Secure Communication in Civil Drones

Abdulhadi Shoufan[1](✉), Hassan AlNoon[2], and Joonsang Baek[1]

[1] Electrical and Computer Engineering Department, Khalifa University, Abu Dhabi, United Arab Emirates
{abdulhadi.shoufan,joon.baek}@kustar.ac.ae
[2] Advanced Technology Consultancy L.L.C, Emirates Advanced Investment Group L.L.C, Abu Dhabi, United Arab Emirates
hassan.alnoon@eai.ae

Abstract. The drone technology is attracting an increasing attention in civil applications. Secure communication is a critical requirement in many scenarios to provide an acceptable level of data confidentiality, integrity, and availability. In this chapter we first present a security analysis of civil drones. Then, a light-weight hardware solution is proposed to assure the confidentiality and integrity of both command data sent by the ground station and payload data transmitted by the drone. Using the developed prototype, finally, we investigate the impact of hardware accelerators on the power consumption of these power-constrained devices. We show that the advantage of hardware as a power-efficient computation platform is not necessarily valid for drones due to the extra hardware weight.

Keywords: Civil drones · Security · Cryptoengine · Speedup · Power consumption

1 Introduction

Unmanned aerial vehicles have long been used for surveillance in homeland security. Due to their high costs, however, the effectiveness of UAVs in civil applications has always been under discussion. This circumstance contributed to the development of lower-cost platforms in the form of quadrotors or multirotors, which we refer to as civil drones (CD). The absence of mechanical linkages to vary the rotor blade pitch angle, the usage of multiple rotors and the improvements in the algorithms that controls its advanced electronic systems and sensors has allowed CDs to be of small-size and easy to fly, control, and maintain. Due to their ability to interact with the environment in close proximity safely, CDs are gaining an increasing attention in different civil application areas [1]. In environment monitoring CDs use sensors and cameras to collect information that is difficult to be obtained by helicopters because of space or cost reasons. An example for this application area is monitoring the woods, desert, animals, and agriculture. Disaster management is another application area where CDs can

O. Camp et al. (Eds.): ICISSP 2015, CCIS 576, pp. 177–195, 2015.
DOI: 10.1007/978-3-319-27668-7_11

give a quick overview of the size and the grade of a disaster caused by flooding, earthquake, or fire. Based on this information an efficient plan for rescue activities can be defined and implemented. Especially in the surveillance and law enforcement areas CDs are receiving an increasing acceptance to observe restricted areas, state borderline, pipelines, private properties, or public events for detecting suspicious actions and preventing terrorism.

Commercial CDs are penetrating and the importance of these devices was recognized by the governments of many countries. Several research projects were supported by governmental and non-governmental funding sources: USICO (Unmanned Aerial Vehicle Safety Issues For Civil Operations) is a European project that dealt with the operation and the safety of UAVs, e.g., for collision avoidance. CAPECON (Civil UAV Application & Economic Effectivity of Potential Configuration Solution) is another European project, which aimed at the specification of civilian applications for the UAVs. A major aspect of this project is the integration of large-scale UAVs into the air traffic control system. The design of a distributed control system for cooperative detection and monitoring using heterogeneous UAVs [2] was the subject of the project COMETS funded by the European Union, too. μDrones is another European project which focuses on microdrones for autonomous navigation for environment sensing. The purpose is the development of hardware and software modules to ensure flight stability, navigation, localization, and robustness to unexpected events. Several topics related to networked UAVs were investigated at the Aerospace Controls Laboratory at MIT [3]. These include sensor network design, adaptive control, and model predictive control. Starmac is a project at Stanford University [4], which works on autonomous collision and obstacle avoidance and task assignment formation flight using both centralized and decentralized techniques. Additionally to these projects, an enormous amount of individual research chapters can be found in the literature that address different topics such as specific control systems [5–7] and obstacle avoidance approaches [8–10].

With all this attention to the functional aspects of this new technology, the consideration of security aspects is still very limited. When it comes to security, the CD should be considered from two points of view: as a threat and as a target. CDs are considered as security threat because they can be used for mischievous or criminal activities. With the versatile technical possibilities, the drones can be abused to spy on unaware individuals. Privacy and civil liberty advocates have raised many doubts about the legitimacy of facial recognition cameras, thermal imaging cameras, open Wi-Fi sniffers, license plate scanners and other sensors. For example, the researchers at the London-based Sensepoint security firm showed how to equip a drone with a software program called Snoopy that allows the vehicle to steal data from surrounding mobile devices searching for a Wi-Fi network. The researchers successfully demonstrated the ability of the Snoopy application to steal Amazon, PayPal, and Yahoo credentials from random citizens while the drone was flying over their heads in the streets of London. Not only individual's privacy and security seem to be threatened by the CD technology but also commercial, industrial, and governmental sectors.

Recently, a drone was used to leak behind the scenes footage of the filming of the new Star Wars movie series without the authority to be able to do anything about it. The penetration of new commercial products such as DroneShield, that help detect spying drones based on acoustic noise or radio signals is a clear evidence for the seriousness of these concerns.

CDs, however, can themselves be an attack target. The principal risks are represented by the possibility that criminals and cyber terrorists can attack unmanned aerial vehicles for several purposes such as hacking or hijacking. The chapter deals with the CD security from this latter point of view and provides an in-depth analysis of the CD communication security. Based on this analysis a hardware-based solution is proposed to obtain the required performance for cryptographic functions. The solution is investigated with respect to power consumption and compared with a software solution. This investigation shows that the cryptoprocessors advantage of low power consumption is suppressed in this application because of the additional power that is needed to carry and fly the additional hardware.

