2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)

Global and Secured UAV Authentication System based on Hardware-Security

Dominic Pirker*†, Thomas Fischer*†, Christian Lesjak†, Christian Steger*
Email: {dominic.pirker, thomas.fischer3, christian.lesjak}@infineon.com, steger@tugraz.at
*Institute for Technical Informatics, Graz University of Technology, Graz, Austria
†Development Center Graz, Infineon Technologies AG, Graz, Austria

***Abstract*—UAVs are gaining traction outside their usual markets of hobbyists, areal recordings, and surveillance services with cloud computing enabled applications and their massive combined computing power. These applications rapidly grow the UAV market, consequently raising the priority of safety solutions. Tremendous incidents, such as the air traffic interruption in London (Dec. 2018), raised awareness and demand for UAV identification, authentication, and tracking. To prevent these type of incidents, aviation authorities, such as the FAA or EASA, are currently working on proper regulations. The implementation of the regulations demands dependable technical solutions.**

This paper proposes a secured and globally operative UAV authentication system, based on reliable security mechanisms and standardized protocols. Therefore, this system must provide mutual and strong cryptographic authentication. First, the TLS protocol is used for mutual authentication and for protecting the communication. Then, hardware-security is implemented to store the necessary keys and certificates in a protected storage, thus supporting the TLS handshake to avoid common attacks against pure software implementations. Lastly, a concept for protected sensor values is introduced. The proposed UAV authentication concept is demonstrated by a proof-of-concept implementation, evaluated for performance and compared to existing solutions.

***Index Terms*—UAV, authentication, protected sensor values, TLS, hardware-security**

I. Introduction

Unmanned Aerial Vehicle (UAV) identification is an issue with increasing concern, especially these days, as several international high profile incidents occurred. One of the most important aspects is preventing UAVs from flying into, or over, critical zones. These zones could be airports, power plants, crowded places, oil pipelines etc.

In this work, we propose a concept for a global and secured UAV authentication system for commercial UAVs and evaluate it against other solutions. The proposed system provides secured authentication of UAVs to flight control reliably. Due to the fact that standardized protocols, a certified Hardware Security Module (HSM), and a globally available physical link are used, the proposed authentication system could be attractive for upcoming regulations. In Fig. 1 the general use case diagram for a UAV authentication system is depicted. A pilot wants to steer a UAV. The UAV, and thus, its pilot, must authenticate and send its location information to a flight control server managed by a regional authority. In case of a forbidden movement or action of the UAV, the pilot needs to be informed by the flight control server, based on regulations and rules defined by the regional authority.

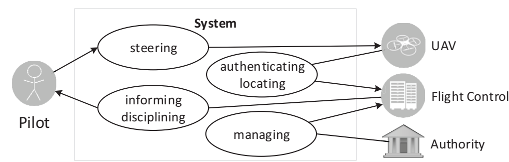

Fig. 1. Use case diagram for authenticated UAV steering

II. State-of-the-Art

Until now, there are no regulations to consider regarding digital identification of UAVs. In this context, authentication is a cryptographically verifiable identification. Regulations for UAV authentication are non-existent. UAVs are a heavily discussed topic on EU level, where the European Union Aviation Safety Agency (EASA) is the responsible authority and the Federal Aviation Administration (FAA) is the american equivalent. Starting mid 2019, regulations for operation of UAVs have been gradually released and the EASA expects full applicability by 2022 [1].

Independent of the authorities draft regulations, several systems are being developed to control the increasing market of civilian UAVs. The concepts of the systems under development differ, but most concepts are inappropriate for two reasons. First, most systems require a detection prior to the actual identification, for instance radar-based approaches. Second, the majority of the systems require base stations, leading to tremendous infrastructural costs, as every region to be observed must be in the range of a base station.

The main contributions of this work are:

- Proposal of a global and secured UAV authentication system with sensor values protected against remote attacks
- Design and implementation of a proof-of-concept for the proposed system supported by an HSM
- Evaluation against existing systems and analysis of potential threats

A. Vodafone RPS

Vodafone is developing a system called Vodafone Radio Positioning System (RPS), based on 4G. This system requires a UAV to be equipped with a 4G modem together with a Subscriber Identity Module (SIM) to enable the key features, such as tracking and identification. The tracking algorithm extracts the location information from the cellular network

978-1-7281-1035-6/20/$31.00 ©2020 IEEE
DOI 10.1109/MobileCloud48802.2020.00020

by combining information of detected cells. The cell-based location information gathered by the 4G modem is sent to a server, where the data is combined with the radio fingerprint database to estimate the UAV's location [2]. The identification of the UAV is based on the authentication process performed during the connection establishment with the SIM to the mobile network.

