations can be put in place. These modifications will impact the operations, forcing the UAS to change trajectories, or even grounding the UAVs. The availability of this service is critical, as well as authentication, integrity, and non-repudiation. Providing confidentiality to this information is not recommended, as it concerns every entity in the airspace, and would need to be interpreted without the security mechanisms.

The direct link between the UTM system and a UAS is similar to the link an aircraft has with a control tower in aviation. Information concerning only one UAS is transmitted. Direct flight recommendations are given by the UTM system, for conflict resolution or other traffic management services. Flight plan modification requests from the UAS are also transmitted on this link, as well as the UTM system responses. This system will converse with the pilot himself, the GCS, or the UAV's flight manager (similarly to the different ATC communications with an airplane). This system induces course corrections for the UAV and is therefore critical to the safety of traffic management. Authentication of both parties, integrity, and non-repudiation are needed for securing the traffic, and confidentiality is recommended for privacy issues.

UAVs need to be identified remotely and to communicate part of their telemetry (position, speed...) to the UTM system. The UTM system needs to be sure it talks to a real UAV as its presence can affect traffic management. For this link, it has been proposed to use a system similar to Automatic Dependent Surveillance-Broadcast (ADS-B), where some telemetry data is openly broadcast without any added security. However commercial aviation has redundancy and does not use this system for the ATC [32]. Other propositions rely on cellular networks to transmit this information. This would improve availability and has

a few native security mechanisms. Whatever the communication system used, there is an important need for authentication, integrity, and non-repudiation, because vulnerabilities on this link compromise traffic surveillance. The need for confidentiality is still being debated. As UAVs can perform missions where, if the trajectories and the identity of the users were to be leaked, some private information can be extracted (delivery from or to a hospital, transport to sensitive locations...). It is then relevant to propose a security solution that adds confidentiality, or at least some anonymization for the UAV-UTM link.

2.6.3 UAV-UAV link security

Three types of communications can exist between UAVs in UAS networks. The network can use UAVs as relay nodes for the UAV-GCS communication or UTM services. Organizing the network requires routing information to be transmitted. Lastly, UAVs can propagate environmental information to neighboring UAVs.

When a UAV is used as a relay, it becomes a part of the link between the end parties. But to enable the safe forwarding of messages, authentication of the relay node is necessary, as well as integrity and non-repudiation. Confidentiality is not as important if the larger link is properly secured, only associated data is left unprotected. For privacy reasons, an operator could want to anonymize the source and destinations of the messages.

To be used as relays, the UAVs need to use routing protocols to organize dynamically the network. Routing messages are often sent between nodes to update the routes. In order to keep only legitimate nodes in the network, these routing messages need to be authenticated, and integrity and non-repudiation also need to be provided.

Environmental information is used by UAS to optimize trajectories. It is important to have it authenticated, as false information can impact the safety of an operation. Integrity and non-repudiation are also important to ensure the legitimacy of these messages. These messages can be broadcast to all neighboring aircraft, and similarly to emergency messages from the UTM system (see Section 2.6.2), adding confidentiality is not recommended.

3 UAS communication vulnerabilities

3.1 Sensitive data interception attack

3.1.1 Eavesdropping: description and operational impact

Eavesdropping, sniffing, or passive listening is a simple attack that can be performed on any electromagnetic signal. The attacker only has to intercept the communication. In any wireless setting, it is achieved simply by setting up a receiver and observing the communication between two parties. If the attacker is then able to extract sensitive information from the signals, the attack is successful. Even when the signal is encrypted, if the identity of the source and destination are not hidden from the attacker, some private information is leaked as well.

Current protocols for telemetry, like the MAVlink, are particularly vulnerable to eavesdropping. Kwan *et al.* [33] detail these flaws in an empirical analysis of the MAVlink protocol. The lack of confidentiality can cause privacy issues, even with telemetry being the only information leaked. The MAVlink can be

transmitted over a secure channel, but as telemetry is not usually considered sensitive, operators do not generally bother and simply use the MAVlink over unencrypted channels.

The video link is particularly vulnerable to data interception, as it can contain sensitive images. The security of the video link varies a lot depending on the UAV and its camera. UAV manufacturers either include the video feed in their main communication link between the drone and the GCS (this is usually done by Wi-Fi enabled UAVs), or they use a separate channel to transmit the video (this is common on long-range UAVs using LoRa or similar protocols for the command link). In this second case, an unprotected method can be used to transmit the video. National Television System Commitee (NTSC), Phase Alternating Line (PAL), or Sequential Color and Memory (SECAM) are the analog standards for video broadcasts used by most CCTVs and off-the-shelf wireless cameras. UAVs that encode their video with those protocols are not protected. Any receiver can decode these signals and therefore no privacy exists with these transmission methods.

3.1.2 Eavesdropping: mitigation and countermeasures

Recording and analyzing ambient signals is a passive task. It is impossible to detect if someone is listening on a wireless channel. An attacker will always be able to log the signals and try to extract information. The signals can however be protected.

In a multiple UAVs system, it is possible to use other nodes to send artificial noise, confusing the eavesdropper. Zhong, Yao, and Xu presented a cooperating jamming approach [34] that uses a second UAV to mask the confidential information transmitted to the GCS. The solution assumes that the system knows the location of the GCS and estimates the eavesdropper's position. It then adjusts the UAV's trajectories over time to facilitate the jamming. This solution is only viable when the eavesdropper's approximate position is known in advance and requires the full control of a second UAV for the entire communication period.

The physical layer can be protected. Poor and Shaefer [35] present the research on the abilities of the wireless physical layer to provide security. The properties of radio channels such as diffusion and superposition can provide secrecy in wireless data transmission. This is an active field of research, and this solution is not often applied in operational contexts.

However, as discussed in Section 2.4 physical layer security is not in the scope of this survey. For more information on these methods applied to UAVs, please refer to the surveys dedicated to physical layer security presented in Section 2.4 as it will not be investigated further in this paper.

Data confidentiality is added with encryption. If correctly utilized it makes it impossible for the attacker to extract any information from the sniffing. This confidentiality needs to be sustained as the information remains sensitive even long after the flight. The commands and telemetry links can be encrypted using symmetric algorithms. The AES algorithm is however not recommended for constrained systems as it induces a lot of computation overhead. Lightweight algorithms have been developed to solve this problem (see Section 4.3).

An analog video link cannot be encrypted without being converted into a digital signal. Then encryption becomes possible. As a video feed is a real-time sensitive part of multimedia systems, Chen *et al.* have designed a secure video communication system using chaos-based encryption [36]. This system has ex-

cellent real-time performances but is extremely costly in terms of computational power and is therefore not optimized for small UAVs. The use of lightweight symmetric algorithms will be more optimized for UAS. To limit hardware accumulation, computation overhead, and communication overhead, including the video feed from the UAV in a single link to the GCS with the commands is recommended.

3.2 Jamming

3.2.1 Communication channel jamming: description and operational impact

An attacker can interfere with a wireless signal by broadcasting a strong noise over the communication channel. This can disrupt the communication between parties as the signals they want to transmit to each other will be drowned under the noise created by the jammer. The jamming strategy requires the ability to broadcast signals that will be strong enough to disrupt real communication upon reception. A jammer that simply broadcasts random noise over a single frequency is called a spot jammer. Jamming simultaneously a large bandwidth by changing frequency extremely rapidly is barrage jamming, but requires an immense power output to still be effective over the whole bandwidth. Some more advanced techniques exist, such as sweep jamming where the jammer jumps from one spot to another in order to disrupt a larger communication channel with similar power output to a spot jammer. The sweep jamming technique does not block the entire signal, and some data will get through. Sweep jammers rely on the fact that they sufficiently disrupt the communication to induce a Denial of Service (DOS). The jamming strategy works on many different communication links used by UAVs. Wi-Fi, LoRa, cellular networks, GNSS signals, Bluetooth, and many more [37].

Jamming the different links in a UAS causes a DOS on the targeted service. This has various consequences depending on the link and the type of UAS. For autonomous UAVs, the temporary loss of the C2link and video link will compromise any in-flight input by the GCS, but the drone will pursue its mission. This causes a threat to flying objects in the vicinity for emergency cases. The detect and avoid systems should mitigate the risk, but a loss of C2link and video link is unacceptable for more than a few seconds for BVLOS flights. In the case of less autonomous UAVs the loss of the control links is a lot more critical.

Pärlin, Alam, and Le Moullec [38] have developed a protocol-aware jamming system for UAVs, improving the service disruption for low jam-to-signal ratios in comparison to sweeping jammers. A simple Software Defined Radio (SDR) is used to effectively perform a DOS attack on the command link of the UAV. The authors tested their jammer on two generic remote control systems (FASST and ACCST). By comparing the distance of effectiveness at a fixed power output, they determined that their system was an improvement over the sweeping jammer by a factor of 2.4 for the FASST and 5.7 for ACCST.

Jamming is not always an offensive technique. As seen in Section 3.1.2, cooperative jamming is a helpful tool to defend against eavesdropping. As this paper does not thoroughly investigate physical layer security, please refer to the survey works presented in Section 2.4 for more information about defensive jamming.

3.2.2 Communication channel jamming: mitigation and countermeasures

Conventional anti-jamming approaches either mitigate the effects of jamming with limited effectiveness or rely on detection and deploy a countermeasure while interrupting the communication [37].

Mitigation techniques are numerous. The Frequency Hopping Spread Spectrum (FHSS) is one of the simplest techniques and is often used in LoRa and Wi-Fi networks, but does not work against smart jammers and is not efficient in terms of spectrum utilization. Specific signal modulations are more resilient to jamming, but also provide a lower bit rate. Research is still ongoing but solutions like massive Multiple-Input Multiple-Output (MIMO)-based anti-jamming techniques are too costly to be implemented on a small scale. However, coupling a MIMO system with the Intelligent Reflecting Surface (IRS) technology [39] would significantly lower the cost of this solution. Results have shown that IRS-aided MIMO will perform similarly to a massive MIMO with a lot less hardware and power usage. IRS could then be deployed with smaller MIMO systems on much smaller wireless networks, allowing the anti-jamming and the performance improvements offered by massive MIMO to be used in smaller UASs.