The chapter is structured as follows. Section 2 discusses the security vulnerabilities and threats of civil drones and presents a use-case based classification of the drone security requirements in terms of confidentiality, integrity, and availability. Section 3 describes the security controls built in our prototype. Section 4 describes the proposed hardware solution and Sect. 5 gives some implementation details. In Sect. 6 we analyze the performance and the power consumption of the developed prototype. Section 7 concludes the chapter.

2 Security Aspects in Civil Drone Communication

This section first describes the vulnerabilities of CDs and the threats they are exposed to, in general. Obviously, the level of threat highly depends the particular application of the drone and the security requirements on drone communication should be defined in the context of the particular use case. Therefore, this section also provides a use-case based analysis of the security level in terms of confidentiality, integrity, and confidentiality.

2.1 Civil Drone Vulnerabilities and Threats

As a flying platform, a drone is exposed to various passive and active attacks with specific impacts as summarized in the following:

Control Data Manipulation. Control data manipulation is perhaps the most critical active attack on a CMD. Sending fake control commands by an attacker may be motivated by one of the following:

1. Dislocating the CD: When CDs are used for surveillance and law enforcement purposes, then people under surveillance, who may be criminals, may work against that by trying to fly the CD away from the monitored area. Recently

GPS spoofing has been a focus of both media and academia. In the spoofing GPS attack, the counterfeit GPS signals, which resemble the real GPS signals, are broadcast to deceive a drone with a GPS receiver. These spoofed signals can cause the receiver to estimate its position to be somewhere other than the real position [11,12].
2. Physical theft (Hijacking): Some commercial microdrones are highly expensive and can fly to far distances. Having it under control, an attacker may fly a CD to a desired place where she or he can steal it physically. The physical theft may also be motivated by the intention to tamper with the device to disclose cryptographic keys or secret data.
3. Damage to persons and property: Due its light weight, a CD can fly with high speeds. A malicious attacker may use this feature to steer a CD and cause it to collide with high momentum with an arbitrary or certain target. In addition to the risk of person's injury and damage to property, such attacks may cause major legal liability problems to the CD owner or to his or her insurance provider.

Replay Attacks on Control Data. Adversaries may record control data and resend it later to misuse the CD. This kind of attack works even if control data are protected against manipulation.

Denial-of-Service Attacks (DoS). CDs are power-critical microcontroller-based systems. Any computation overhead causes additional power consumption and shortens the endurance of the CD. An attacker may use this vulnerability to flood the CD with faked or replayed commands and, thus, impair the availability of the CD. Even if the CD is able to identify these commands as fake or replay, e.g., using a verification process, this approach demands considerable computation power and time. In extreme cases, such a DoS attack may cause the CD to be completely engaged in the authentication process until the CMD battery is fully discharged. Note that flooding the CD with faked or replayed commands, as treated in this chapter, can be regarded as a DoS attack on the application layer. DoS attacks in wireless networks on lower layers such as the physical layer (jamming) and the MAC layer are well-studied in the literature [13,14] and out of the scope of this chapter.

Information Theft. The bird's-eye view provided by the CD is attracting professional photographers to take high-quality pictures or record videos from the sky. As a rule, these pictures or videos are sent to the ground station not only to save the memory usage on the CD but also for the photographer to control the picture taking or the video recording. Obviously, such data may be of high value and under copy right. Sending the data in plaintext opens the way for adversaries to record and distribute the data at low cost and to cause considerable financial loss to the professional photographer. Understandably, information theft may be exercised in many other CDs' application areas with different motives.

Information Manipulation. Information data sent by the CD may be used for critical purposes. For instance, pictures taken in surveillance and law enforcement applications may be used as means of evidence. Also, the success of a rescue plan for disaster management may rely on the picture taken by the CD. Obviously, any manipulation of these data including replay attacks may cause severe problems.

2.2 Use-Case Based Classification of CIA Security Requirement

The level of security requirements on drone communication depends on the particular application of the drone. We first developed a use-case independent classification scheme for these requirements as given in Table 1. The requirement level of confidentiality, integrity, and availability is classified into *High*, *Medium*, or *Low*. For that we differentiated between *control data* sent from the ground station to the drone and *information data* sent in the other direction.

Then, we conducted a research to create a comprehensive list of possible use cases as reported in media or research chapters. For each use case we tried to qualitatively assess the security risk arising through the communication channel between the drone and the ground station in both directions. Accordingly, we assigned a level for each security requirement as summarized in Table 2.

Table 1. CIA level classification scheme.

		High	Medium	Low
Control data	Confidentiality	Flight path and/or flight destination are secret or highly secret	Flight destination is roughly defined and flight path is semi-random	Flight path and flight destination are known or easily predictable
	Integrity	Manipulating commands causes high severity level such as injuries or loss of life	Manipulating commands causes medium severity level such as moderate asset damage or loss	Manipulating commands causes low or no violation
	Availability	Real-time human-controlled flight mode	Human-controlled flight mode but no hard real-time control is required	Autonomous flight mode
Information data	Confidentiality	Data is highly sensitive or has high commercial value	Data is not sensitive and has medium commercial value	Data is not sensitive and has no commercial value
	Integrity	Highly critical data with real-time requirements. Data manipulation causes high severity levels	Critical data, however, without real-time demands	Less critical data
	Availability	High data rates and real-time response to data content is required	Either high data rates or real-time response to data content are required	Low data rates and time-tolerant response (or no response) to data content is required

In the following we describe the thoughts behind the classification scheme given in Table 1 referring to some examples in the Table 2. Please note that the proposed classification of some use cases into some CIA levels may seem to be arguable. This is essentially because of the different angles from which the use case can be looked at and the different possible threats and attack scenarios. To reduce the uncertainty of our classification we followed the following approach. After agreeing on the classification scheme, each of the three authors has separately classified the uses cases. Then, we aggregated the three classifications in the following way:

1. If the three authors agreed on the same security level, we adopted it.
2. If two authors assigned the same level and the third one selected a different level, we adopted the level that was selected by two authors.
3. If the three authors selected three different levels, we assigned the level medium to the corresponding security requirement.

