Secure Communications for Autonomous Multiple-UAV Media Production

Ioannis Mademlis, Paraskevi Nousi, Damien Lavaux, Thomas Aubourg, Cedric Le Barz and Ioannis Pitas

Abstract Equipping Unmanned Aerial Vehicles (UAVs/drones) with professional cameras has rapidly transformed the media production landscape in recent years. However, their creative potential in aerial cinematography applications can only be fully exploited by enhancing their cognitive autonomy and deploying them in a collaborative, multi-drone fleet setting. Thus, networking, security and data streaming issues arise naturally. In this Chapter, we assume a stand-alone UAV fleet coordinated in real-time by a central on-ground compute station for live outdoor event media coverage, with high-definition, low-latency video streaming from many moving sources. This is the most general and technically difficult filming scenario: on top of security concerns, fluctuations in wireless signal power inevitably make stable wireless communications a real challenge with current technology. Motivated by these difficulties, we designed and evaluated a novel multiple-UAV platform for live

Ioannis Mademlis (*corresponding author)
Aristotle University of Thessaloniki, Aristotle University of Thessaloniki Campus, Thessaloniki, Greece e-mail: imademlis@csd.auth.gr

Paraskevi Nousi
Aristotle University of Thessaloniki, Aristotle University of Thessaloniki Campus, Thessaloniki, Greece e-mail: paranous@csd.auth.gr

Damien Lavaux
Thales, Advanced Studies Department THERESIS, Palaiseau, France e-mail: damien.lavaux@thalesgroup.com

Thomas Aubourg
Thales, Advanced Studies Department THERESIS, Palaiseau, France e-mail: thomas.aubourg@thalesgroup.com

Cédric Le Barz
Thales, Advanced Studies Department THERESIS, Palaiseau, France e-mail: cedric.lebarz@thalesgroup.com

Ioannis Pitas
Aristotle University of Thessaloniki, Aristotle University of Thessaloniki Campus, Thessaloniki, Greece e-mail: pitas@csd.auth.gr

outdoor media production, featuring a communications architecture able to handle and overcome the relevant communication issues. Both 4G/LTE and WiFi are utilized to make this infrastructure easy to deploy, secure and robust, as indicated by the included empirical evaluation. Notably, this is an innovative, prototype platform: the first one specifically designed for handling difficult professional filming scenarios with multiple autonomous UAVs.

Key words: autonomous drones, Unmanned Aerial Vehicle, media production, UAV cinematography, UAV communications, wireless network security, 4G, LTE, WiFi, data streaming

1 Introduction

Unmanned Aerial Vehicles (UAVs, or "drones") have revolutionized the media production landscape during the past decade, by allowing flexible and easy aerial cinematographic shot acquisition, access to narrow, or difficult-to-reach spaces and the possibility to easily obtain impressive footage (e.g., dynamic panoramas or novel, multiview and 360-degree shots). Their ability to fly and/or hover, as well as their small size, high agility and low cost, have made them an indispensable tool in the film/TV/media industry.

The cumbersome logistics of fully manual, professional UAV filming (a trained pilot and a separate camera operator are required per drone, acting with precise coordination during filming) and technological progress are slowly leading the market towards increased adoption of cognitive autonomy functionalities. Commercial cinematography UAVs already provide several autonomous capabilities for both safe flight and filming, such as obstacle detection and avoidance, automated landing, physical target tracking or orbiting (for low-speed, manually preset targets), as well as with automatic central composition framing: that is, constantly rotating the camera so that the preselected target always remains properly centred on-frame.

Clearly, the foreseeable future holds the promise of fully autonomous UAVs that only require minimal, high-level supervision by a human operator. This can be achieved via Artificial Intelligence (AI) algorithms, which run either solely on-board the vehicle, or are split between on-board execution and remote execution on a powerful ground compute station. The AI methods most relevant to autonomous UAVs are computer vision/machine learning algorithms, which conduct semantic visual analysis of each captured video frame (e.g., for object detection on images), and task/motion planning methods, which assign tasks to the UAV and plan/adapt its flight trajectories.