The jamming detection techniques have evolved from basic noise monitoring to multi-factor learning-based approaches. With factors including the directional parameters of signals, the newer detection techniques can more effectively detect jammers, and pinpoint their location and characteristics.

The detect and counter strategy is more efficient than mitigation techniques but it results in a temporary loss of the connection. As this is unacceptable for UASs, another approach would be to conceive jamming resilient systems by design. Some physical layer properties could help differentiate real signals from noise, based on directional input and more advanced noise filters.

3.3 Spoofing attack

3.3.1 Communication links spoofing: description and operational impact

Spoofing is a situation where an attacker successfully usurps the identity of a legitimate user or network node. By taking the identity of a GCS, the UTM, or a UAV, an attacker can perform Man-In-The-Middle (MITM) attacks, compromising the entire UAS through data injection or DOS.

Spoofing the command link from the GCS to send false information to the drone gives control of the drone to the attacker. In [40], this is used on the Parrot AR 2.0 drone. The authors captured the signals used by the GCS for different commands and analyzed their structure. They were then able to generate fake command inputs, spoofing the controller's IP address, and the drone interpreted these messages as legitimate.

Spoofing the telemetry link from the UAV can cause the GCS to send course corrections, modifying the trajectory and compromising the UAV's mission.

An attacker can also target the video link, with similar results as the telemetry spoofing. The pilot will try to correct the trajectory, compromising the UAV and its mission.

The telemetry spoofing attack can also be aimed at the UTM. This can simulate fake objects to modify the path of oncoming traffic, and create false threats to commercial aviation, disrupting the whole airspace control system.

The UTM en-route service itself can also be spoofed. An attacker could disrupt the UAV's trajectory by creating false exclusion zones, removing real ones. It could even send false trajectory modifications to the rest of the UAS.

The MAVlink protocol can be particularly vulnerable to spoofing attacks as it does not provide any security. It is easily spoofed if used over a non-secure channel. The MAVlink can be used for the command link and the telemetry link, meaning that an attacker can use this vulnerability to take full control of the drone.

3.3.2 Communication links spoofing: mitigation and countermeasures

A smart Intrusion Detection System (IDS) can detect spoofing [41]. It requires monitoring from a central overseeing position to be most effective. This system works better on Ad-Hoc networks and is based on the identification of malicious packets. Machine Learning (ML) techniques can then be used to distinguish legitimate nodes from spoofed ones. New spoofing techniques will however potentially work undetected.

Spoofing is strongly countered by proper authentication. The use of cryptographic primitives with correct implementation ensures the authentication of all parties. Over the internet, the TLS protocol ensures such properties with the use of HTTPS. The particular conditions of UAS make it incompatible with TLS due to the bandwidth overhead and computational power required for sustained use of TLS. Lightweight authentication techniques are detailed in Section 4.2.

3.4 False information dissemination (UAV to UAV)

3.4.1 False data injection: description and operational impact

False data injection is an attack in which false information is transmitted from a compromised UAV. This can concern false environmental conditions forcing legitimate UAVs to modify their trajectories, reducing the success rate of their missions as well as their survivability. This can also concern the ADS-B in the cases where it is used to avoid collisions. Since ADS-B is an open broadcast with no authentication protocols, an attacker can create a fake object at critical positions or broadcast counterfeit positions for the legitimate UAVs by impersonating them.

3.4.2 False data injection: mitigation and countermeasures

The IDS proposed in [42] can detect ADS-B attacks by cross-checking the ADS-B information with the location estimated with signal intensity and round trip time data. This IDS also verifies the coherence of environmental information with the other drones in the network, but this depends on the sufficient presence of legitimate users in the area. The IDS can raise an alarm and the UAS will deal with the compromised node.

These attacks can be countered by cryptographic methods (see Section 4) that ensure authentication and integrity. If the UAVs are trustworthy and the integrity of the signals is verified, the attack is no longer possible as an outside attacker will not be able to counterfeit authenticated data.

3.5 Malicious detection and identification

3.5.1 Malicious detection: description and operational impact

With the arrival of ADS-B, Remote-ID, and other UAV identification frameworks, some privacy concerns have been raised as UAV detection is easily performed. If UAVs and their mission can be easily identified, attackers can detect and physically threaten relevant UAVs. This topic has been debated, with the National Business Aviation Association (NBAA) raising concerns about the privacy issues created by the mandatory use of Remote-ID in the United States [43].

Even without such systems, works such as [44] allow for remote detection and identification of UAVs based on Radio Frequency (RF) fingerprints in their controller's signals. The authors used ML techniques to classify the signals and identify 14 types of UAVs. In [45], the same authors propose a scheme where these identifications are made possible with interference.

Shoufan *et al.* have proposed a system that can identify a UAV's pilot based on flight behaviour [46]. Using ML techniques they are able to identify 20 pilots with 90% accuracy. This is only possible when the pilot is directly commanding the drone and requires a dataset for all pilots to be effective.

3.5.2 Malicious detection: mitigation and countermeasures

The authentication scheme behind Remote ID and other potential identification frameworks can be protected for privacy. In [47], Alsoliman, Rabiah, and Levorato developed an extension of the Remote ID framework with privacy-preserving capabilities. This solution allows for an anonymized authentication where the pilot and the operator's identities are known only by the authorities. It is also able to verify the flight permissions of a UAV flying in a specific area without revealing the UAV's entire flight path. In this work, the flight plans are sliced, and the Remote-ID messages are modified with a pseudonymous certificate, allowing for UAV authentication and authenticated flight permission for the current area.

The FAA proposed the Privacy ICAO Address [48] to respond to the privacy concerns raised by UAV operators regarding the use of ADS-B. This solution provides operators with temporary ICAO addresses for their aircraft which are not assigned to the owner in the civil aviation registry. This enables owners to broadcast ADS-B messages with anonymized identifiers.

3.6 Routing attacks

3.6.1 Black hole and gray hole: description and operational impact

The black hole attack is a network attack where a compromised node presents itself as the route for all destinations, but then deletes all the packets it receives, inducing a DOS on the network. This is done by replying favorably to any route request message received, hence attracting all future packets to the compromised node.

The gray hole attack is an improved version of the black hole, where in order to not be detected and excluded from the network, the compromised node will only drop the packets with a certain probability. Alternatively, gray hole attacks can be selective with the dropping of packets. This results in an increase in communication delay, or to a full DOS depending on the network characteristics and the importance of the data transmitted.

VANETs are particularly vulnerable to these attacks. The dynamic nature of the network topology causes routing tables to be continuously updated, thus increasing the potential impact of attacks using routing vulnerabilities.

3.6.2 Black hole and gray hole: mitigation and countermeasures

In [42], the IDS is able to detect black and gray hole attacks thanks to a trusted supervisor that monitors packet loss. The system raises an alarm when a node is failing to forward a number of packets superior to a threshold representing natural packet loss.

Applying cryptographic primitives to routing messages is an alternative if the compromised node is not an authenticated part of the network [49]. This is also a mechanism that protects against black hole attacks where the attacker spoofs a legitimate node of the network. The authentication mechanism is however vulnerable to DOS, as the verification delay can be used to slow the nodes by flooding them with packets. This effect is mitigated by the use of lightweight cryptography (see Section 4.2).

3.7 Wi-Fi specific attacks

3.7.1 Wi-Fi enabled attacks against UAS: description and operational impact

Wi-Fi enabled UASs are mostly recreational and usually have little to no focus on information security. Their security properties rely mostly on the security properties of the communication link, the Wi-Fi. Some do not have any security and have an open Access Point (AP) that is easily hijacked. Others use old protocols such as WEP that have been rendered obsolete by modern cryptanalysis. Recent Wi-Fi enabled UAVs generally use a private AP secured by WPA2, but they are still extremely vulnerable. The use of WPA3 is not yet widespread but is more strongly defended with the correct settings. WPA2 is vulnerable, particularly when the credentials are not randomized. Some bruteforce attacks on the secret key such as the PMKID attack will even work at low resources with weak passwords. Rogue AP can be used for MITM attacks.

He, Chan, and Guizani [50] have performed standard Wi-Fi attacks on UAS. The WEP protocol is extremely weak, only the WPA2 can remain strong against low resource bruteforce attacks. They used the Aircrack-ng suite to compromise the Wi-Fi network used by the drone. It is also possible to crack the key using ARP replay attacks, as the drone will always respond to ARP requests with variable Initialization Vectors (IVs), which helps in cracking the key. A deauthentication attack is also effective, the attacker can send deauthentication frames, disrupting the connection with the legitimate user.

Westerlund and Asif [40] evaluated two commercial Wi-Fi enabled UAVs: the Parrot AR 2.0 and the Cheerson CX-10W. They investigated several Wi-Fi attacks to test the security of the communication links of these drones. In particular, they performed DOS attacks by deauthentication, MITM by deauthentication and reconnection to fake AP, deauthentication and reconnection to an illegitimate controller. Most of these attacks are induced by the lack of pilot credentials in the native system. The authors then built a UAV disabler for the Parrot with a Raspberry Pi3, using their previous findings to exploit the communication vulnerabilities.

3.7.2 Wi-Fi enabled attacks against UAS: mitigation and countermeasures

Wi-Fi enabled drones can be protected by Wi-Fi security features. Using proper security provided by the WPA2 protocol, with a strong random key mostly protects against low-resource attacks.

In [51], Hooper *et al.* explore the security flaws of the Parrot Bebop UAV and propose a security framework to defend the AP of Wi-Fi enabled UAVs. This research proposed solutions against the ARP poisoning attack, as well as DOS created by the presence of multiple potential controllers. The authors discuss the importance of a multi-layered security framework against zero-day vulnerabilities. They argue that the low importance given to security aspects of small UAS causes a lot of zero-day vulnerabilities to exist and that only a multi-layer security approach remains protected when a new attack is discovered.