Apart from this, we believe that this investigation clearly reflects the sophistication of defining security requirements for drones. Identifying the appropriate security level is the first step towards selecting appropriate security controls.

CIA Levels for Control Data. The basic information embedded in control commands relates to three critical flight dynamic parameters referred to as the roll, pitch, and yaw angles; as well as to the throttle. Based on this information and on the embedded dynamic model and control mechanism, the drone moves from its current position to a new position following a certain trajectory. Thus, the control data sent by the ground station relates in the end to the new position of the drone and to the trajectory it follows to reach there. Obviously, the confidentiality level of this data is commensurate with the confidentiality level of the drone new position and trajectory. Depending on the use case this information can be critical if the attacker can model the drone and calculate the trajectory starting from sniffed commands. For instance, in the case of package delivery, this may give an attacker information about the delivery address. It is not unthinkable that drone-based delivery services will attract malicious groups to develop professional techniques for package theft. In such a case, the control data should be classified as highly confidential and appropriate security controls must be implemented. On the other hand, in many applications such as in the dam inspection scenario, the drone flight space is limited and its position in the air is almost always predictable. In such cases the control data confidentiality can be considered as low. In other cases, the drone can fly within a limited area but its trajectory should be kept secret, e.g., to reduce shooting risk. In such cases, the confidentiality level of the control data can be classified as medium. An example for these applications is the drone-based crowd surveillance and control.

Drones should follow the trajectory determined by the pilot. Manipulating the control data or sending false control data by an attacker may cause the drone to follow an undesired trajectory that may intentionally or unintentionally lead

Table 2. Classifying the CIA levels of reported use cases.

Use Case	Control Data			Information Data		
	Conf.	Int.	Ava.	Conf.	Int.	Ava.
Climate Monitoring	L	M	M	M	M	L
Glacier Dynamics Monitoring and Analysis	L	L	M	M	M	M
Volcano Monitoring and Analysis	L	L	M	M	M	M
Atmospheric Sampling	L	L	L	M	M	L
Journalism and News Gathering	M	H	M	M	M	M
Environmental Control and Monitoring	L	M	M	L	M	L
Mineral Exploration and Exploitation	M	M	M	H	M	M
Farm Monitoring / Agriculture	M	M	M	M	M	M
Remote Sensing	M	M	L	M	M	L
Pest Eradication	L	M	M	L	M	M
Predator deterrence	L	H	M	L	M	H
Scientific Research	M	M	M	M	M	M
Factory Production line malfunctions	L	H	M	L	M	M
Film Industry	M	H	H	H	M	H
Real Estate Photography	M	H	M	M	M	M
Invasive Species Identification	L	M	M	L	L	H
Archaeological / Historic Site Mapping and Inspection	L	M	M	L	M	M
Wind Turbine Inspection	L	M	M	M	M	H
Wildlife monitoring	L	M	M	L	M	M
Ship Inspection and Monitoring	M	M	M	M	L	M
library Bookshelf Monitoring	L	H	M	L	L	M
Package Delivery	H	H	M	M	H	L
Deep-Sea Fossil Fuels Scanning	H	M	M	M	M	M
Insurance Claim	L	M	M	M	H	M
Air Photography	M	M	M	M	M	M
Power lines inspection	M	M	L	H	M	H
Inspect Nuclear Installations	M	H	H	H	H	H
Nuclear Waste Transport	H	H	H	H	H	H
Dam Inspection	L	M	M	H	L	H
Railway Track Inspection	L	M	M	H	M	H
Road Inspection	L	M	M	M	L	M
Oil & Gas Pipeline Inspection	M	M	M	H	H	H
Bridge Inspection	L	M	M	H	M	M
Fire Scene Inspection	L	H	H	M	M	H
Search and Rescue	L	H	H	L	H	H
Emergency Response	M	H	H	M	H	H
Traffic Control	L	H	H	L	M	M
Poaching Activity	M	M	H	L	L	M
Disaster Site Monitoring	L	M	H	M	H	H
Forest monitoring	M	M	M	L	L	M
Perimeter Surveillance	H	M	M	M	M	M
Traffic Accident Analysis	L	M	M	M	H	M
Crowd Surveillance and Control	M	H	H	M	M	M
Borderline monitoring	H	H	L	H	H	M
Pollution Monitoring	L	H	L	L	M	L

to a damage or loss of properties (including the drone itself) or cause injuries or even loss of life. The level of control data integrity should be linked to the level of severity caused by sending false or manipulated commands. This severity level depends on the value of the drone itself, the mission costs, the value of objects that may be damaged, the density of humans or other animate being that may be injured. In many cases, the level of potential severity is obvious. This, for instance, applies to the use case Crowd Surveillance and Control, where many people can be gathered in relatively small areas. The risk of injuries by potential attacks is extremely high in this case. In contrast, a drone flying for Volcano Monitoring and Analysis is supposed to be less critical. In many applications, however, the severity level should be considered in the context of the particular use case. In the Farm/Agriculture Monitoring application, for instance, the severity level may depend on the kind of the agriculture or on the presence of farmers on field. This kind of use cases were assigned a medium integrity level in Table 2.