B. Control-Signal-based Systems

UAV identification and tracking is possible by extracting information from the control signal. The transceiver of the UAV broadcasts telemetry data and additional information, such as serial number and location information. This information is gathered by these systems, if the UAV is within range of a base station. The range is limited and depends on the antenna attached to the receiver unit. Control-signal-based systems are proprietary, because UAV manufacturers do not follow any common standard for the control signal. To monitor global air traffic in critical areas, an infrastructure must be build up from scratch. The only commercial available system is DJI AeroScope, which has a detection range of up to 50 km [3]. Beside DJI's AeroScope, there exist numerous other systems based on the control signal. In [4], the packet length is used to differ between types or vendors of UAVs.

C. Radar-based Solutions

Another experimental approach for UAV localization is based on radar systems. This approach comes with difficulties, because UAVs are small in physical size, making the detection and classification challenging for classical radars. In [5] the classification problem is partly solved, but identification is still unsupported.

D. Alternative concepts

In [6] an image-based detection and identification system using artificial intelligence was proposed. It is a two-step process, where first the UAV is detected on the image and second the UAV is classified into vendor models. A similar approach was suggested in [7], where acoustic waves are used to differ between different UAV vendors. These two systems are not capable of identifying individual UAVs, but only of types and vendors.

A promising concept for UAV identification and monitoring is based on Automatic Identification System (AIS), that is used for ships and vessel traffic services [8]. In [9], threats for AIS based systems were identified. These are split into software-based and RF-based threats, where spoofing, hijacking, and availability disruptions are possible attack vectors.

E. Main Drawbacks of existing Systems

Summing up, the main weaknesses of systems based on control signals or radars, are the lack of identification and only local coverage. These were mitigated by Vodafone's RPS, but since the identification relies on 4G, it does not support state-of-the-art security mechanisms, such as data integrity and authentication.

III. The Global and Secured Authentication System

The authentication system proposed in this paper shall counteract existing problems and weaknesses of state-of-the-art systems. Based on those, the following requirements were defined:

- *Authentication* not only identification, which means there must be a possibility to proof the identity. Provide protected sensor values, that are tamper-resistant against remote attacks.
- *Global availability* is a necessity to avoid regional proprietary systems.
- *Protected communication* with authenticity, confidentiality, and integrity are required to fulfill the security and privacy obligations.
- *High chance of acceptance at authorities*, because only these can require UAV manufacturers to implement and use the proposed system.

A. General Concept

Considering the general use case (Fig. 1), the two important parties are the UAV and the flight control that is monitoring UAV activities. In Fig. 2 a connection overview together with the UAV HSM extension is shown.

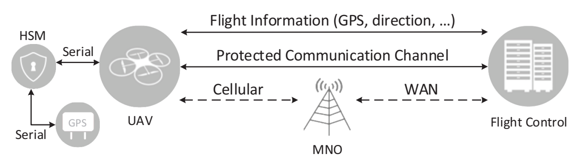

Fig. 2. Connection overview between UAV and flight control

To fulfill the global connectivity requirement without further expensive infrastructure costs as well as having a wireless connection, the UAVs are connected to the internet via cellular network. As depicted in the connection overview in Fig. 2, a protected communication channel must be established to fulfill the security requirements. One of the crucial points for the proposed UAV authentication system, is the combination of the Transport Layer Security (TLS) authentication procedure together with exchanging trusted location information and additional UAV information via a secured communication channel. The TLS protocol is a state-of-the-art, well established and IETF-approved, security protocol, that provides confidentiality, authenticity, and integrity. Pure software implementations of the TLS protocol are prone to traditional network and side channel attacks, that can both lead to extraction of confidential information [10]. Storing confidential information directly on the host controller instigates key extraction or identity cloning attacks. Therefore, the TLS protocol implementation used in this system is supported by an HSM connected to the UAV. The HSM provides a protected storage for authentication keys and certificates, that are necessary for performing the authentication procedure in the TLS protocol. The authentication procedure uses X.509 certificates containing information about the owner, which is also used to verify the identity of the owner.