3.8 Port scanning and open services

3.8.1 Open ports and services: description and operational impact

In most off-the-shelf UAVs, once connected to the wireless network, the services used to control the drone, receive video or other data, or transmit software updates run on different ports. The Nmap tool can scan those ports, and determine the ones that are used and open for communication. The telnet and File Transfer Protocol (FTP) ports are often opened and, by design, unprotected. Rudo and Keng [52] have performed these tests on a commercial recreational UAV, the Parrot Bebop 2. They found that the FTP ports (20 and 21) were used by the system and performed a fuzzing attack onto the FTP control port (21). This attack relies on randomly sending protocol-specific keywords until getting a response from the service running on the targeted port.

In [40], the open telnet port allows direct root access on the Parrot AR drone 2.0, without credentials. The FTP service is also enabled and allows file transfer during flight simply by knowing the drone's static IP.

3.8.2 Open ports and services: mitigation and countermeasures

The simple application of good practices resolves most of the problems. Simply adding a credentials system and being preventive by shutting down services during flight greatly reduces the risks presented above. In the cases of [52] and [40], FTP service is only used for software updates, and should not be running in flight mode. If ssh, telnet, FTP, or other services are needed for the UAS's operation, manufacturers should not allow their access with no credentials as it offers easy hijacking possibilities to illegitimate users.

4 Securing UTM two-way communications with encryption

4.1 Description

Cryptography can provide confidentiality, integrity, authentication, and non-repudiation to information. The use of encryption, signature, and hash functions provides different properties to a message. For UAS communications, those properties are needed throughout the different channels. Authentication

needs asymmetrical algorithms in a complex network, as the quadratic number of keys required for symmetrical encryption or password authentication is not acceptable. Each member has a secret key used to generate temporary session keys with another member, which are then used for symmetric encryption. This process called AKA or AKE is the basis for authentication, integrity, confidentiality, and non-repudiation. This method is optimal for security but requires two-way communication. When only integrity is required, a hash function is used. This solution is valid only when the only threat is caused by involuntary phenomenons (such as natural transmission loss) and not purposeful manipulation. For integrity and authentication without encryption, a signature scheme is preferred. This is needed when a system does not require confidentiality. For broadcast messages, where everyone is a receiver, this solution is highly preferable.

4.2 Providing authentication to UAS actors with encryption

4.2.1 Description

Due to the poor performance encountered in UAV networks, classic authentication techniques are not preferred. As an example, the TLS handshake has too many steps and uses RSA or DH asymmetrical algorithms to exchange the session keys. These primitives are not efficient in terms of computation and are vulnerable to future quantum threats. Many lightweight AKA schemes have been proposed in the UAV field as well as other fields with similar constraints.

4.2.2 UAS specific research

A lot of research has focused on improving the performance of cryptographic solutions for authentication in a UAV context. Lightweight AKAs have been proposed by several authors. Many use the IoD control architecture as a model.

Wazid *et al.* have proposed an AKA scheme for the IoD architecture [53]. It provides mutual authentication between a drone and a user. The user authentication is done with three factors: user password, smart card (replaced by a mobile device), and user biometrics. Registration needs to be done over a secure channel, as the server generates secrets for users and drones. The scheme is lightweight and uses only hash functions and Exclusive Or (XOR) operations (excluding the biometrics extraction). The server generates and stores every secret key, and is a Single Point Of Failure (SPOF) of the scheme. User passwords and biometrics can be updated, and drone-to-drone session keys can be generated. This scheme was tested with the AVISPA tool, and compared with other lightweight AKAs through simulation, using SHA-1 for the hash function in their comparison. As this protocol is designed for an IoD architecture, the hardware is owned by a service provider who has overarching capabilities on the drones through the server that manages all secret keys.

In [54], Srinivas *et al.* have proposed TCALAS, a lightweight AKE for the IoD architecture. It only uses hash primitives and XOR operations. The ground station server manages every key for drones and users. This scheme provides mutual authentication, parameter updates, and user or drone revocation. Formal security analysis shows the resistance against various attacks. Performance comparisons have been done with the SHA-1 algorithm as the hash function.

Ali *et al.* have proposed an improvement over TCALAS in [55] called iT-CALAS. It is scalable, allows for multiple flying zones, provides user anonymity, and defends against stolen verifier attacks. The security is evaluated with a formal security analysis, and with the ProVerif tool.

The Lake-IoD AKE is a solution developed by Tanveer *et al.* for the IoD architecture [56]. It is a 3-party AKE protocol based on AEGIS (see Section 4.3) and SHA-256 algorithms. User parameters can be updated, and drones and users can be dynamically deployed and revoked by the system. This scheme requires the management system to store keys for every user and UAV. The management system is always involved in communications and is a SPOF.

There have been propositions using internal physical properties of the hardware to generate unclonable reproducible randomness. This allows any integrated circuit to provide a physically defined footprint that cannot be reproduced. This is called a Physical Unclonable Function (PUF) and has been used as a physical authentication basis of UAVs by Pu and Li [57]. They use a PUF of the drone to create a challenge-response pair that is stored only in the GCS. This challenge is only reproducible by the original hardware and a new one is generated each time an authentication mechanism is completed.

In [58], Zhang *et al.* propose an AKA for the IoD based on passwords. It requires a hash primitive and bitwise XOR operations and is faster and lighter than the schemes it compares to.

Cho *et al.* proposed an authentication framework called SENTINEL, based on HMAC that was 3 times faster than the equivalent TLS solution [59]. However in [60], it is proven vulnerable to several attacks. In this paper, Jan *et al.* also remark that the SENTINEL protocol lacks dynamic node addition and revocation. [60] proposes an improvement that is then formally analyzed by ProVerif 2.02.

Nikooghadam *et al.* propose a provably secure lightweight authentication scheme for the IoD architecture [61]. It is based on ECC and hash primitives. A formal security analysis is performed with the Scyther tool. The scheme's performance is compared when implemented with SHA-1 and a 160-bit elliptic curve.

4.2.3 IoT research

In 2014, Turkanovic, Brumen, and Höbl proposed a lightweight authentication scheme based on hash functions and XOR operations [62]. It provides mutual authentication between parties, password protection, free password choice, password changing, and dynamic node addition. It is a two-factor (user password and smart card) authentication scheme. Unfortunately, it has since been proven to be vulnerable to stolen smart card and MITM attacks [63]. It also does not provide properties such as forward and backward secrecy and untraceability. [63] tries to correct these issues at the cost of some performance. Amin *et al.* [64] proved that some vulnerabilities remained and corrected them.

In [65], Suarez-Albela *et al.* made a performance comparison between ECC and RSA for signature algorithms. It shows that ECDSA is two times faster for low security (128 bits) and that the gap grows with the level of security.

In [66], Roy *et al.* propose an anonymous three-factor user authentication scheme. It is based on a hash primitive, a fuzzy extractor, and Chebyshev maps. Chebyshev chaotic maps are better suited to resource-constrained devices than ECC and RSA. A formal security analysis of this scheme has been done with

the ProVerif 1.93 tool, and its performance is evaluated against other chaotic map-based solutions.

4.2.4 Medical field research

The medical field has similar constraints to UAS's for certain systems. For example, healthcare sensors or pacemakers are critically important and resource-limited. These characteristics allow the protocols developed for these systems to also be relevant for UAS security.

In [67], an ECC based AKE is proposed for wireless healthcare sensors. This protocol provides mutual authentication, and three-factor authentication for users: smart card, password, and biometrics. It supports smart card revocation and parameter update methods. three-factor authentication protocols have been proposed for UASs, by swapping the smart card for a mobile device (see Section 4.2.2). The lightweight properties of the system have been optimized, and the computational and bandwidth overheads are limited.

4.2.5 Ad-Hoc networks research

MANET, VANET in particular, are difficult to secure with little computational power and bandwidth. Thus some research aims at developing solid authentication schemes for them.

He *et al.* have developed a privacy-preserving authentication scheme providing mutual authentication [68]. Due to the nature of VANET, the scheme aims at being as lightweight as possible. This scheme uses ECC and hash primitives and is suitable for VANET deployment. The implementation uses SHA-1 and a 160-bit elliptic curve.

4.2.6 AKE/AKA performance comparison

To compare the different AKA's performance, there are different metrics to take into account :

- The properties like mutual authentication, quantum resistance, multiple factors, perfect forward secrecy, secret key storage, and other implementation specifics will determine the attacks that the protocols remain vulnerable to.
- The level of security is determined as the complexity of the best-known attack against the system (for example, attacking a 1024 bits RSA public key has a complexity of roughly 2^{80}, yielding 80 bits of security).
- The bandwidth overhead is determined by the number of supplementary bytes sent during the authentication phase (not during registration/initialization).
- The computation overhead is usually a time comparison between standards and new protocols. It may be less representative as it is often performed on different CPUs. The relative overhead compared to the standards is used in this comparison even if it is not accurate.
- The memory overhead is the size taken in memory by the protocol parameters before and during authentication (IVs, keys...). This variable depends on the scale used for the results provided and is probably the least homogeneous metric.

Security comparison: Table 4 compares the security properties of the different authentication protocols presented above. ✓means the protocol provides the feature or protects against the designed attack. An empty cell means the feature is not supported or that the protocol is vulnerable to the attack.

	Mutual authentication	Public-Key authentication	Two-factor authentication	Three-factor authentication	Anonymity	Traceability attack	Quantum resistance	Revocability	Formal security analysis	Credential updates	MITM	Replay attack	Impersonation	Password guessing	Privileged insider	Stolen authentication factor
[53]	✓		✓	✓		✓			✓	✓	✓			✓		✓
[54]	✓		✓	✓				✓	✓	✓	✓	✓	✓	✓	✓	✓
[55]	✓		✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
[56]	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
[57]	✓						✓	✓		✓	✓	✓	✓	✓		✓
[58]	✓		✓		✓	✓	✓				✓	✓	✓	✓	✓	✓
[59]	✓		✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓		✓
[60]	✓				✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
[61]	✓	✓			✓	✓			✓	✓	✓	✓	✓	✓	✓	✓
[62]	✓		✓				✓		✓							
[63]	✓		✓				✓		✓		✓	✓	✓	✓	✓	✓
[64]	✓		✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓
[66]	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓		✓
[67]	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
[68]	✓	✓			✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓

Table 4: Security features of presented protocols.