Drones must response to the ground station control commands whenever required immediately. The amount and the rate of control data sent to the drone depend on the use case and whether the drone flies in an autonomous mode or in a pilot-controlled mode. In the autonomous mode, the pilot usually loads mission data to the drone before starting. With the help of a GPS receiver, the drone then follows the defined path, altitude, and orientation to arrive at the final landing destination. Thus, use cases that assume autonomous flight mode do not require high-level availability for control data, as a rule. Examples for such use cases include Borderline Monitoring and Power Line Monitoring. Many use cases presume a real-time control of the drone by a human pilot for appropriate performance such as in Nuclear Waste Transport, Search and Rescue applications, or Film Industry. In such cases the availability of the control data must be provided on a high level. Some applications require human control. However, the real-time requirement on control data is not especially high because the drone mission is mainly performed in a hovering state or under very low speed. In the Air Photography, for instance, the pilot needs to find an appropriate perspective for her or his pictures. However, some amount of delay can be tolerated. So the availability level of control data can be regarded as medium.

CIA Levels for Information Data. Some commercial drones are supplied with actuators to perform some physical function on the fly such as Pesticide Spraying Drones. However, the majority of drones still serve sensory applications where data in different forms is collected on the fly and submitted to the ground station or stored on board for later processing and analysis. The confidentiality level of this data tightly relates to the use case. Images submitted by drones on missions for critical infrastructure inspection such as Oil and Gas Pipelines are classified as highly confidential, in general. Also, data collected in some commercial applications such as Mineral Exploration and Exploitation can be of high confidentiality level. In some commercial use cases such as in the Film Industry, the producer may prefer to keep the data secret within limited time

frames and the confidentiality level can be classified as medium. In many other applications, the data provided by the drone is public or of less commercial and private value so that its confidentiality can be classified as low. Examples for such applications include Library Bookshelf Monitoring and Wildlife Monitoring.

Integrity is a fundamental requirement on any data. Nevertheless, the level of integrity is an important concept to describe the impact of the loss of data integrity. The integrity level required for information data gathered by the drone depends on the type of this data and its criticality in the context of the use case. In many applications, the data sensed by the drone is processed in ground station computers to determine an appropriate response. For example, drones can be supplied with thermal imaging sensors for Rescue Operations in the night or in invisible areas. Manipulating the sensor data may cause the rescue team to lose sight of injured or trapped people. In such cases the data integrity must be regarded as a high-level requirement. In some use cases the data integrity is essential to obtain accurate simulation results or precise future predictions but there is no real-time requirements or a need for urgent responses. In such cases the integrity level can be classified as medium. Examples for these use cases include Climate Monitoring and Glacier Dynamics Monitoring and Analysis. In some applications, the drone sends visual image data that are only inspected by the pilot or other operators for uncritical routine surveillance or inspection purposes. In such cases, the required level of data integrity can be described as low. Examples for such use cases are Dam inspection and Road Inspection.

The required availability level of information data mainly depends on the timing criticality of this data and its rate. Drones that send high-rate data in real-time to enable prompt response should show a high level of availability. Examples for such applications include Emergency Response and Film Production. When the data rate is low or the response time is not especially critical we classify the requirement on the availability level as medium. This is the case in many applications such as Ship Inspection and Monitoring or Air Photography. In use cases, where neither high data rates are required nor a real-time response to the data is expected, the data availability level can be classified as low. Examples for these cases include Climate Monitoring and Remote Sensing.

3 Security Controls

In this section we describe the security controls that we applied in our prototype to meet the different security requirements.

3.1 Data Confidentiality

Depending on the application, remote control data (Upstream), information data (Downstream), or both should be encrypted. For CD communication the AES algorithm is selected with a key length of 128 bit [15]. AES in its native operation mode (Electronic Code Book (ECB)) results in the same ciphertext block if the same plaintext block is encrypted, which presents a security risk. To avoid this,

the Cipher Block Chaining mode (CBC) can be used. CBC encryption provides confidentiality against Chosen Plaintext Attack (CPA), which is a strong but essential requirement for secure symmetric-key encryption [16].

3.2 Data Integrity and Authenticity

To enforce Data Integrity and Authenticity we used a message authentication code scheme (MAC) that uses a symmetric key. A MAC scheme can be either proprietary, hash-based, or block-cipher based. We chose to use CBC-MAC which is block-cipher based MAC scheme so that is can share the same AES core used for encryption due to hardware resource constraints.

The high similarity between the MAC scheme and the CBC-mode of encryption is essential for the design of a compact cryptographic engine as will be detailed in Sect. 4.1. Note that message authentication code uses AES in encryption mode only in both the sender and receiver sides of communication. MAC also implicitly provides data integrity, as any change in the message will result in a different MAC value.

3.3 Resistance Against Replay-Attacks

Even encrypted and authentic messages may be captured by an attacker and replayed at a later point of time. Replayed data passes the authentication process successfully on the receiver side. Therefore, to detect replay attacks additional information is added to the message, which enables the receiver to verify the freshness of the message. The additional information can be a nonce (number used only once), time stamp, or a sequential number. In CD communication, we propose using sequential numbers against replay attacks, as these numbers can be deployed for additional purposes, specifically to detect packet loss and to restore the packet order.