However, filming with a single UAV, which is still the norm in professional media production, severely limits the creative potential. Each target can only be captured from a specific view angle and with a specific framing shot type at any given time, while there can only be a single target at each time instance. Finally, the need to move the UAV from one point to another in order to shoot from a different angle, aim at a different target, or return to the recharge platform, results in "dead" periods that prevent smooth and unobstructed shooting.

A fleet of multiple, cooperating UAVs that are deployed simultaneously for a shooting mission can easily solve the above issues. However, the burden of manual multi-UAV operation makes cognitive autonomy a necessity, achievable through AI and robotics technologies which can greatly enhance the attractiveness of UAV fleets in media production. But that's not the end of the story, since additional issues arise due to the need for communication and coordination between the UAVs. In addition, if the purpose of the shooting mission is live broadcast, an on-ground compute station must be able to handle video streams transmitted simultaneously by all members of the fleet. Depending on the platform's architectural design, this central station may also act as a coordinator between them.

As expected, security is of the utmost importance in a UAV-based media production environment. The consequences of a compromised platform can include serious legal implications and privacy violations. The main risks involved are data hijacking, drone hacking and/or capture during flight by a malicious third party, with the aim of studying it and convert it (e.g., for carrying explosives) or crash it directly on people/infrastructures. In addition, in UAV-based live broadcast, the air-to-ground communication specifications must always ensure a minimum bitrate, sufficient for acceptable real-time video broadcast quality; therefore data streaming is also not trivial.

Overall, communication challenges are especially prominent among the issues an autonomous multiple-UAV platform for media production/cinematography applications must be able to handle. This Chapter assumes an autonomous UAV fleet coordinated by a centralized on-ground compute station for live coverage of outdoor events. This is the most general and technically difficult filming scenario, where wireless signal strength fluctuations are inevitably making radio communications a real challenge with current technology.

Such difficulties have motivated us to design a novel, autonomous multiple-UAV platform specifically targeting live outdoor media production, i.e., the so-called MULTIDRONE platform. This Chapter details said innovative, prototype platform, showcasing that it is indeed able to overcome the relevant communication challenges. MULTIDRONE features a robust and secure architecture, providing resilient and secure communications for UAV control and payload data transport. Both 4G/LTE and WiFi are employed to make this infrastructure easily deployable, secure and resilient, as indicated by the included empirical evaluation. Notably, MULTIDRONE is the first platform specifically designed for handling difficult multiple-UAV professional filming scenarios. However, although the emphasis is on semi-autonomous live filming in extended outdoor environments, the determined challenges and solutions apply equally to a vast range of different applications, with only minor modifications.

Note that this Chapter focuses on the relevant networking, security and data streaming aspects. For the cinematography, artificial intelligence, robotics and software architecture aspects, previous literature can be consulted; it is summarized in Table 1. The remainder of this Chapter is organized in the following manner. Section 2 presents and discusses the various networking, streaming and security issues arising in semi-autonomous multiple-UAV live filming in extended outdoor environments. Then, Section 3 briefly presents the overall MULTIDRONE platform architecture, so as to put into perspective the analysis of its communications subsystems and modules. The following Section 4 details exactly the MULTIDRONE communications architecture, derived from a set of choices aiming at overcoming the challenges mentioned in Section 2. Next, Section 5 details the conducted, partial experimental evaluation of the MULTIDRONE communications platform, before the Chapter is concluded with potential future research and innovation directions in Section 6.

Artificial intelligence	**Software architecture**	**Cinematography**	**Robotics**
[29]	[21]	[17]	[33]
[26]	[20]	[18]	[31]
[27]	[23]	[19]	[5]
[37]	[16]	[14]	[2]
[28]		[15]	[1]
[12]		[13]	[32]
[10]		[3]	[4]
[11]			[7]
[36]			
[35]			

Table 1 Previous literature stemming from MULTIDRONE.