Table 5 presents the relative cost of computation for different operations at a similar security level (80 bits) as defined by [54], [68] (for the ECC point addition only) and [66] (for Chebyshev Map operation). These values are normalized with a hash computation considered to cost 1 T (where T is the time complexity of a hash function) and the other values are pondered and rounded to the closest integer. In this context, the cost of an operation costing an amount inferior by several orders of magnitude to the hash function is approximated to 0 T. This is the case for elementary operations :

Operation	Computation cost
Hash function (T_H)	1 T
Elementary operations (XOR, addition...)	0 T
ECC point addition ($T_{ECC_{PA}}$)	18 T
ECC multiplication (T_{ECC_M})	53 T
Fuzzy Extraction (T_{FE})	53 T
Symmetric encryption/decryption (T_{sym})	2 T
Chebyshev Map Operation (T_{Cheb})	17 T

Table 5: Computational cost of basic operations.

Abbreviation	Meaning
t	size of timestamp
h	size of hash function output
ec	size of elliptic curve input
id	size of node identity
crp	size of challenge-response input
cheb	size of Chebyshev polynomial input/output

Table 6: Abbreviations for the bandwidth overhead.

Performance comparison: Table 7 presents the performance of the authentication protocols presented above. When possible, the values in this table are independent of the variables depending on the algorithms chosen by the implementation. If only numerical values are provided, a similar security level is considered. The table contains a relative computational performance comparison with the values defined in Table 5.

The values followed by * come from comparisons done outside of the original paper, by different authors. The storage overhead is often undisclosed (ND).

	Computation Overhead Analytic and Evaluated (drone side)	Total Bandwidth Overhead	Number of Messages	Storage overhead (drone side)
[53]	$31T_H + T_{FE}$ = 84 T ($7T_H$ = 7 T)	10h + 3t	3	>2888b (>480 b)
[54]	$30T_H + T_{FE}$ = 83 T ($7T_H$ = 7 T)	9h + 3t	3	2888b* (640b*)
[55]	$24T_H + T_{FE} + 3T_{sym}$ = 83 T ($7T_H$ = 7 T)	10h + 3t	3	2888b* (640b*)
[56]	$11T_H + T_{FE} + 6T_{sym}$ = 76 T ($3T_H + 2T_{sym}$ = 7 T)	1376b (fixed)	3	2088b (512b)
[57]	approx. 1/10 of [53] = 9 T (approx 1/3 of [53] = 3 T)	2h + 3id + 4crp	3	ND
[58]	$24T_H$ = 24 T ($7T_H$ = 7 T)	9h + t	3	2756b*
[59]	approx. 3 of [53]* (according to [60]) = 252 T* (21 T*)	4944b	3	2488b
[60]	$13T_H + 4T_{sym}$ = 21 T ($7T_H + 2T_{sym}$ = 11 T)	3t + 12h	4	1120b
[61]	$19T_H + 4T_{ECC_M}$ = 231 T ($5T_H + 2T_{ECC_M}$ = 111 T)	8h + 3t + 6ec	3	ND
[62]	$19T_H$ = 19 T ($5T_H$ = 5 T)	15h + 10t	4	4336b*
[63]	$32T_H$ = 32 T ($7T_H$ = 7 T)	16h + 6t	4	ND (2128b)
[64]	$32T_H$ = 32 T ($7T_H$ = 7 T)	15h + 3t	6	ND
[66]	$14T_H + T_{FE} + 3T_{Cheb}$ = 115 T ($5T_H + T_{Cheb}$ = 22 T)	3h + 2t + 3cheb	2	ND
[67]	$19T_H + T_{FE} + 3T_{ECC_M}$ = 115 T ($5T_H$ = 5 T)	4h + 4t + 3ec	3	1776b* (320b*)
[68]	$10T_H + 4T_{ECC_{PA}} + 12T_{ECC_M}$ = 718 T ($5T_H + 2T_{ECC_{PA}} + 6T_{ECC_M}$ = 359 T)	2h + 2t + 12ec	2	ND

Table 7: Performance comparison of presented protocols.

4.2.7 Discussion

Commonly, the implementation of these solutions was done with the minimal accepted level of security: 80 bits. This security level is too low for sensitive information. The analytical comparison is more relevant for evaluating a scheme's efficiency, as it does not depend on the level of security. In [59] and [56] however, the algorithms are inherently linked to the architecture, and substantial work is required to change the level of security. For the memory overhead, the details are not provided, thus making the results fixed to the security level used in the implementation of each solution. Unfortunately, using the SHA-1 algorithm as a collision-resistant hash function is wrong. SHA-1 is flawed, and has been proven non-collision-resistant in 2004, and even more so with chosen-prefix attacks by Leurent and Peyrin in [69]. Moreover, 80 bits is insufficient to counter high-resource bruteforce attacks. The increase in security level does not change the analytical results but changes the memory storage given by the experimental approach.

These performance comparisons are not absolute. Given dedicated hardware, the computational overhead of certain operations can change relative to the others. This is only a rough estimate of the performance offered by these solutions compared to one another. It is also important to note that while the schemes using authentication by password seem to offer more security features and are more performant, they do present a few drawbacks. Firstly the addition of new elements requires an initial authentication that is not considered in this comparison. Moreover, communication between two nodes cannot be initiated without contacting the management station, as it is the only element able to authenticate every single node. Should the passwords leak from the management

server, an attacker will be able to take full control of the system. With public key infrastructures, these problems do not exist, as private keys are known only by their proprietary and only approved by the management system. These schemes are more expensive in terms of performance, but when coupled with a certification system, are not so dependent on the management server. Provided security features also seem to be inferior to password authentication schemes, but most are achievable at the cost of more memory, computation, and bandwidth. Increasing the scale is also a lot easier than with password authentication. It does not require a massive increase in the management server's capabilities. Authentication with external elements like UTM systems is more reliable. Indeed, it offers the possibility of contacting nodes individually without passing through the management server for every initial communication. The other major problem aside from the cost is their lack of quantum resistance, which is mainly due to the recency of the development of quantum-resistant asymmetrical solutions.

Password/hash-based authentication protocols will work best for the control of a fleet belonging to a single operator, but are not adapted for communication with external entities, and thus cannot fulfill the requirements for data links directed to other drones, other aircraft, and the UTM systems. It is not acceptable to have to contact the management station in order to establish a time-sensitive communication necessary for safety.

The research works presented above will not all be compliant with the security requirements of large-scale UTM infrastructures. They have vulnerabilities that are not acceptable, a lack of scalability, or a lack of flexibility. But they can all be relevant for different infrastructures. The password authentication schemes are very good in terms of performance, and for nano UAV swarms, they can be preferred over anything else. For larger UAVs in reduced density, the performance constraints are not so strict, and it might be preferable to use reliable non-lightweight solutions. However, with the increase in traffic density, the bandwidth available for communications will be forcefully limited regardless of the computational and memory abilities of the aircraft. Focusing on bandwidth overhead reduction is the most important objective for enabling a safe UTM in traffic-heavy areas.

4.3 Symmetric encryption lightweight solutions

4.3.1 Description

In a secure communication system, most of the data is transmitted through symmetric encryption, using session keys obtained during the authentication. This section presents relevant lightweight alternatives to AES with their advantages and drawbacks.

4.3.2 Usual algorithms

The Chacha20 algorithm is the preferred current lightweight symmetric encryption algorithm for IoT [70]. It performs better than the AES standard in terms of energy cost, time cost, and memory usage. Chacha20 is 2 to 3 times more efficient than any version of AES-128 for time and energy consumption, as well as using less memory for a shorter time. It uses 256 bits keys (or 128 bits keys that are expanded to 256) and is twice as secure as AES-128. However, with the use of hardware acceleration, the computation time of AES can be greatly improved.

An improvement over the Chacha20 algorithm has been proposed [71] where the complexity of the bruteforce attack grows from 2^{248} to 2^{512}, while only reducing the performance by about 20 %. 512 bits of security is however not needed in any current application. This solution may be useful only for long-term secrets or if a technological jump allows for a great improvement in computation capabilities.

AEGIS [72] is a lightweight symmetrical algorithm based on the AES encryption round function. It can therefore use the AES instructions implemented in processors while being twice as fast.

4.3.3 UAS specific research

In [73], Avdonin *et al.* propose using OTP to secure communication. Besides being the only perfectly secure encryption scheme (in an information theory way of speaking), encryption is performed using only elementary bit-operation XOR. This means it is by far the lightest possible solution in terms of the computation required. There is however a big drawback: it requires a shared random key, as long as the data transmitted, and usable only once. The memory storage on the drone side would be enormous, but on the server side, with one key per drone, it will be multiplied. The solution may still be viable for communication channels that require very little data flow, such as emergency channels. Theoretically, Quantum Key Distribution could provide a secure way to exchange such keys on the fly without resorting to an encryption layer, assuming it is feasible to maintain a quantum communication channel between the ground station and the flying drone. Such assumptions do not seem realistic to the authors, and even by using a classical communication channel with an encryption layer, OTP encryption does not seem to be close to optimal in practice.

4.3.4 Discussion

Symmetrical algorithms are the simplest way to maintain authenticated communication. They do not use considerably more bandwidth than the cleartext (AEAD algorithms can add a few bytes). Chacha20 is old enough to have been thoroughly investigated for faults and is the more reliable option. If stronger security is required, [71] may be a better alternative. For systems with hardware acceleration for AES, AEGIS is also a good alternative. The key exchange will have to be adapted to the algorithm, as the level of security given to the session key needs to be as high as the symmetrical algorithm's.

If however, a secure way of transmitting (or storing) very long keys is found, the OTP solution will be by far the fastest and most secure. It is however currently incompatible with the limits of the system.

5 Securing UTM broadcast communications

5.1 Securing ADS-B-like communication

It has been proposed to add integrity, authentication, and confidentiality to the already formatted ADS-B packets in order to communicate with UTM services. Even for commercial aviation, there have been numerous propositions to secure the system, as even if ADS-B is not the primary source of information for critical systems, it is used more and more often for secondary applications.