3.4 Resistance to DoS Attacks

DoS attacks are versatile and can be carried out on different network layers. Countermeasures are usually specific to one or small number of attacks and operate on specific layers embedded in firewalls, network routers, switches, etc. As noted previously, we focus on a DoS on the application layer by assuming that the attacker is able to flood the CD with fake or replayed commands to affect the availability of the vehicle. In CD communication, command authentication and the replay attack countermeasure play a detective and a preventive role in the defense against DoS attacks. First, the CD keeps track of received commands and periodically determines the ratio of non-authentic commands and replay commands to the total number of received commands. If this ratio becomes higher than a specific value a DoS attack is assumed. Second, command authentication and the replay attack countermeasure perform a primary filtering of DoS commands. This means that the system components that follow the

authentication process are preserved from the DoS effects. Using authentication to mitigate (not eliminate) DoS attacks is deployed in the IPSec protocol suite, for instance.

3.5 Tamper-Resistant Key Management

Key management is a challenging task that addresses key generation, key exchange, key storage, key update, and key revocation, in general. The following paragraphs describe how the proposed key management scheme works for CD communication.

Key Generation. The encryption and authentication keys are generated by the ground station based on the key generator specified in ANSI X9.17 which is a key management standard for financial institutions published by the American National Standard Institute [17]. This key generator relies on the block cipher 3DES but can use any other block cipher. In our case we use AES, as it is already available for other security functions.

Key Exchange and Storage. Key exchange and key storage are usually treated separately. In our case they are related due to the used hardware platform. As will be seen later, we use an FPGA to run the security functions on the CD. The used FPGA is SRAM-based, which means that the configuration data must be loaded to the FPGA at each start. The configuration data is stored in a small external configuration memory mounted on the same board. Thus, a permanent key storage on the FPGA is impossible. Furthermore, storing the keys in the configuration memory as a part of the configuration data poses two risks. First, if the attacker gets physical access to the CD she or he can temper with the memory chip to extract the key. Furthermore, the attacker may analyze the configuration data while transferred from the memory to the FPGA to obtain the key.

To avoid these risks we propose the following simple scheme. Before each flight, keys are generated by the ground station and written to the FPGA by wire. Wireless submission is improper as radio data can be intercepted by adversaries. The keys are stored in dedicated registers inside the FPGA. These registers can only be read by the cryptographic engine and has no read interface to outside. Writing the keys to the FPGA by wire may appear to cause an operational overhead. However, flying a CD is always preceded by a setup phase. The proposed key exchange approach can be seen as a step in this setup phase.

Key Update and Revocation. Updating symmetric keys is recommended to enhance security. The idea is to reduce the amount of data encrypted with the same key to limit the damage, if the key is compromised. Usually, symmetric keys are updated for each new message or for each new communication session. For the CD we propose updating the encryption and the authentication keys for each

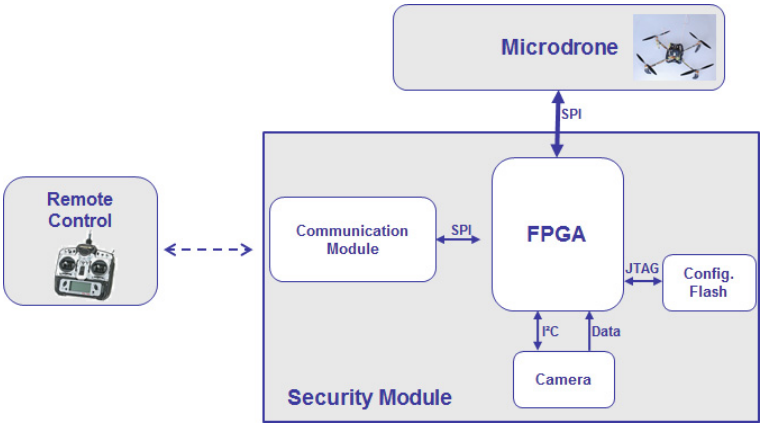

Fig. 1. General architecture of the secure CD system.

flight. The new keys are generated according to standardized key management algorithm (ANSI X9.17) and sent to the FPGA by wire as described in the previous paragraph.

The registers used to store the keys are provided by a reset input that can be activated by a special command from the ground station. The CD operator can submit this command in emergency cases when she or he loses control over the CD for any reason.

4 System Architecture

The system consists of three main components: The remote control, the drone, and an extension module connected to the drone that embeds the cryptographic engine, see Fig. 1. The hardware architecture of the extension module is depicted in Fig. 2. The architecture comprises a cryptographic engine; the on-chip JPEG encoder, which on its part embeds a camera controller; a video streamer and the control data receiver to manage the data communication; A Digital-2-PPM converter, which receives the digital control data extracted from the upstream packet and converts it back into a PPM signal (Pulse Position Modulation). In the following sections the different components of this architecture will be explained with more attention to the Cryptographic Engine as it provides the core of the security solution.

