Surveying cryptographic methods for UAV communications

Ridwane Aissaoui*, Jean-Christophe Deneuville*, Christophe Guerber*, Alain Pirovano*
*ENAC, French Civil Aviation University, Toulouse
first.last@enac.fr

***Abstract*—This article presents our survey work on Unmanned Aerial Vehicle (UAV) communication security for UAV Traffic Management (UTM) safety [1]. A majority of UAV missions require flying through public airspace. Airspace management is a sector with very high safety standards, as can be seen with commercial civil aviation. Reliable communication links between aircraft, their pilots and UTM systems are necessary to safely carry out these missions. Several security properties have to be provided in order to ensure a safe traffic. Current cryptographic standards used over the internet are not suitable to Unmanned Aerial System (UAS), mainly due to their computational complexity. The survey discusses every communication link and assesses the security needs in order to enable a safe traffic management. We then present and discuss several research works providing the required properties using cryptographic primitives. In particular, authenticated key exchange protocols specifically developed for constrained systems are compared and evaluated as solutions for UAS security. We also discuss symmetric encryption alternatives to the AES algorithm as well as works to secure current UTM protocols such as ADS-B and RemoteID. The analysis reveals a lack of signature solutions, the need for the development of a complete secure architecture able to provide authentication and integrity and a need for post-quantum lightweight solutions. We then present our current work which focuses on implementing post-quantum signature standards for UAS.**

Keywords : UAV, Drone, UAS, UTM, Information Security, Cryptography, Authentication, Safety

I. Introduction

A. Unmanned aerial systems applications and traffic management

There are many operations that a civil UAV carries out in a safer and more timely efficient manner than humans [2]. The UAV sector is strongly growing, with more operating capabilities being researched. Infrastructure monitoring, deliveries or surveillance are examples of such applications. Many of these applications require operating Beyond the Visual Line Of Sight (BVLOS), thus requiring more attention to safety and security. The aircraft are indeed controlled remotely, and cannot be visually monitored to ensure flight safety.

B. UAS security issues

UAS are targeted by numerous cyberthreats. They can contain sensitive and private information, they can transport payloads of large financial or human value (high end goods or medical supplies) which can be hijacked by attackers if the UAS is compromised. They also pose a physical threat to the public with their kinetic energy. It is therefore important to protect UASs against cyber attacks.

C. UAS Communications

A UAS is comprised of every part and communication mean used to operate a UAV. It is at minimum composed of a UAV and a Ground Control Station (GCS). Advanced UAS operating BVLOS include more actors such as UTM systems and intermediate ground stations. Three main communication axis can be found in a UAS (Figure 1). Command, telemetry, video and other mission specific data links exist between a UAV and a GCS. These links can be physically or logically separated, as these different types of data are not always sent on the same channel. A second axis exists between the UAS and the UTM systems when flying in controlled airspace. The UAS transmits telemetry information which serves to monitor the traffic and manage the airspace. And the UTM systems can transmit emergency geofencing zones (broadcast) and specific control information to a single UAS. A third type of communications exists between two UAVs. They can share environmental information with one another, or be used as routers to transmit data to a remote GCS or the UTM.

Defending against cyber attacks can require computation power, memory space, bandwidth, sizable software or dedicated hardware. UAS are highly constrained systems, and their operability is partially based on the cost-efficiency of their usage. The defense mechanisms have to be adapted and optimized to be efficiently implemented. More specifically, information security in communications is mostly based on cryptography. Lightweight cryptographic primitives are developed for constrained systems, aiming to provide sufficient security while requiring less resources.

II. UAS security requirements and cryptographic solutions

The survey evaluates the security requirements for UASs communications. BVLOS operations are used for security evaluation as they represent the focus point of UTM research [3]. This means that the video link is critical for UAV control, alongside the command link. Safe traffic management requires different levels of information security :