The authentication framework proposed by Baek *et al.* [74] adds an identity-based signature to secure ADS-B, using a trusted third party to generate their secret key. It has been adapted into a three-level hierarchical identity-based signature (HIBS) by Yang *et al.* [75]. This improvement reduces the runtime of the protocol, both in signature generation and verification by adding a batch verification mechanism to the system. This system has some lightweight properties, but requires modifications to the ADS-B protocol to be implemented, or needs to use a different channel to send the signatures. It does not provide confidentiality regarding the identity of the aircraft.

Another approach for an ADS-B security solution was proposed by Yang *et al.* [76]. This scheme uses a trusted third party to generate secrets and transmit them to relevant parties. It ensures privacy by using Format-preserving, Feistel-based encryption (FFX) on the unique identification of an aircraft to anonymize them. Attackers are then unable to correlate valuable information to any aircraft. The format-preserving nature of FFX makes it compatible with current ADS-B systems. The scheme also provides integrity and authentication with the TESLA protocol, using a special identifier on 4 additional ADS-B packets to transmit the Message Authentication Code (MAC) and keys instead of standard ADS-B information. This solution requires a loose time synchronization and has a polynomial overhead in terms of bandwidth and computation. The authors then extended their work [77], achieving adaptive TESLA and solving other problems. They also implemented their solution in a real airport environment, demonstrating the feasibility of their solution. This proposition was designed for commercial aviation and is not optimized for the scale and constraints of UAS.

5.2 Cellular networks

ADS-B is not the preferred solution for the UAV-UTM link. Most proposed alternatives use cellular networks as their communication link, either with the UAV directly or through the GCS. 4G and 5G networks include security features, including an authenticated key agreement for symmetric encryption of the traffic. Therefore the vulnerabilities of the UAV-UTM link would be dependent on the vulnerabilities discovered within the cellular networks. Ahmad *et al.* have compiled the security issues in cellular networks in a survey [78]. They outline that some issues remain even with the latest versions of these networks, and summarize the potential solutions to clear those issues.

These solutions cannot be implemented everywhere, as cellular coverage will not be available for certain missions. Protecting those communications can be done on the transport layer, with TLS for example. This is far from being the best solution as TLS is very demanding in terms of performance, and is more optimized for larger data flows.

5.3 RemoteID

RemoteID is a specification defined by the FAA [79] providing the means to integrate UAVs in the American airspace. It includes regulations for communication with external entities such as UTM services. UAVs need to regularly broadcast timestamped messages containing an identifier, position, heading, speed, and emergency status. It does not provide any cryptographic means to protect the information and is therefore vulnerable to the same attacks as ADS-B.

In [80], Brighente, Conti, and Sciancalepore propose different solutions to mitigate the privacy problems brought by this system. The authors present a system able to anonymize and mask the geographical data while detecting 94% of invasions.

5.4 Discussion

Current UTM protocols like ADS-B and RemoteID are inherently flawed. The need of transmitting cleartext messages limits considerably the possibility of cryptographic solutions. It is possible to anonymize, but there is a need for authentication with the threat of accepting a lot of false information.

Developing new standards for broadcasting and direct communication with native cryptographic solutions added may be the best way to address the security issues. A signature scheme is sufficient for the broadcast messages (from UAS or UTM systems alike), and a hybrid encryption scheme is preferable for direct communication between a specific UAV or pilot and the UTM systems.

6 Challenges, open issues, and future directions

The safety of air traffic has been a point of focus since the inception of commercial aviation. Unmanned air traffic is inserted in this environment and therefore seeks to maintain the level of safety existing in the airspace. Communication is a pillar of traffic management, therefore communication security is an important factor of air traffic safety. For unmanned vehicles, communication is even more important than for manned aircraft, as the control is performed remotely through communication means. To develop safe traffic management systems, they must be designed with mandatory security requirements. The UAS field presents strict limitations in terms of performance, limiting the use of classic cryptographic solutions found over the internet. In response to this problem, research has developed lightweight solutions, suited to low-resource systems. This survey presented a non-exhaustive overview of the research works proposing cryptographic security solutions for UAS, to ensure air traffic safety. Privacy and traceability issues are not directly related to the safety of air traffic. These issues were presented and were noted when covered by the research works. However, they were considered secondary to safety in the recommendations for UTM security solutions. By studying these works of research, a few findings emerge which indicate several paths for future research into UTM security.

6.1 Limits in the testing process

The main challenge for the majority of the authentication protocols presented in this study is the lack of upscaling and real implementation. Choosing these solutions is not currently recommended due to the lack of experience and testing. These protocols have to be tested for large-scale UAV networks. The performance may decrease exponentially with the increase of nodes in the network. Real implementation on various hardware will provide data on communications delays induced by the protocols, and help improve the implementation. For example, this will determine a maximum round-trip time, after which the sender can reasonably estimate the loss of a packet.

6.2 Anonymity and traceability

The regulatory framework to authorize BVLOS flights will, at the minimum, impose the levels of security detailed in Section 2.6 as they are mandatory for the security of the UTM. The privacy issues can also be addressed by the regulation but are not directly linked to the safety of UAS operations. However, those issues are often resolved by providing solutions for the security requirements of UTM. If some anonymity is required for privacy, maintaining traceability and non-repudiation will be a challenge, and additional work will be needed to provide the property.

6.3 Complete security architecture

Though a lot of research has focused on developing security protocols for UAS, there has not been a proposition for a complete security architecture. Integrating the relevant cryptographic solutions into a global scheme will be necessary to meet the security goals required for secure traffic management. An analytic study is necessary to produce a model that will maintain the security requirements within the whole system. It will then be possible to optimize the model under the constraints of the system and the security levels deemed necessary for each communication. This architecture can be designed with the network structure of UAS and UTM. By choosing certain algorithms and implementations, it is possible to optimize the system for improved routing in a FANET.

6.4 Need for public-key architectures

Many authentication protocols rely on passwords yet it is not optimal for large-scale infrastructures. Public-key architectures will be necessary for dense traffic areas. Their cost in terms of computation is higher, but the benefits in flexibility, reliability, and bandwidth occupation outweigh those costs for large-scale systems. Public-key architectures can be based on signature or asymmetrical encryption. Developing secure authentication frameworks using them is necessary to reach acceptable levels of security for large-scale UTM.

6.5 Quantum-resistant solutions

Post-quantum solutions will be needed against the approaching threat of quantum computing. The first Post-Quantum Cryptography (PQC) standards have been chosen by the NIST in July 2022 [81], but they are not lightweight. Quantum-resistant lightweight algorithms exist ([82]), but they need more testing to be approved as secure against modern cryptanalysis.

6.6 Securing broadcast communications

UTM will also need a signature system, as broadcast messages need to be authenticated. This concerns both the emergency broadcast from the UTM system as well as any broadcast message by UAS during operations (telemetry information for surveillance, detect-and-avoid messages, environmental information...). A signature system will authenticate the messages impacting UTM safety without initiating two-way secure communication with every intended receiver. The computational overhead and the bandwidth overhead have to be minimized.

6.7 Key management system

Public-key architectures for AKE and signatures require trust in public keys. A Key management system can certify those public keys. This is necessary as nodes will need to authenticate the public keys before initiating AKE or trusting signatures verified with those public keys.

6.8 Lightweight cryptography and large UAVs

UAS with larger UAVs (over 2 kg) are less restricted in terms of performance. They can support more complex software. It can be recommended to embark non-lightweight standards, as they have withstood the test of time, unlike their lightweight counterparts. Due to the increased risk of flying over populated areas, stronger, more reliable security solutions are a relevant alternative. When lightweight standards are considered reliably secure, these systems could also switch to those lighter solutions.

6.9 Conclusion

Research into UAS communication security is relatively recent due to the rapidly developing field of UAVs. This causes a lack of hindsight for developing safe UTM systems. It is therefore important to challenge works of research that could quickly be used in real-world implementations. As the field has no set standards and is developed privately, many works of research will focus on it in the coming years. The goal of this survey is also to help criticize and evaluate these new propositions, and to help in maintaining the airspace as safe as it currently is despite the increase in unmanned traffic.