4.1 Cryptographic Engine

The Cryptographic Engine is the central part of the hardware architecture. The authentication key and the encryption key are written to the corresponding registers during the CD setup. The Cryptographic Engine serves the video streamer and the control data receiver. It expects from these modules an intermediate

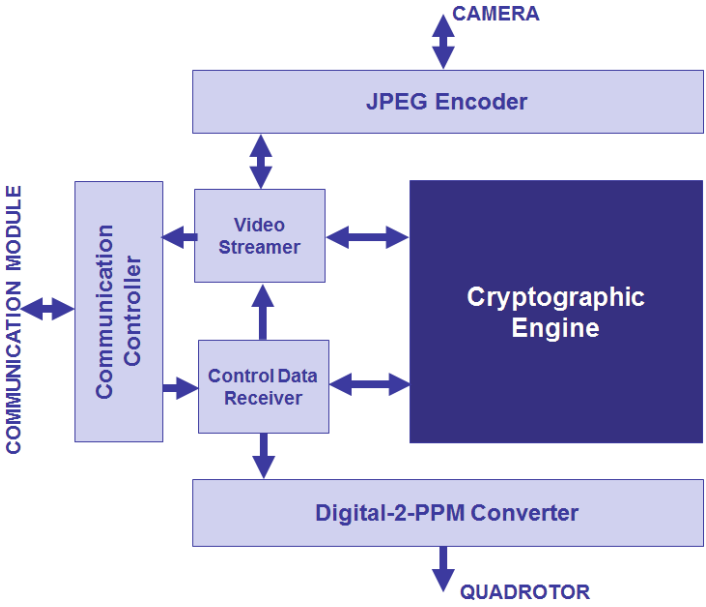

Fig. 2. General architecture of the FPGA hardware system.

MAC value, a plaintext block, and a cipher text block. The particular module indicates its need for data processing by sending a start signal, the cryptographic module also decides which module will be served next using a "fairness scheme" that was developed to prevent the data-intensive video streamer from occupying the cryptographic engine for a long time at the cost of the control data receiver. In the idle state the control data receiver is given priority over the video streamers. This is necessary because the control data includes some information for video control.

Processing Video Streamer Data. Video data are prepared and sent by the CD. Before sending the data, the Cryptographic Engine processes the video data in two stages for encryption and authentication. First, the Cryptographic Engine receives the video data block to be encrypted and either the cipher text block of the previous block or the encryption initialization vector (IV). Secondly the Cryptographic Engine is fed with the encrypted video data block and either with the intermediate MAC value or with the authentication initialization vector.

Processing Control Data. Control data are sent to the drone by remote control. The Cryptographic Engine processes the control data in two stages before sending it the to the drone. First, in the authentication stage the Cryptographic Engine receives the data block and either the intermediate MAC value or the authentication initialization vector. Secondly, in a decryption stage the

Cryptographic Engine processes either the encrypted control data block or the encryption initialization vector.

4.2 Remote Control Data Receiver

The Control Data Receiver receives control data from the communication controller in form of a 384-bit packet that is compound of three 128-bit blocks. The first block represents the encryption initialization vector IV_{enc} which is not encrypted but authenticated by the ground station. The second block is the control block that includes the actual control data in encrypted form. The third block is the MAC value of the first two blocks. These data are sent to the Cryptographic Engine for authentication and to decrypt the control data block.

4.3 Video Streamer

Control data are sent from the ground station at a low rate according to the PPM scheme. In contrast, video data are sent continuously at high rate. One image occupies many packets. The size of the packet relies on the used communication module.

Each video packet includes an 128-bit encryption initialization vector IV_{enc} (or the last cipher text block), a variable number of 128-bit video cipher text blocks, a 128-bit encrypted status block, and the 128-bit MAC value of the entire packet.

The Video Streamer receives the video data byte-wise from the JPEG Encoder through a first-in first-out memory (FIFO). Using a shift register, 16 bytes of these data are concatenated to construct a 128-bit data block. In addition to the video data, the Video Streamer constructs and appends a status block to each downstream packet. The VS controller also exchanges control signals with the Control Data Receiver, the Cryptographic Engine, the Communication Module, and the JPEG Encoder. Data is processed according to a developed abstract finite state machine which is responsible for creating the different block of encrypted data according to the stream.

4.4 Digital-2-PPM Converter

The used remote control generates a PPM frame with a length of 22 ms. For each control channel a rectangular pulse is produced, whereas the pulse width is proportional to the control value. The minimum and the maximum width is 0.7 ms or 1.5ms, respectively. The minimum distance between each two succeeding pulses is 0.4 ms. The remaining time of the 22 ms is used as a start signal.

The CD receives all the channel data at once embedded in the control block inside the control data packet. The PPM signal is generated using different counters. The first counter has a fixed preset value that depends on the clock frequency to produce the start pulse. The second counter produces the control pulse. It has a variable preset value to produce time values between the minimum

and maximum width of a PPM pulse. The preset value of this counter is the 8-bit digital value of the corresponding control channel. The third counter produces the pause periods which vary between 1.8 and 0.4 ms.

4.5 Other Components

The FPGA hardware includes a communication module and a JPEG encoder that includes a controller for the camera. The JPEG encoder was adopted from [18] and adapted to suit our design.

5 Implementation

To evaluate our solution a complete system prototype was implemented. The system prototype consists of a radio transmitter, a personal computer, and a drone extended with the security module.

The drone was prototyped as a quadrotor based on the Next-Generation Universal Aerial Video Platform (NG-UAVP). The NG-UAVP is "a community-driven open source project to build a modern autonomously flying multicopter" [19]. The NG-UAVP has a special focus on expandability and configurability with a proprietary near real-time operating system and a hardware abstraction layer that enables the platform to support different hardware types and configurations. The NG-UAVP uses three microcontrollers for data acquisition and preparation on the sensor's board and for flight control.

The quadrotor is extended with the security module and a camera module. The camera used is the TCM8240MD from Toshiba with an image resolution of 640×480 pixel, a frame rate of 30 fps, and a color depth of 24 bit. One of the selection criteria of this camera was its small size of $6 \times 6 \times 4.5$ mm. The camera has an Inter-Integrated Circuit (I^2C) interface for configuration and delivers pixel data over an 8-bit parallel interface along with two lines for vertical and horizontal synchronization.