2 Communications for Autonomous Multiple-UAV Filming

2.1 Autonomous Multiple-UAV Filming Architectures

Autonomous multiple-UAV filming typically requires the following types of cognitive software components to be present in the platform:

- **perception** modules; e.g., semantic visual analysis (e.g., object detection/tracking), obstacle/collision detection, localization and mapping (SLAM), etc.
- **planning** modules; e.g., mission/task planning, path planning, etc.
- **control** modules; e.g., UAV trajectory control, UAV formation control, camera/gimbal control, etc.

These SW components can be distributed among the various platform nodes, i.e., the UAVs and, optionally, a central on-ground compute station. Typically, only a subset of them interacts with UAV sensors and motors, but they must all intercommunicate at a high frequency, either via memory (when the components reside on the same node), or wireless networking (in UAV-to-UAV, UAV-to-ground or ground-to-UAV communication exchanges). Additionally, in cinematography applications, high-resolution video stream(s) may also have to be transmitted over-the-air with low latency, regardless of the cognitive SW components.

Three different scenarios of multiple-UAV cinematography applications can be defined:

- off-line shooting with full post-production editing (i.e., for TV programmes or movies);
- filming of live events for deferred broadcast and, thus, with potential post-production modifications (i.e., for deferred TV programmes);
- full live event shooting (i.e., for live TV programmes) with limited post-production effects.

Obviously, full live event shooting is both the most general and the most challenging scenario, therefore it is emphasized by the presented communications architecture. Below, communication issues are first introduced from a high-level perspective.

2.2 Overview of Communications Challenges

In order to successfully deploy fleets of UAVs, especially for live event media coverage applications, having a strong communications infrastructure is crucial. It is difficult to stream high-resolution video (particularly 4K) down to a ground station with Quality-of-Service (QoS) guarantees and simultaneously execute real-time algorithms, even in single-UAV missions. While professional cameras and open-source software can handle on-the-fly video acquisition, compression, synchronization, and transmission, the scarcity of commercial media production-quality camera models with Camera Serial Interface (CSI) connectivity, which guarantees reliable high-speed, low-power data transfer between a camera and a computer, gives rise to practical issues. Using dedicated hardware is not a viable solution due to additional energy consumption, cost, and weight, which are critical factors in UAVs. A trade-off must be made between broadcast video resolution, hardware cost, and degree of vehicle intelligence.

In non-live coverage scenarios, such as filming for deferred broadcast or shooting a scripted sequence, video can simply be stored onboard and retrieved later. However, communications are necessary for all other cases, including non-live single-UAV filming where a subset of the AI algorithms are being executed remotely on a ground compute station. Private QoS-guaranteeing 4G/LTE infrastructure is suitable for outdoor event filming due to the high mobility of the UAVs and long distances that need to be covered. Traditional WiFi is a suboptimal alternative with higher latency and smaller range. Public LTE networks are unreliable because UAV communications cannot be prioritized over telephony. Live broadcasting is the most challenging scenario, even with private LTE infrastructure, leading to a fall back on FullHD resolution for video streaming.

When using a fleet of multiple cooperating UAVs, more problems arise. Available bandwidth may not be enough to support live FullHD video streaming from all drones simultaneously, resulting in a limit on the number of drones. Direct coordination between drones may be required for distributed variants of algorithms or redundancy/fault tolerance, requiring an intra-fleet Flying Ad Hoc Network (FANET, WiFi mesh) that enables ad hoc routing and accounts for dynamic network topology with high node mobility. However, FANETs are not yet a mature technology, and either custom, optimized WiFi extensions, or falling back to LTE infrastructure is necessary for actual deployment, at the cost of increased latency.