Beside safeguarding digital keys and preventing key extraction attacks, the HSM is used to provide protected sensor values to the host controller. As depicted in Fig. 2 the flight information data, containing the location information of the UAV, is exchanged via the protected communication channel.

B. Protocol Stack

To make a clear separation of responsibilities during data transmission and allow efficient cross-platform implementations, a communication protocol stack is required. According to the ISO/OSI model, Fig. 3 depicts the communication protocol stack extended with the interface to the HSM, adopted to the proposed UAV authentication system.

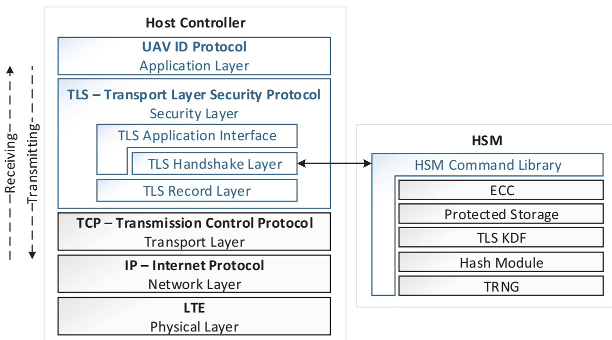

Fig. 3. Communication protocol stack for a UAV authentication system with hardware-based security

1) Application Layer: In this application, the UAV ID protocol represents the flight information data. It contains Global Positioning System (GPS) coordinates, which have to be transmitted between the UAV and the flight control.

An adversary, having control over the host controller, could attempt to alter the GPS values that are sent to the flight control server. To mitigate this issue the sensor values are protected by directly connecting the sensors to the HSM via an I2C bus, that is not accessible by the host controller.

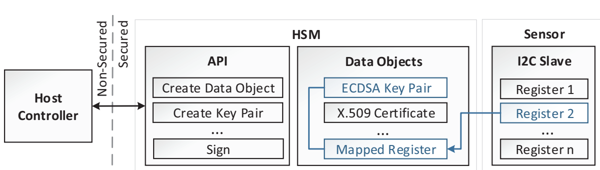

Fig. 4. Concept for protected I2C sensor values

As depicted in Fig. 4, the corresponding sensor register is mapped to a data object of the HSM. An ECDSA key pair is permanently linked to this data object, which means only this specific data object can be signed with this key. Every sensor output, is signed with the private key, and then provided to the host controller for further processing. With this measure, the host controller only receives signed sensor values. Therefore, the system can be sure at every point in time, that the sensor values (GPS in this case) were not tampered. Nonces, such as time stamps or sequence numbers, mitigate replay-attacks.

For transmission of sensor values via a communication channel, data serialization is required to translate data objects into data streams. Several data serialization formats with different purposes are defined and standardized. Hence, most applications can build upon existing standards. A comparison of four common formats is given in the evaluation chapter (see Section V-B).

2) Security Layer: To protect the communication channel, the TLS protocol is used at the security layer, which is capable of mutual authentication. The primary components of this protocol are record layer, handshake layer, and application interface, as depicted in Fig. 3.

The security properties provided by the record layer are confidentiality, authenticity, and integrity as described in [11].

This TLS protocol implementation is supported by an HSM, therefore the TLS layer is partitioned between the host controller and the HSM. The partitioning depends on the application and on the HSM functionality. A typical TLS partitioning is depicted in [12].

Fig. 5 depicts the handshake sequence between the server and the client, supported by an HSM. A detailed step-by-step description is given in the corresponding RFC [11]. In this section, the steps interacting with the HSM are described together with the three steps required for authentication (highlighted in Fig. 5).

The first key step regarding the UAV authentication system is the *CertificateRequest* message (*Client Authentication* Step (1) in Fig. 5), that forces the client to send a certificate for mutual authentication. Following the TLS standard [11] this message is optional, but required in the proposed concept. The client's *Certificate* message (Step (2) in Fig. 5), contains the client certificate, fetched from the HSM's protected certificate storage. It is used to authenticate the UAV against the flight control server. After reception, the server verifies the received certificate. The *CertificateVerify* message (Step (3) in Fig. 5), contains a signature calculated by the HSM using the private key, and a hash (created by the HSM) over all TLS handshake messages sent and received up to now. This verifies that the client possesses the private key corresponding to the certificate used for authentication and to prevent message reuse [11]. The server uses the public key from the certificate received before, to verify the signature generated at the client side using the private key.