Acronyms

ADS-B Automatic Dependent Surveillance-Broadcast. 17, 22, 23, 33, 34

AEAD Authenticated Encryption with Associated Data. 12, 33

AES Advanced Encryption Standard. 12, 14, 19, 32, 33

AKA Authenticated Key Agreement. 12, 13, 26–28

AKE Authenticated Key Exchange. 12, 13, 26–28, 37

AP Access Point. 24, 25

ARC Aviation Rukemaking Committee. 3

ATC Air Traffic Control. 7, 8, 17

ATM Air Traffic Management. 3, 7, 9

BVLOS Beyond the Visual Line Of Sight. 2–5, 9, 16, 20, 36

CNS Communications, Navigation and Surveillance. 8, 9

CPU Central Processing Unit. 5, 14

DEM Data Encapsulation Mechanism. 13

DES Data Encryption Standard. 12

DH Diffie-Hellman. 14, 26

DHE Diffie-Hellman Ephemeral. 13

DOS Denial of Service. 20, 21, 23–25

EASA European Aviation Safety Agency. 2, 3, 5, 6

ECC Elliptic Curve Cryptography. 14, 27–30
ECDHE Elliptic Curve Diffie-Hellman Ephemeral. 13
ECDSA Elliptic Curve Digital Signature Algorithm. 13, 27
EdDSA Edwards Curve Digital Signature Algorithm. 13
FAA Federal Aviation Administration. 3, 23, 34
FANET Flying Ad-Hoc Network. 6, 7, 36
FHSS Frequency Hopping Spread Spectrum. 21
FTP File Transfer Protocol. 25
GCS Ground Control Station. 2, 4, 8, 9, 16–21, 27, 34
GNSS Global Navigation Satellite Systems. 4, 20
HMAC Hash-based Message Authentication Code. 11, 27
ICAO International Civil Aviation Organization. 3, 8, 23
IDS Intrusion Detection System. 22
IoD Internet of Drones. 7, 16, 26, 27
IoT Internet of Things. 2, 4, 27, 32
IRS Intelligent Reflecting Surface. 21
KEM Key Encapsulation Mechanism. 13
LWC Lightweight Cryptography. 14
MAC Message Authentication Code. 34
MANET Mobile Ad-Hoc Network. 7, 28
MIMO Multiple-Input Multiple-Output. 21
MITM Man-In-The-Middle. 21, 24, 27, 29
ML Machine Learning. 22, 23
NBAA National Business Aviation Association. 23
NIST National Institute of Standards and Technology. 14, 15, 36
NTSC National Television System Commitee. 19
OTP One-Time-Pad. 11, 33
PAL Phase Alternating Line. 19
PQC Post-Quantum Cryptography. 36
PUF Physical Unclonable Function. 27
RF Radio Frequency. 23
RSA Rivest Shamir Adelman. 12–14, 27, 28
RSA-PSS RSA with Probabilistic Signature Scheme. 13
SDR Software Defined Radio. 20
SECAM Sequential Color and Memory. 19
SESAR Single European Sky ATM Research. 3
SPOF Single Point Of Failure. 26, 27
TLS Transport Layer Protocol. 12, 13, 22, 26, 27
UAS Unmanned Aerial System. 1–4, 6–10, 15–18, 20–22, 24–26, 28, 33–37
UAV Unmanned Aerial Vehicle. 1–10, 15–27, 32, 34, 35, 37
UTM UAV Traffic Management. 1–4, 7–10, 16–18, 21, 22, 25, 32–37
VANET Vehicular Ad-Hoc Network. 7, 24, 28
WSN Wireless Sensor Network. 2, 7, 15
XOR Exclusive Or. 26, 27, 30, 33

References

[1] Hazim Shakhatreh, Ahmad H. Sawalmeh, Ala Al-Fuqaha, Zuochao Dou, Eyad Almaita, Issa Khalil, Noor Shamsiah Othman, Abdallah Khreishah, and Mohsen Guizani. "Unmanned Aerial Vehicles (UAVs): A Survey on Civil Applications and Key Research Challenges". In: *IEEE Access* 7 (2019), pp. 48572–48634. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2019.2909530.

[2] Edison Pignaton de Freitas, Tales Heimfarth, Ivayr Farah Netto, Carlos Eduardo Lino, Carlos Eduardo Pereira, Armando Morado Ferreira, Flávio Rech Wagner, and Tony Larsson. "UAV relay network to support WSN connectivity". In: *International Congress on Ultra Modern Telecommunications and Control Systems*. Oct. 2010, pp. 309–314. DOI: 10.1109/ICUMT.2010.5676621.

[3] *Civil drones (unmanned aircraft)*. URL: https://www.easa.europa.eu/domains/civil-drones (visited on 06/21/2022).

[4] *Easy Access Rules for Unmanned Aircraft Systems - Revision from September 2021*. URL: https://www.easa.europa.eu/document-library/easy-access-rules/online-publications/easy-access-rules-unmanned-aircraft-systems (visited on 06/17/2022).

[5] Aviation Rulemaking Committee. *Unmanned Aircraft Systems Beyond Visual Line of Sight*. Tech. rep. Mar. 2022. URL: https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/UAS_BVLOS_ARC_FINAL_REPORT_03102022.pdf.

[6] Tim McCarthy, Lars Pforte, and Rebekah Burke. "Fundamental Elements of an Urban UTM". In: *Aerospace* 7.7 (July 2020), p. 85. ISSN: 2226-4310. DOI: 10.3390/aerospace7070085. URL: https://www.mdpi.com/2226-4310/7/7/85 (visited on 06/14/2022).

[7] Samira Hayat, Evşen Yanmaz, and Raheeb Muzaffar. "Survey on Unmanned Aerial Vehicle Networks for Civil Applications: A Communications Viewpoint". In: *IEEE Communications Surveys & Tutorials* 18.4 (2016), pp. 2624–2661. ISSN: 1553-877X. DOI: 10.1109/COMST.2016.2560343. URL: https://ieeexplore.ieee.org/document/7463007.

[8] Arslan Shafique, Abid Mehmood, and Mourad Elhadef. "Survey of Security Protocols and Vulnerabilities in Unmanned Aerial Vehicles". In: *IEEE Access* 9 (2021), pp. 46927–46948. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2021.3066778.

[9] Abhishek Sharma, Pankhuri Vanjani, Nikhil Paliwal, Chathuranga M. Wijerathna Basnayaka, Dushantha Nalin K. Jayakody, Hwang-Cheng Wang, and P. Muthuchidambaranathan. "Communication and networking technologies for UAVs: A survey". In: *Journal of Network and Computer Applications* 168 (Oct. 2020). ISSN: 1084-8045. DOI: 10.1016/j.jnca.2020.102739. URL: https://www.sciencedirect.com/science/article/pii/S1084804520302137 (visited on 02/23/2022).

[10] Xuefei Chen. *Documents - Draft Glossary of terms.docx*. Tech. rep. Aug. 2017. URL: https://www.icao.int/safety/cargosafety/Documents/Forms/AllItems.aspx (visited on 10/19/2022).

[11] Cristina Barrado, Mario Boyero, Luigi Brucculeri, Giancarlo Ferrara, Andrew Hately, Peter Hullah, David Martin-Marrero, Enric Pastor, Anthony Peter Rushton, and Andreas Volkert. "U-Space Concept of Operations: A Key Enabler for Opening Airspace to Emerging Low-Altitude Operations". In: *Aerospace* 7.3 (Mar. 2020), p. 24. ISSN: 2226-4310. DOI: 10.3390/aerospace7030024. URL: https://www.mdpi.com/2226-4310/7/3/24 (visited on 11/17/2022).

[12] Ben Nassi, Asaf Shabtai, Ryusuke Masuoka, and Yuval Elovici. "SoK - Security and Privacy in the Age of Drones: Threats, Challenges, Solution Mechanisms, and Scientific Gaps". In: *CoRR* abs/1903.05155 (2019). arXiv: 1903.05155. URL: http://arxiv.org/abs/1903.05155 (visited on 06/21/2022).

[13] *Open Category - Civil Drones*. URL: https://www.easa.europa.eu/domains/civil-drones/drones-regulatory-framework-background/open-category-civil-drones (visited on 06/21/2022).

[14] Lidong Zhou and Z.J. Haas. "Securing ad hoc networks". In: *IEEE Network* 13.6 (Nov. 1999), pp. 24–30. ISSN: 1558-156X. DOI: 10.1109/65.806983.

[15] *MANET vs VANET vs FANET-Difference between MANET,VANET,FANET*. URL: https://www.rfwireless-world.com/Terminology/MANET-vs-VANET-vs-FANET.html (visited on 06/21/2022).

[16] Amira Chriki, Haifa Touati, Hichem Snoussi, and Farouk Kamoun. "FANET: Communication, mobility models and security issues". In: *Computer Networks* 163 (Nov. 2019). ISSN: 1389-1286. DOI: 10.1016/j.comnet.2019.106877. URL: https://www.sciencedirect.com/science/article/pii/S1389128618309034 (visited on 06/21/2022).

[17] Mohamed Nidhal Mejri, Jalel Ben-Othman, and Mohamed Hamdi. "Survey on VANET security challenges and possible cryptographic solutions". In: *Vehicular Communications* 1.2 (Apr. 2014), pp. 53–66. ISSN: 2214-2096. DOI: 10.1016/j.vehcom.2014.05.001. URL: https://www.sciencedirect.com/science/article/pii/S2214209614000187 (visited on 11/15/2022).

[18] Sunilkumar S. Manvi and Shrikant Tangade. "A survey on authentication schemes in VANETs for secured communication". In: *Vehicular Communications* 9 (July 2017), pp. 19–30. ISSN: 2214-2096. DOI: 10.1016/j.vehcom.2017.02.001. URL: https://www.sciencedirect.com/science/article/pii/S2214209616300018 (visited on 11/15/2022).

[19] Surbhi Sharma and Baijnath Kaushik. "A survey on internet of vehicles: Applications, security issues & solutions". In: *Vehicular Communications* 20 (Dec. 2019). ISSN: 2214-2096. DOI: 10.1016/j.vehcom.2019.100182. URL: https://www.sciencedirect.com/science/article/pii/S2214209619302293 (visited on 11/15/2022).

[20] Mirmojtaba Gharibi, Raouf Boutaba, and Steven L. Waslander. "Internet of Drones". In: *IEEE Access* 4 (2016), pp. 1148–1162. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2016.2537208.

[21] Laith Abualigah, Ali Diabat, Putra Sumari, and Amir H. Gandomi. "Applications, Deployments, and Integration of Internet of Drones (IoD): A Review". In: *IEEE Sensors Journal* 21.22 (Nov. 2021), pp. 25532–25546. ISSN: 1558-1748. DOI: 10.1109/JSEN.2021.3114266.

[22] ICAO. *Unmanned Aircraft Systems Traffic Management (UTM) – A Common Framework with Core Principles for Global Harmonization*. Tech. rep. 2019, p. 45. URL: https://www.icao.int/safety/UA/Documents/UTM%20Framework%20Edition%203.pdf.

[23] Xiaofang Sun, Derrick Wing Kwan Ng, Zhiguo Ding, Yanqing Xu, and Zhangdui Zhong. "Physical Layer Security in UAV Systems: Challenges and Opportunities". In: *IEEE Wireless Communications* 26.5 (Oct. 2019), pp. 40–47. ISSN: 1558-0687. DOI: 10.1109/MWC.001.1900028.

[24] Qingqing Wu, Weidong Mei, and Rui Zhang. "Safeguarding Wireless Network with UAVs: A Physical Layer Security Perspective". In: *IEEE Wireless Communications* 26.5 (Oct. 2019), pp. 12–18. ISSN: 1558-0687. DOI: 10.1109/MWC.001.1900050.