The security module is compatible with the other NG-UAVP boards. It contains mainly a communication module, an FPGA, and a flash memory for programming the FPGA. The used communication module (from the company Avisaro AG) is connected to the FPGA through a serial peripheral interface (SPI), which allows a maximum data rate of 2.8 MBit/s.

As an FPGA we use Spartan E from Xilinx. Image processing demands large memory size. The used open-source JPEG encoder works on 8×8-pixel blocks. However, data is read from the camera row by row. Thus, for the JPEG encoder to start, at least seven rows and the first 8 pixels of the 8-th row must be read first. With 640 pixel per row and 24-bit color depth a minimum memory space of $(7*640+8)*24 = 108$ kbit is required. To increase throughput, the JPEG encoder uses pipelined processing of 16 rows which demands a total memory usage of 163.840 kbit. Additional memory space is required for the encoder output buffer, for the AES Sboxes, and for the input and output FIFOs of the video streamers.

Instead of using external memory for data storage we decided to use the largest member of the Spartan E family. By this means, the design is kept simpler and data is transferred synchronously between the different FPGA components, which is essential for the performance. The FPGA works at 50 MHz clock frequency that is supplied by an external oscillator. The FPGA is configured using a SPI serial flash PROM (programmable read-only memory) from Atmel.

6 Results and Analysis

The hardware prototype was tested for the data given in Table 3. The raw frame size results from multiplying the image resolution by the color depth. Through encoding, the frame size is reduced 15 times. The encoded frame is divided by 128 to get the number of AES blocks that need to be processed for one frame.

Table 3. Image Parameters used in the Prototype Implementation.

Parameter	Value	Unit
Image resolution	640×480	pixel
Color depth	24	bit
Frame size before encoding	7372800	bit
Compression ratio	15	%
Frame size after encoding	491520	bit
No. AES blocks per frame	3840	Block

Table 4 shows a comparison between the hardware solution and a comparable software solution running on the drone microcontroller ARM7 LPC2148 clocked at 60 MHz. The comparison metrics are the timing, the power consumption, and flight time.

With respect to timing, the developed FPGA solution provides an approximately 20-time higher throughput than the software solution. The software solution only achieves a frame rate of 3.2 fps, which is clearly below acceptable rates for live feed, and therefore fails to deliver a moving picture.

With respect to power, the consumption of the hardware solution exceeds the consumption of the software solution by 3.356 watts. This amount comprises three components:

1. The power consumption of the FPGA chip as provided by the Xilinx Xpower Analyzer (0.22 watts).
2. The measured electrical power consumed by the FPGA board exclusive of the FPGA chip (0.64 watts)
3. The mechanical power needed to raise the additional weight caused by the FPGA card (2.5 watt). This value was determined using a commercial calculator as detailed below.

Table 4. A HW-SW Comparison of the Image Coding, Encryption, and Authentication.

Compared Value	Software	Hardware	Unit
Time needed to encode one JPEG frame	100	14.4	ms
Time needed to encrypt and authenticate one JPEG frame	209.6	1.54	ms
Time needed to encode, encrypt and authenticate one JPEG frame	309.6	15.9	ms
Throughput	3.2	62.8	fps
Measured drone power consumption while hovering	220	223.36	watt
Estimated flight time under maximum possible throughput	9.03	8.89	min

By comparing the pure computational power consumption, the FPGA with 0.22 watt is superior to the software solution that consumes 1.8 watt on ARM7 LPC2148. This is in line with the general understanding of FPGAs as power-efficient alternatives to software. This is valid even when we compare with the power consumed by the entire FPGA board ($0.64 + 0.22 = 0.88$ watt).

In this application, however, we have to consider the power needed to carry the weight of the FPGA board. Apparently, this part is significant and it contributes to shortening the flight time by almost 1.5 %. The latter figure is based on the voltage and the capacity of the battery used in our model. These are 14 volts and 2300 mAh, respectively.

Note, however, that the actual impact on the flight time should be considered in the light of the required throughput. The advantage of the software solution is only valid when 3.2 fps or less are required. As stated before, this rate is not sufficient for moving pictures.

To determine the power needed to carry the FPGA we used eCalc which is a commercially available online tool that provides calculations for electrically driven remote controlled devices [20]. The vendor states that the calculation accuracy is 10 %. eCalc provides four different tools for RC model calculation: propeller airplanes, multicopters, ducted fan airplanes and helicopters. eCalc can be used for free however with limited capability in terms of supported models and components as well as provided output data. For our calculations we used the commercial edition of eCalc to be as specific as possible in the data entry.

It is important to note that the obtained throughput of the hardware implementation can be easily optimized by using different techniques such as parallelism and pipelining and/or by using more memory. However, for the sake of proof-of-concept implementation, the delivered throughput of 62.8 fps was satisfactory, as it is more than twice the rate needed for moving pictures.

7 Conclusions

The chapter presented a security analysis for civil drone communication. Considering security aspects of the drone technology is urgent at this stage because

of the rapidly increasing interest in applying this technology in diverse private, commercial, and governmental areas. Unfortunately, civil drone vendors are still focusing on functional aspects of drones and we are not aware of any supplier that underlines the security requirements of civil drones.

The chapter highlighted that the security requirements on drones differ from one use case to another. That means that the concept of "one size fits all" should not be used when developing security controls for civil drones. This is because such a solution would be the one that provides the highest level of confidentiality, integrity, and availability regardless of the requirements of the use case. This would not only cause unnecessary costs but also affect the system performance and power consumption negatively. Furthermore, additional overhead would be caused to manage the security solution including key management.