That means the essential messages for UAV (client) authentication are: *CertificateRequest* message, client *Certificate* message, *CertificateVerify* message (highlighted and enumerated in Fig. 5). Any possible abortion of the handshake happens during the corresponding message parsing.

3) Physical Layer: *LTE Advanced* is the state-of-the-art wireless communication technology with a large areal coverage, especially near civilization, and therefore chosen for the proposed system. Due to the fact that *LTE Advanced* is only used for communication and clearly separated from upper layers, it can easily be replaced by 5G.

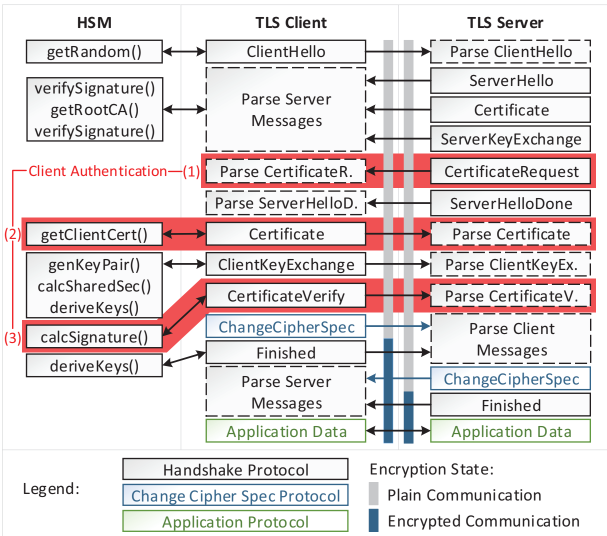

Fig. 5. TLS handshake sequence supported with hardware-based security (modified from [13])

IV. Proof-of-Concept

A. Certificate Provisioning Architecture

For the proof-of-concept implementation, a simple Public Key Infrastructure (PKI) is used. The root for the certificate provisioning is the Certificate Authority (CA) with the root CA certificate. Both UAV and the flight control server must store the CA certificate. Additionally, the CA provisions corresponding certificates to the UAV and the flight control server. The public key of the CA certificate is used to check the validity of the opposite party by verifying the calculated signature. The certificate exchange and the verification are done during the TLS handshake, as explained in the *Security Layer* Section III-B2.

B. Software Architecture

1) UAV Software Architecture: The existing command library for the chosen HSM is written in C, therefore the application running on the UAV is also written in C to avoid re-writing the command library or writing a wrapper. The UAV application has two tasks: UAV ID and RC relay. The RC relay task relays received steering commands to the flight controller via UART. In the proof-of-concept, steering commands are sent by the flight control server. In practice, steering commands will be transmitted by the operator's remote control. The UAV ID task extracts location information from a GPS module, or whatever localization system is used, serialize it in accordance to the CBOR format, and sends the data to the flight control server. To clearly separate the responsibilities of these tasks, each task is using a dedicated TLS secured TCP/IP socket for communication.

2) Flight Control Server Software Architecture: The structure of the flight control server software is analogous to the structure of the software running on the UAV. The application is extended by a GUI for interaction.

C. Hardware Architecture

The UAV hardware used for the proof-of-concept is depicted in Fig. 6 and consists of stacked modules placed on top of battery and carbon frame. Motor control board (ESC board), Raspberry Pi, and LTE module are freely available on the market. The flight controller board *Larix Edu* is a multicopter project by *Management Center Innsbruck* and *Infineon Technologies AG* [14]. The board is built around an Infineon 32-bit industrial microcontroller. It controls the ESC board using Pulse Width Modulation (PWM) according to the received remote control commands from the Raspberry Pi that is connected via UART. The LTE base shield was redesigned from [15]. The main components of the base shield are an Embedded SIM (eSIM) and the HSM. The LTE module itself is connected to the base shield via a Mini PCIe connector.