[25] Hui-Ming Wang, Xu Zhang, and Jia-Cheng Jiang. "UAV-Involved Wireless Physical-Layer Secure Communications: Overview and Research Directions". In: *IEEE Wireless Communications* 26.5 (Oct. 2019), pp. 32–39. ISSN: 1558-0687. DOI: 10.1109/MWC.001.1900045.

[26] R. L. Rivest, A. Shamir, and L. Adleman. "A method for obtaining digital signatures and public-key cryptosystems". In: *Communications of the ACM* 21.2 (Feb. 1978), pp. 120–126. ISSN: 0001-0782. DOI: 10.1145/359340.359342. URL: https://doi.org/10.1145/359340.359342 (visited on 11/15/2022).

[27] T. Elgamal. "A public key cryptosystem and a signature scheme based on discrete logarithms". In: *IEEE Transactions on Information Theory* 31.4 (July 1985), pp. 469–472. ISSN: 1557-9654. DOI: 10.1109/TIT.1985.1057074.

[28] P.W. Shor. "Algorithms for quantum computation: discrete logarithms and factoring". In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. Nov. 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.

[29] Lov K Grover. "A fast quantum mechanical algorithm for database search". In: *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*. 1996, pp. 212–219. URL: https://arxiv.org/abs/quant-ph/9605043 (visited on 10/19/2022).

[30] Information Technology Laboratory Computer Security Division. *Post-Quantum Cryptography — CSRC — CSRC*. Jan. 2017. URL: https://csrc.nist.gov/Projects/post-quantum-cryptography (visited on 06/23/2022).

[31] Information Technology Laboratory Computer Security Division. *Lightweight Cryptography — CSRC — CSRC*. Jan. 2017. URL: https://csrc.nist.gov/projects/lightweight-cryptography (visited on 06/22/2022).

[32] ICAO. *ADS-B Implementation and operations Guidance Document*. Tech. rep. July 2018. URL: https://www.icao.int/APAC/Documents/edocs/AIGD%20Edition%2011.pdf (visited on 06/24/2022).

[33] Young-Min Kwon, Jaemin Yu, Byeong-Moon Cho, Yongsoon Eun, and Kyung-Joon Park. "Empirical Analysis of MAVLink Protocol Vulnerability for Attacking Unmanned Aerial Vehicles". In: *IEEE Access* 6 (2018), pp. 43203–43212. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2018.2863237.

[34] Canhui Zhong, Jianping Yao, and Jie Xu. "Secure UAV Communication With Cooperative Jamming and Trajectory Control". In: *IEEE Communications Letters* 23.2 (Feb. 2019), pp. 286–289. ISSN: 1558-2558. DOI: 10.1109/LCOMM.2018.2889062.

[35] H. Vincent Poor and Rafael F. Schaefer. "Wireless physical layer security". In: *Proceedings of the National Academy of Sciences* 114.1 (Jan. 2017), pp. 19–26. DOI: 10.1073/pnas.1618130114. URL: https://www.pnas.org/doi/full/10.1073/pnas.1618130114 (visited on 05/25/2022).

[36] Shikun Chen, Simin Yu, Jinhu Lü, Guanrong Chen, and Jianbin He. "Design and FPGA-Based Realization of a Chaotic Secure Video Communication System". In: *IEEE Transactions on Circuits and Systems for Video Technology* 28.9 (Sept. 2018), pp. 2359–2371. ISSN: 1558-2205. DOI: 10.1109/TCSVT.2017.2703946.

[37] Hossein Pirayesh and Huacheng Zeng. "Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey". In: *IEEE Communications Surveys & Tutorials* 24.2 (2022), pp. 767–809. ISSN: 1553-877X. DOI: 10.1109/COMST.2022.3159185.

[38] Karel Pärlin, Muhammad Mahtab Alam, and Yannick Le Moullec. "Jamming of UAV remote control systems using software defined radio". In: *2018 International Conference on Military Communications and Information Systems (ICMCIS)*. May 2018, pp. 1–6. DOI: 10.1109/ICMCIS.2018.8398711.

[39] Qingqing Wu and Rui Zhang. "Intelligent Reflecting Surface Enhanced Wireless Network via Joint Active and Passive Beamforming". In: *IEEE Transactions on Wireless Communications* 18.11 (Nov. 2019), pp. 5394–5409. ISSN: 1558-2248. DOI: 10.1109/TWC.2019.2936025.

[40] Ottilia Westerlund and Rameez Asif. "Drone Hacking with Raspberry-Pi 3 and WiFi Pineapple: Security and Privacy Threats for the Internet-of-Things". In: *1st International Conference on Unmanned Vehicle Systems-Oman (UVS)*. Feb. 2019, pp. 1–10. DOI: 10.1109/UVS.2019.8658279.

[41] Eirini Anthi, Lowri Williams, Małgorzata Słowińska, George Theodorakopoulos, and Pete Burnap. "A Supervised Intrusion Detection System for Smart Home IoT Devices". In: *IEEE Internet of Things Journal* 6.5 (Oct. 2019), pp. 9042–9053. ISSN: 2327-4662. DOI: 10.1109/JIOT.2019.2926365.

[42] Hichem Sedjelmaci, Sidi Mohammed Senouci, and Nirwan Ansari. "A Hierarchical Detection and Response System to Enhance Security Against Lethal Cyber-Attacks in UAV Networks". In: *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 48.9 (Sept. 2018), pp. 1594–1606. ISSN: 2168-2232. DOI: 10.1109/TSMC.2017.2681698. URL: https://ieeexplore.ieee.org/document/7890467.

[43] *NBAA: Privacy, Security Concerns Remain Regarding UAS Remote ID Final Rule*. Jan. 2021. URL: https://nbaa.org/aircraft-operations/emerging-technologies/uas/nbaa-privacy-security-concerns-remain-regarding-uas-remote-id-final-rule/ (visited on 06/15/2022).

[44] Martins Ezuma, Fatih Erden, Chethan Kumar Anjinappa, Ozgur Ozdemir, and Ismail Guvenc. "Micro-UAV Detection and Classification from RF Fingerprints Using Machine Learning Techniques". In: *2019 IEEE Aerospace Conference*. Mar. 2019, pp. 1–13. DOI: 10.1109/AERO.2019.8741970.

[45] Martins Ezuma, Fatih Erden, Chethan Kumar Anjinappa, Ozgur Ozdemir, and Ismail Guvenc. "Detection and Classification of UAVs Using RF Fingerprints in the Presence of Wi-Fi and Bluetooth Interference". In: *IEEE Open Journal of the Communications Society* 1 (2020), pp. 60–76. ISSN: 2644-125X. DOI: 10.1109/OJCOMS.2019.2955889.

[46] Abdulhadi Shoufan, Haitham M. Al-Angari, Muhammad Faraz Afzal Sheikh, and Ernesto Damiani. "Drone Pilot Identification by Classifying Radio-Control Signals". In: *IEEE Transactions on Information Forensics and Security* 13.10 (Oct. 2018), pp. 2439–2447. ISSN: 1556-6021. DOI: 10.1109/TIFS.2018.2819126.

[47] Anas Alsoliman, Abdulrahman Bin Rabiah, and Marco Levorato. "Privacy-Preserving Authentication Framework for UAS Traffic Management Systems". In: *4th Cyber Security in Networking Conference (CSNet)*. Oct. 2020, pp. 1–8. DOI: 10.1109/CSNet50428.2020.9265534.

[48] *ADS-B Privacy*. URL: https://www.faa.gov/air_traffic/technology/equipadsb/privacy/ (visited on 06/15/2022).

[49] J Godwin Ponsam and R Srinivasan. "A survey on MANET security challenges, attacks and its countermeasures". In: *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)* 3.1 (2014), pp. 274–279. URL: https://www.ijarcce.com/upload/2016/august-16/IJARCCE%20129.pdf (visited on 06/09/2022).

[50] Daojing He, Sammy Chan, and Mohsen Guizani. "Drone-Assisted Public Safety Networks: The Security Aspect". In: *IEEE Communications Magazine* 55.8 (Aug. 2017), pp. 218–223. ISSN: 1558-1896. DOI: 10.1109/MCOM.2017.1600799CM.

[51] Michael Hooper, Yifan Tian, Runxuan Zhou, Bin Cao, Adrian P. Lauf, Lanier Watkins, William H. Robinson, and Wlajimir Alexis. "Securing commercial WiFi-based UAVs from common security attacks". In: *MILCOM 2016 - IEEE Military Communications Conference*. Nov. 2016, pp. 1213–1218. DOI: 10.1109/MILCOM.2016.7795496. URL: https://ieeexplore.ieee.org/document/7795496.

[52] David Rudo and Dr Kai Zeng. "Consumer UAV Cybersecurity Vulnerability Assessment Using Fuzzing Tests". In: arXiv:2008.03621 (Aug. 2020). DOI: 10.48550/arXiv.2008.03621. URL: http://arxiv.org/abs/2008.03621 (visited on 05/25/2022).

[53] Mohammad Wazid, Ashok Kumar Das, Neeraj Kumar, Athanasios V. Vasilakos, and Joel J. P. C. Rodrigues. "Design and Analysis of Secure Lightweight Remote User Authentication and Key Agreement Scheme in Internet of Drones Deployment". In: *IEEE Internet of Things Journal* 6.2 (Apr. 2019), pp. 3572–3584. ISSN: 2327-4662. DOI: 10.1109/JIOT.2018.2888821.

[54] Jangirala Srinivas, Ashok Kumar Das, Neeraj Kumar, and Joel J. P. C. Rodrigues. "TCALAS: Temporal Credential-Based Anonymous Lightweight Authentication Scheme for Internet of Drones Environment". In: *IEEE Transactions on Vehicular Technology* 68.7 (July 2019), pp. 6903–6916. ISSN: 1939-9359. DOI: 10.1109/TVT.2019.2911672. URL: https://ieeexplore.ieee.org/document/8693567.

[55] Zeeshan Ali, Shehzad Ashraf Chaudhry, Muhammad Sher Ramzan, and Fadi Al-Turjman. "Securing Smart City Surveillance: A Lightweight Authentication Mechanism for Unmanned Vehicles". In: *IEEE Access* 8 (2020), pp. 43711–43724. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2020.2977817.