- 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

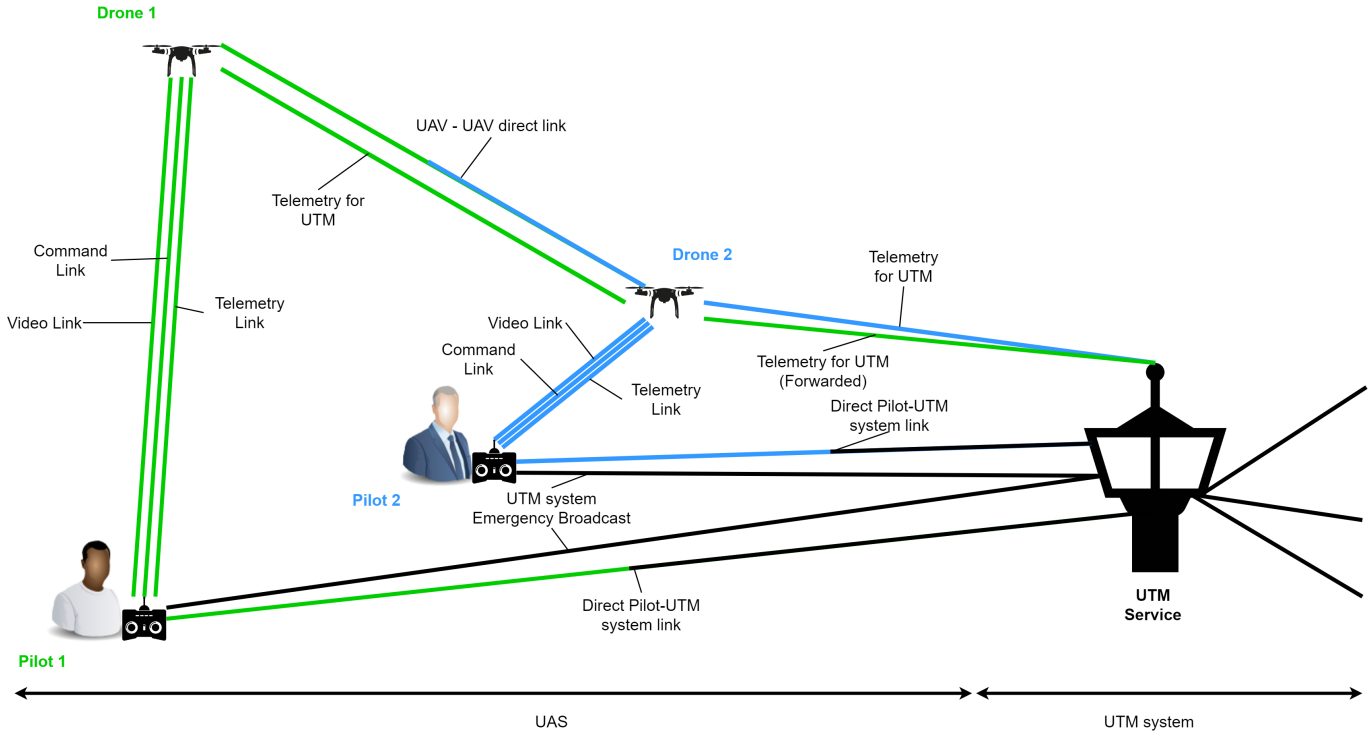

Fig. 1. UAS with UTM system organisation. Green links originate from UAS 1, blue links from UAS 2 and black links from the UTM system. Two-color links contain data from both sources.

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 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 of these links, confidentiality is a privacy concern, and does not directly impact safety. However it is important to consider it when designing a system, as privacy issues have to be addressed. Moreover, the safety of the system can be indirectly impacted by the lack of confidentiality (*i.e.* intercepting a drone by anticipating its trajectory). The same reasoning holds for non-repudiation, which is a traceability issue. This property is necessary to allow authorities to investigate past incidents, but does not directly impact air traffic safety. Authentication is provided through encryption; which also provides confidentiality; or through signature, which also provides non-repudiation. In the survey, confidentiality and non-repudiation are discussed when addressed by research works but not considered as a major issue regarding UTM safety.

Table I presents the security properties needed to safely operate a drone in a BVLOS mission.

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 I
UAS LINKS AND THEIR SECURITY REQUIREMENTS (CONFIDENTIALITY, INTEGRITY, AUTHENTICATION, NON-REPUDIATION).

The survey details Authenticated Key Agreement (AKA), symmetric encryption algorithms and signature for these specific needs. The different AKA's performance are compared using the following metrics :

- 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.
- The computation overhead represents the number of CPU cycles required for authentication.
- The memory overhead is the space taken in memory by the protocol parameters for authentication (IVs, keys...).

The survey presents symmetric encryption algorithms and signature schemes with their benefits and drawbacks compared to current standards.

III. Takeaways, current work and future directions

The authentication protocols presented in the survey lack upscaling and real implementation. Choosing these solutions is not currently recommended due to the lack of testing.

Though a lot of research has focused on developing security protocols for UAS, there is no proposition for a complete security architecture. Integrating the relevant cryptographic solutions into a global scheme is necessary to meet the security goals required for a secure traffic management. By choosing certain algorithms and implementations, it is possible to optimize the implementation for a specific UTM architecture.

UAS with larger UAVs (over 2 kg) are less restricted in terms of performance. 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 for flying over populated areas, stronger, more reliable security solutions are a relevant alternative.

Many authentication protocols rely on passwords, but this is not optimized for large scale infrastructures for which public-key architectures will be necessary. Their cost in terms of computation is a lot higher, but the benefits in terms of flexibility, reliability, and bandwidth occupation outweigh those costs. Developing secure authentication frameworks using public-key architectures is necessary to reach acceptable levels of security for large scale UTM.

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 National Institute of Standards and Technology (NIST) in July 2022 [4], but they are not lightweight. Quantum resistant lightweight algorithms exist ([5]), but they need more testing to be approved as secure against modern cryptanalysis.

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 (detect and avoid systems, environmental information...).

Following the conclusions of the survey, our current work focuses on implementing the Falcon and CRYSTALS-Dilithium signature standards [4] for broadcasts communications. Falcon was chosen due to its smaller signature size and computational complexity compared to the other two standards (CRYSTALS-Dilithium and SPHINCS+), but CRYSTALS-Dilithium was also retained as preliminary results show that its computational complexity is better than Falcon on heavily constrained hardware. We will implement them with different levels of security on representative hardware, to study the impact it causes on performance and improve its lightweight properties. We will also study the impact of background processing tasks on the performance of each scheme. After evaluating signature algorithms, we will extend this process to Authenticated Key Exchange (AKE) standards.

IV. 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 into real-world implementations. As UTM has very few set standards and is mainly developed privately, many will focus on its improvements in the coming years. The goal of this work 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.

References

[1] Ridwane Aissaoui, Jean-Christophe Deneuville, Christophe Guerber, and Alain Pirovano. *UAV Traffic Management : A Survey On Communication Security*. Nov. 2022. DOI: 10.48550/arXiv.2211.05640. URL: http://arxiv.org/abs/2211.05640.

[2] 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.

[3] 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.

[4] Information Technology Laboratory Computer Security Division. *Selected Algorithms 2022 - Post-Quantum Cryptography — CSRC — CSRC*. Jan. 2017. URL: https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022.

[5] 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.