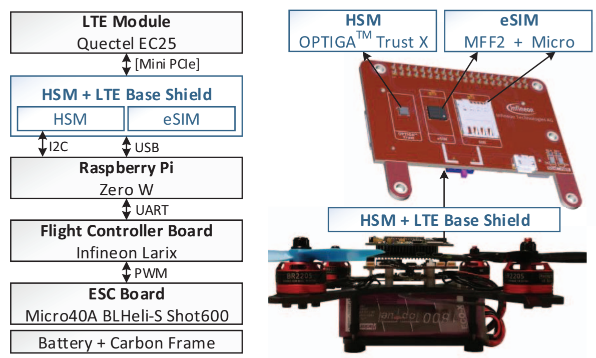

Fig. 6. UAV hardware implementation

The flight control server was realized with a Raspberry Pi 3 together with a touchscreen monitor for interaction. Since the server is not a focus of this work, it is not described in detail.

V. Evaluation

A. Threat model

The threats for the proposed system are distinguished between physical and remote attacks. For physical attacks, the adversary has to tamper with the UAV hardware. Side channel attacks could be used to extract key material from the HSM [10]. The proposed system is hardened against these attacks by integration of an HSM with a protected storage for key material. If an adversary is tampering with the hardware, the remaining protection keeps the keys in the HSM and prevent key cloning.

Remote attacks are threats where the adversary has no physical access to the UAV. To prevent remote software corruption, measures such as secured boot are required. Remote attacks against the host controller, to alter the values received from the GPS, are prevented by using the concept for protected I2C sensor values. A drawback of this concept is the introduced latency by the necessary signing of each sensor output. The power consumption increases too, due to the fact that the HSM is also needed during operation, not only during the TLS connection establishment.

The proposed system security does not depend on the 4G security measures, because the 4G link is only used for transport. If 4G jamming is used to disturb the control link, the *Failsafe* mode of the UAV is triggered. If the UAV ID is affected by jamming attacks, the socket for control link could be shut down in order to also trigger the *Failsafe* mode.

The proposed system can be applied for non-commercial or proprietary UAVs, but it is impossible to prevent UAVs from launching without this system, it can only be enforced by law. Since the market share for commercially available UAVs is seven times as big as for custom built UAVs, the necessity for such a solution is acute and inevitable. However, if an adversary wants to perform prohibited actions, either the UAV can be built from scratch, or a commercial UAV could be modified in software or the hardware could be tampered with. To mitigate these threats, radar-based solutions can be taken into account for use in highly critical areas, which may also detect UAVs without an authentication system.

B. Serialization Formats

Mobile applications, such as the UAV authentication system, are typically resource limited and therefore the encoded data size is a key property. That means, the chosen data serialization format should have minimized encoding overhead for the given application. In addition, the chance of acceptance of the system should be maximized, meaning a well-established and standardized format should be used. Serialization speed and ease of use of the chosen implementation are also essential factors. For the selection of the data serialization format and its specific implementation, several widely spread, standardized formats and implementations were compared, as depicted in Table I. For comparison, a raw data set with the size of 26 bytes containing location information and an additional 8 byte string was used.

TABLE I
COMPARISON OF DATA SERIALIZATION FORMATS

Format	ASN.1	CBOR	BSON	XDR
Raw [bytes]	26	26	26	26
Encoded [bytes]	34	31	57	32
Overhead [bytes]	8	5	31	6
Overhead [%]	31	19	119	23
Encoding [ms]	0.622	0.045	0.500	0.258
Decoding [ms]	0.405	0.041	0.160	0.101
Python Library	asn1tools	cbor	bson	xdrlib
Library Version	0.122.0	1.0.0	0.5.6	0.0.0
Standardized	ISO	RFC	BSON spec	RFC

Table I depicts that CBOR has compared to ASN.1, BSON, and XDR, the lowest encoding overhead and the fastest en- and decoding of test data with the tested libraries. These are critical efficiency properties, if messages are sent on a wireless channel several times per second, as in the case of the proposed UAV authentication system. Due to the availability of software libraries for en- and decoding according to the CBOR standard, extensive library implementation are avoided. CBOR specifies the type of the field, but not the purpose. Therefore, correct ordering of the raw data fields is necessary, which is solved by using TCP at the transport layer. CBOR is promoted by the IETF as an RFC (see [16]), which increases the chance of acceptance from authorities. Based on these advantages, CBOR is chosen as a serialization format at the application layer.