[56] Muhammad Tanveer, Amjad Hussain Zahid, Musheer Ahmad, Abdullah Baz, and Hosam Alhakami. "LAKE-IoD: Lightweight Authenticated Key Exchange Protocol for the Internet of Drone Environment". In: *IEEE Access* 8 (2020), pp. 155645–155659. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2020.3019367. URL: https://ieeexplore.ieee.org/document/9176990.

[57] Cong Pu and Yucheng Li. "Lightweight Authentication Protocol for Unmanned Aerial Vehicles Using Physical Unclonable Function and Chaotic System". In: *IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN)*. July 2020, pp. 1–6. DOI: 10.1109/LANMAN49260.2020.9153239.

[58] Yunru Zhang, Debiao He, Li Li, and Biwen Chen. "A lightweight authentication and key agreement scheme for Internet of Drones". In: *Computer Communications* 154 (Mar. 2020), pp. 455–464. ISSN: 0140-3664. DOI: 10.1016/j.comcom.2020.02.067. URL: https://www.sciencedirect.com/science/article/pii/S0140366419319358 (visited on 09/07/2022).

[59] Geumhwan Cho, Junsung Cho, Sangwon Hyun, and Hyoungshick Kim. "SENTINEL: A Secure and Efficient Authentication Framework for Unmanned Aerial Vehicles". In: *Applied Sciences* 10.9 (Apr. 2020). ISSN: 2076-3417. DOI: 10.3390/app10093149. URL: https://www.mdpi.com/2076-3417/10/9/3149 (visited on 02/22/2022).

[60] Saeed Ullah Jan, Fawad Qayum, and Habib Ullah Khan. "Design and Analysis of Lightweight Authentication Protocol for Securing IoD". In: *IEEE Access* 9 (2021), pp. 69287–69306. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2021.3076692.

[61] Mahdi Nikooghadam, Haleh Amintoosi, SK Hafizul Islam, and Mostafa Farhadi Moghadam. "A provably secure and lightweight authentication scheme for Internet of Drones for smart city surveillance". In: *Journal of Systems Architecture* 115 (May 2021). ISSN: 1383-7621. DOI: 10.1016/j.sysarc.2020.101955. URL: https://www.sciencedirect.com/science/article/pii/S138376212030206X (visited on 09/07/2022).

[62] Muhamed Turkanović, Boštjan Brumen, and Marko Hölbl. "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion". In: *Ad Hoc Networks* 20 (Sept. 2014), pp. 96–112. ISSN: 1570-8705. DOI: 10.1016/j.adhoc.2014.03.009. URL: https://www.sciencedirect.com/science/article/pii/S157087051400064X (visited on 06/15/2022).

[63] Mohammad Sabzinejad Farash, Muhamed Turkanović, Saru Kumari, and Marko Hölbl. "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment". In: *Ad Hoc Networks* 36 (Jan. 2016), pp. 152–176. ISSN: 1570-8705. DOI: 10.1016/j.adhoc.2015.05.014. URL: https://www.sciencedirect.com/science/article/pii/S1570870515001195 (visited on 09/07/2022).

[64] Ruhul Amin, SK Hafizul Islam, G. P. Biswas, Muhammad Khurram Khan, Lu Leng, and Neeraj Kumar. "Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks". In: *Computer Networks*. Industrial Technologies and Applications for the Internet of Things 101 (June 2016), pp. 42–62. ISSN: 1389-1286. DOI: 10.1016/j.comnet.2016.01.006. URL: https://www.sciencedirect.com/science/article/pii/S1389128616000207 (visited on 09/07/2022).

[65] Manuel Suárez-Albela, Tiago M. Fernández-Caramés, Paula Fraga-Lamas, and Luis Castedo. "A Practical Performance Comparison of ECC and RSA for Resource-Constrained IoT Devices". In: *Global Internet of Things Summit (GIoTS)*. June 2018, pp. 1–6. DOI: 10.1109/GIOTS.2018.8534575.

[66] Sandip Roy, Santanu Chatterjee, Ashok Kumar Das, Samiran Chattopadhyay, Saru Kumari, and Minho Jo. "Chaotic Map-Based Anonymous User Authentication Scheme With User Biometrics and Fuzzy Extractor for Crowdsourcing Internet of Things". In: *IEEE Internet of Things Journal* 5.4 (Aug. 2018), pp. 2884–2895. ISSN: 2327-4662. DOI: 10.1109/JIOT.2017.2714179. URL: https://ieeexplore.ieee.org/document/7945557.

[67] Sravani Challa, Ashok Kumar Das, Vanga Odelu, Neeraj Kumar, Saru Kumari, Muhammad Khurram Khan, and Athanasios V. Vasilakos. "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks". In: *Computers & Electrical Engineering* 69 (July 2018), pp. 534–554. ISSN: 0045-7906. DOI: 10.1016/j.compeleceng.2017.08.003. URL: https://www.sciencedirect.com/science/article/pii/S0045790616302622 (visited on 02/23/2022).

[68] Debiao He, Sherali Zeadally, Baowen Xu, and Xinyi Huang. "An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks". In: *IEEE Transactions on Information Forensics and Security* 10.12 (Dec. 2015), pp. 2681–2691. ISSN: 1556-6021. DOI: 10.1109/TIFS.2015.2473820.

[69] Gaëtan Leurent and Thomas Peyrin. "From collisions to chosen-prefix collisions application to full SHA-1". In: *Advances in Cryptology–EUROCRYPT 2019*. Springer. May 2019, pp. 527–555.

[70] Luke E. Kane, Jiaming James Chen, Rebecca Thomas, Vicky Liu, and Matthew Mckague. "Security and Performance in IoT: A Balancing Act". In: *IEEE Access* 8 (2020), pp. 121969–121986. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2020.3007536.

[71] Mohammed Salih Mahdi, Nidaa Falih Hassan, and Ghassan H. Abdul-Majeed. "An improved chacha algorithm for securing data on IoT devices". In: *SN Applied Sciences* 3.4 (Mar. 2021). ISSN: 2523-3971. DOI: 10.1007/s42452-021-04425-7. URL: https://doi.org/10.1007/s42452-021-04425-7 (visited on 06/14/2022).

[72] Hongjun Wu and Bart Preneel. "AEGIS: A Fast Authenticated Encryption Algorithm". In: *Selected Areas in Cryptography – SAC 2013*. Ed. by Tanja Lange, Kristin Lauter, and Petr Lisoněk. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2014, pp. 185–201. ISBN: 978-3-662-43414-7. DOI: 10.1007/978-3-662-43414-7_10.

[73] Ivan Avdonin, Marina Budko, Mikhail Budko, Vladimir Grozov, and Alexei Guirik. "A method of creating perfectly secure data transmission channel between unmanned aerial vehicle and ground control station based on One-Time pads". In: *9th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*. Munich, Germany, Nov. 2017, pp. 410–413. DOI: 10.1109/ICUMT.2017.8255167. URL: https://ieeexplore.ieee.org/document/8255167.

[74] Joonsang Baek, Young-Ji Byon, Eman Hableel, and Mahmoud Al-Qutayri. "An Authentication Framework for Automatic Dependent Surveillance-Broadcast Based on Online/Offline Identity-Based Signature". In: *Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*. Oct. 2013, pp. 358–363. DOI: 10.1109/3PGCIC.2013.61.

[75] Anjia Yang, Xiao Tan, Joonsang Baek, and Duncan S. Wong. "A New ADS-B Authentication Framework Based on Efficient Hierarchical Identity-Based Signature with Batch Verification". In: *IEEE Transactions on Services Computing* 10.2 (Mar. 2017), pp. 165–175. ISSN: 1939-1374. DOI: 10.1109/TSC.2015.2459709.

[76] Haomiao Yang, Mingxuan Yao, Zili Xu, and Baoshu Liu. "LHCSAS: A Lightweight and Highly-Compatible Solution for ADS-B Security". In: *GLOBECOM 2017 - IEEE Global Communications Conference*. Dec. 2017, pp. 1–7. DOI: 10.1109/GLOCOM.2017.8254500.

[77] Haomiao Yang, Qixian Zhou, Mingxuan Yao, Rongxing Lu, Hongwei Li, and Xiaosong Zhang. "A Practical and Compatible Cryptographic Solution to ADS-B Security". In: *IEEE Internet of Things Journal* 6.2 (Apr. 2019), pp. 3322–3334. ISSN: 2327-4662. DOI: 10.1109/JIOT.2018.2882633.

[78] Ijaz Ahmad, Shahriar Shahabuddin, Tanesh Kumar, Jude Okwuibe, Andrei Gurtov, and Mika Ylianttila. "Security for 5G and Beyond". In: *IEEE Communications Surveys & Tutorials* 21.4 (2019), pp. 3682–3722. ISSN: 1553-877X. DOI: 10.1109/COMST.2019.2916180.

[79] *RemoteID Final Rule — Federal Aviation Administration*. URL: https://www.faa.gov/newsroom/remoteid-final-rule (visited on 09/13/2022).

[80] Alessandro Brighente, Mauro Conti, and Savio Sciancalepore. "Hide and Seek: Privacy-Preserving and FAA-compliant Drones Location Tracing". In: *Proceedings of the 17th International Conference on Availability, Reliability and Security*. ARES '22. Aug. 2022, pp. 1–11. ISBN: 978-1-4503-9670-7. DOI: 10.1145/3538969.3543784. URL: https://doi.org/10.1145/3538969.3543784 (visited on 09/13/2022).

[81] Information Technology Laboratory Computer Security Division. *Selected Algorithms 2022 - Post-Quantum Cryptography — CSRC — CSRC*. July 2022. URL: https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022 (visited on 01/23/2023).

[82] Henrique Faria and José Manuel Valença. "Post-Quantum Authentication with Lightweight Cryptographic Primitives". In: *Cryptology ePrint Archive* (2021). URL: https://eprint.iacr.org/2021/1298 (visited on 01/23/2023).