Given the computational overhead of cryptographic operations and, at the same time, the required flexibility to add as much security controls as necessary, configurable hardware such as Field Programmable Gate Arrays offers a suitable alternative for fast and adaptable prototyping.

While developing hardware accelerators for light-weight drones, special attention should be paid to the contribution of the additional hardware weight to the total power consumption. While our case study showed this aspect as an example, more research is required to specify the relation between the speedup obtained by hardware and the additional power consumption and, thus, the flight endurance.

Although the GPS spoofing is one of the serious threats on UAV [21], it is not the focus of our chapter. This chapter is concerned more about providing information flow between CDs and ground station with confidentiality and authentication services. In order to achieve this, we used symmetric key cryptography. As mentioned previously, symmetric keys are generated by the ground station and are installed on the FPGA directly. This way, the shared keys can be protected as they will never be "online". Nevertheless, we are aware that there is a scalability issue here: If there are many CDs to deploy, sharing different keys with each drone will overload the ground station. To alleviate this, we may use public key cryptography. But this should cope with another operational issue of handling digital certificates. For this reason, we envision that identity-based cryptography [22] might be helpful. We leave this as our future work.

References

1. Quaritsch, M., Stojanovski, E., Bettstetter, C., Friedrich, G., Hellwagner, H., Rinner, B., Hofbaur, M., Shah, M.: Collaborative microdrones: applications and research challenges. In: Proceedings of the 2nd International Conference on Autonomic Computing and Communication Systems, p. 38. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering) (2008)
2. Gancet, J., Hattenberger, G., Alami, R., Lacroix, S.: Task planning and control for a multi-UAV system: architecture and algorithms. In: 2005 IEEE/RSJ International Conference on Intelligent Robots and Systems, IROS 2005, pp. 1017–1022. IEEE (2005)

3. How, J., Bethke, B., Frank, A., Dale, D., Vian, J.: Real-time indoor autonomous vehicle test environment. IEEE Control Syst. Mag. **28**, 51–64 (2008)
4. Hoffmann, G., Rajnarayan, D., Waslander, S., Dostal, D., Jang, J., Tomlin, C.: The stanford testbed of autonomous rotorcraft for multi agent control (STARMAC). In: The 23rd Digital Avionics Systems Conference, DASC 2004, vol. 2, p. 12-E. IEEE (2004)
5. Chiu, C., Lo, C.: Vision-only automatic flight control for small UAVs. IEEE Trans. Veh. Technol. **60**, 2425–2437 (2011)
6. Dierks, T., Jagannathan, S.: Output feedback control of a quadrotor UAV using neural networks. IEEE Trans. Neural Netw. **21**, 50–66 (2010)
7. Voos, H.: Nonlinear state-dependent riccati equation control of a quadrotor UAV. In: 2006 IEEE International Conference on Control Applications Computer Aided Control System Design, 2006 IEEE International Symposium on Intelligent Control, pp. 2547–2552. IEEE (2006)
8. Minguez, J., Montano, L.: Nearness diagram (ND) navigation: collision avoidance in troublesome scenarios. IEEE Trans. Robot. Autom. **20**, 45–59 (2004)
9. Yuan, C., Recktenwald, F., Mallot, H.: Visual steering of UAV in unknown environments. In: IEEE/RSJ International Conference on Intelligent Robots and Systems, IROS 2009, pp. 3906–3911. IEEE (2009)
10. Zsedrovits, T., Zarandy, A., Vanek, B., Peni, T., Bokor, J., Roska, T.: Collision avoidance for UAV using visual detection. In: 2011 IEEE International Symposium on Circuits and Systems (ISCAS), pp. 2173–2176. IEEE (2011)
11. Kim, A., Wampler, B., Goppert, J., Hwang, I., Aldridge, H.: Cyber attack vulnerabilities analysis for unmanned aerial vehicles. Infotech@ Aerospace (2012)
12. Shepard, D.P., Bhatti, J.A., Humphreys, T.E., Fansler, A.A.: Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks. In: Proceedings of the ION GNSS Meeting, vol. 3 (2012)
13. Pelechrinis, K., Iliofotou, M., Krishnamurthy, V.: Denial of service attacks in wireless networks: the case of jammers. Commun. Surv. Tutorials **13**, 245–257 (2011). IEEE
14. Bicakci, K., Tavli, B.: Denial-of-service attacks and countermeasures in IEEE 802.11 wireless networks. Comput. Stand. Interfaces **31**, 931–941 (2009)
15. Daemen, J., Rijmen, V.: The Design of Rijndael: AES-The Advanced Encryption Standard. Springer, Heidelberg (2002)
16. Katz, J., Lindell, Y.: Introduction to Modern Cryptography. Chapman & Hall, Boca Raton (2008)
17. NIST: American national standard for financial institution key management (wholesale) (1985). http://csrc.nist.gov/publications/fips/
18. Krepa, M.: Jpeg encoder, project, mkjpeg. http://opencores.org/
19. ANG-UAVP: Next generation universal aerial videoplatform. http://ng.uavp.ch/moin/FrontPage
20. Mueller, M.: ecalc, on-line calculator for electric driven RC models. http://www.ecalc.ch/
21. Mansfield, K., Eveleigh, T., Holzer, T.H., Sarkani, S.: Unmanned aerial vehicle smart device ground control station cyber security threat model. In: 2013 IEEE International Conference on Technologies for Homeland Security (HST), pp. 722–728. IEEE (2013)
22. Joye, M., Neven, G.: Identity-Based Cryptography, vol. 2. IOS Press, Amsterdam (2009)