C. Overhead Evaluation

The overhead evaluation was done on a Raspberry Pi 3 (Model B+) with Wireshark. The packets sent between server and UAV were captured and analyzed.

The total overhead for the TLS handshake in the proof-of-concept implementation is $\sim$1500 bytes. Each Elliptic Curve Cryptography (ECC) certificate has a size of $\sim$500 bytes. The proof-of-concept implementation only uses one certificate per party for authentication. That means each certificate chain, sent during the TLS handshake with the client and server *Certificate* message, contains only one certificate. This results in $\sim$1000 bytes for the certificates. The other handshake messages takes the remaining $\sim$500 bytes.

The three essential handshake messages for the proposed UAV authentication system, highlighted in Fig. 5 are, by default, optional in the TLS standard. This means, the overhead of the usually optional, but in this case obligatory TLS feature results in $\sim$600 bytes ($\sim$500 for the ECC certificate) from the total $\sim$1500 bytes.

On the record layer, the application data is encrypted and sent. Since the chosen serialization format for the proof-of-concept implementation is CBOR, the example application data has a size of 31 bytes, as depicted in Table I. Considering the used cipher suite for the prototype (TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256), the overhead on the record layer is compound by the header (5 byte), the maximum padding size (AES128: max. 15 bytes), and the size of the MAC (SHA-256: 32 bytes). This results in the total size of 83 bytes for each message at the record layer.

The total overhead was deemed, because the major part of the overhead is produced during the TLS handshake, which only happens once during connection establishment.

D. Comparison to State-of-the-Art Systems

Table II depicts essential properties for UAV authentication systems and their availability for state-of-the-art systems and the proposed system.

The proposed UAV authentication system is based on standardized protocols and state-of-the-art hardware-security. Using standardized protocols for authentication (TLS) and data serialization (CBOR) instead of using proprietary protocols, increases the chance of acceptance when submitting the proposed system to an authority, such as the FAA or EASA, to influence upcoming regulations. The authentication of the UAV is the essential part within this context. The TLS protocol is not only used for authentication, but also for securing the communication channel. First, the TLS layer partitioning between host and HSM provides a protected storage for keys and certificates. Second, this design decision allows relieving

TABLE II
COMPARISON OF UAV AUTHENTICATION SYSTEMS

	Vodafone RPS	DJI AeroScope	Radar-based	Image-based	AIS-based	Proposed in Paper
Availability	Global (4G)	Local	Local	Local	Local	Global (4G*)
Infrastructure Type	Server	Base Station	Base Station	Base Station	Base Station	Server
Security Mechanism	4G	Sym. Encryption	No	No	No	4G, TLS (with HSM)
Identification/Authentication	Yes/Yes	Yes/No	No/No	No/No	Yes/No	Yes/Yes
UAV HW Modification necessary	Yes	Yes (except DJI)	No	No	No	Yes
Additional Data Payload possible	No	Yes	No	No	No	Yes
Protected ID Storage	No	No	No	No	No	Yes

the host controller from processing power expensive, cryptographic operations, that are additionally more robust against side channel attacks. In terms of future upcoming regulations, certified security is an essential property. In the proposed system, a Common Criteria certified EAL6+ hardware, the Infineon OPTIGA^{TM} Trust X is used.

This system is an *authentication* system, contrary to DJI's AeroScope, a detection and tracking system only. Meaning, the AeroScope system needs to detect a UAV first to track and identify. Another disadvantage is the limited detection range of maximum 50 km [3], because every region to be observed needs to be equipped with a base station. In contrast to base stations, Vodafone's RPS and the proposed UAV authentication system need servers to communicate with, and further to allow analyzing the received data.

An advantage compared to Vodafones RPS system is, that *LTE Advanced* is only used for communication, not for authentication (indicated with * in Table II). This means the physical channel could easily be replaced at any time, by any other communication channel available in the future (e.g. 5G).

A disadvantage of the proposed system, that is impossible to circumvent if an active authentication process happens, is the necessity that the UAV system must be modified. It has to be equipped with *LTE Advanced* (or its successor), but this comes with other possible use cases, such as beyond line-of-sight steering or transmitting high quality video streams. Further, additional software components must be implemented on the UAV. These could be defined as a standard to limit additional implementation work for the UAV manufacturers. Another drawback that comes with additional system blocks is the decreasing battery duration. However, these disadvantages are acceptable, due to the tremendous security enhancements.

VI. CONCLUSION AND FUTURE WORK

In this work, we proposed a global and secured UAV authentication system based on hardware-security for commercial, non-tampered UAVs. Still, highly sensitive areas require additional detection, for instance based on radars, to also detect the minority of UAVs, flying without the authentication system in future.

Since the authentication is conducted to the connection establishment, periodic messages for tracking only have to contain location information and no identifier. This lowers the periodic data overhead. Using the HSM-backed TLS protocol, location data and privacy of the pilot is protected. Further, the sensors are directly connected to the HSM, which cryptographically signs each sensor output before reaching the non-secured environment, to protect sensor values against remote attacks.

Flight control must be managed by an authority which defines the regulations, as shown in the use case diagram in Fig. 1. Such regulations are region-dependent, thus more than one authority defines the infrastructure. Therefore, future work will investigate a more sophisticated and flexible trust-provisioning process to ensure that UAVs are connecting to a trusted and location-dependent flight control.

REFERENCES

[1] EASA. (2019) Civil drones (Unmanned aircraft). [Online]. Available: https://www.easa.europa.eu/easa-and-you/civil-drones-rpas

[2] Vodafone. (2007) Vodafone Beyond Visual Line of Sight Drone Trial Report. [Online]. Available: https://www.vodafone.com/content/dam/vodafone-images/media/Downloads

[3] DJI, "DJI AeroScope," https://www.dji.com/at/aeroscope, [Online; accessed 2019-07-30].

[4] P. Kosolyudhthasarn, V. Visoottiviseth, D. Fall, and S. Kashihara, "Drone Detection and Identification by Using Packet Length Signature," in *2018 15th International Joint Conference on Computer Science and Software Engineering (JCSSE)*, July 2018, pp. 1–6.

[5] M. Jian, Z. Lu, and V. C. Chen, "Drone detection and tracking based on phase-interferometric Doppler radar," in *2018 IEEE Radar Conference (RadarConf18)*, April 2018, pp. 1146–1149.

[6] D. Lee, W. Gyu La, and H. Kim, "Drone Detection and Identification System using Artificial Intelligence," in *2018 International Conference on Information and Communication Technology Convergence (ICTC)*, Oct 2018, pp. 1131–1133.

[7] N. Siriphun, S. Kashihara, D. Fall, and A. Khurat, "Distinguishing Drone Types Based on Acoustic Wave by IoT Device," in *2018 22nd International Computer Science and Engineering Conference (ICSEC)*, Nov 2018, pp. 1–4.

[8] N. Molina, F. Cabrera, V. Araa, M. Tichavska, B. P. Dorta, and J. A. Godoy, "A Wireless Method for Drone Identification and Monitoring Using AIS Technology," in *2018 2nd URSI Atlantic Radio Science Meeting (AT-RASC)*, May 2018, pp. 1–2.

[9] M. Balduzzi, K. Wilhoit, and A. Pasta, in *A Security Evaluation of AIS*, Trend Micro Incorporated, 2014.

[10] Marcus Janke, Dr. Peter Laakmann, in *Attacks on Embedded Devices*, Embedded World Conference Nurenberg, 2016.

[11] R. E. Dierks T., "The Transport Layer Security (TLS) Protocol Version 1.2," Internet Requests for Comments, RFC Editor, RFC 5246, August 2008. [Online]. Available: https://tools.ietf.org/html/rfc5246

[12] L. Qi *et al.*, "A Secure End-to-End Cloud Computing Solution for Emergency Management with UAVs," December 2018.

[13] Thomas Fischer, *Design and Implementation of a Secure Personal Assistant Device with BLE and NFC*. TU Graz, 2016.

[14] Management Center Innsbruck, "Wiki for the Infineon Multicopter Demoboard," https://github.com/ManagementCenterInnsbruck/Multicopter_LARIX/wiki, [Online; accessed 2019-08-26].

[15] Sixfab, "Raspberry Pi Iot Shields Sources," https://github.com/sixfab/Sixfab_RPi_3G-4G-LTE_Base_Shield, [Online; accessed 2019-07-30].

[16] B. C. and H. P., "Concise Binary Object Representation (CBOR)," Internet Requests for Comments, RFC Editor, RFC 7049, October 2013. [Online]. Available: https://tools.ietf.org/html/rfc7049