Regarding security, simple ways for an attacker to intervene are radio communication or GPS signal jamming, GPS spoofing, UAV autopilot firmware hacking and/or communication hijacking. Additionally, a Man-in-the-Middle attack can allow an unauthorized person to pose as the ground station and take command of the UAV. Weak security in communications can also allow obtaining the video captured by the drone, or its intended flight path.

Moreover, during a shooting session, a subset of the generated data is stored on-board, while another subset is being on-the-fly transmitted over the air. Depending on the application, video footage may be both stored and broadcasted, or only stored on-board for offline processing at a later time. In contrast, real-time transmission of telemetry and control data is necessary for ensuring a secure and safe flight, making them vulnerable to potential security threats. Thus:

- Video footage must be protected during storage, using authentication mechanisms to restrict its accessibility to the copyright owners.
- Telemetry and control commands need to be transmitted at the highest priority and be protected against misuse at the same time.

2.3 Data Streaming Challenges

To stream outdoor events in real-time, there are several cinematography factors that need to be considered, such as tracking targets of interest, adjusting zoom, composition and focus, and using multiple UAVs to get different perspectives. However, these UAVs must also fly autonomously and adhere to safety regulations (e.g., avoid to fly over human crowds, or exceed a specific altitude).

When designing a communications architecture for real-time live video streaming, several factors must be considered, including weak wireless communication, the large size of video data, and the need to use video compression to reduce this size (1 minute of raw 720p 8-bit video at 30 Frames Per Second is 1.55 GBs). H264 and H265 coding are good options, but they introduce delays and quality loss. Using Real-time Transport Protocol (RTP) with User Datagram Protocol (UDP) is a good choice for the network protocol stack, as it prefers timeliness over reliability.

If multiple UAVs are involved in the streaming, clock synchronization becomes important. Network Time Protocol (NTP) can be used to ensure that all devices use a single clock. However, on-board analysis of the captured video frames introduces delays, so metadata, including the results of AI-enabled semantic visual analysis and UAV telemetry, must be transmitted along with the respective video frame, in a manner immune to any compression-induced corruption. This is the only way for any software running at the receiving end, e.g., on a ground compute station, to properly correspond metadata with the respective visual content. The best approach to achieve this is to insert such metadata as an RTP header extension.

GStreamer, an open-source multimedia framework with multiple programming language bindings, can be used for low-level handling of these issues.

3 The MULTIDRONE architecture

This Section briefly describes an innovative prototype platform that attempts to handle the issues and challenges outlined in Section 2. It has been developed in the context of the EU-funded research and development project MULTIDRONE[1], which aimed exactly at designing and implementing a semi-autonomous multiple-UAV platform for live outdoor filming, featuring a small fleet of drones and a ground compute station. The purpose here is not to fully describe the overall MULTIDRONE platform, which has been detailed in [21], but to provide the background necessary for discussing the MULTIDRONE communications architecture in Section 4.

The presented MULTIDRONE architecture includes a fleet of cooperating, camera-equipped UAVs and a central *Ground Station* (GS). GS is employed for preplanning the shooting mission by the Director's team (using an appropriate GUI named "Dashboard") and for dynamic, autonomous mission replanning and execution monitoring. Additionally, it is used for on-line semantic environment mapping concerning human crowds [12], since such areas constitute no-flight zones due to regulations and safety issues. Finally, the *Supervision Station* (SS) is included on-ground, i.e., a GUI permitting a human operator to constantly monitor the status of the UAVs, so as to cancel the mission in case any security issues arise during its execution.

The UAVs are responsible for collectively executing the mission, i.e., mainly filming and physically following prespecified moving targets (e.g., athletes), in an adaptive manner, so as to capture the desired cinematographic shot types. Additionally, they gather visual data to facilitate semantic mapping and on-map localization of targets. Each UAV carries a PixHawk/PX4 Autopilot [22] (i.e., a popular low-level flight trajectory control system), an Intel NUC computer (with a powerful CPU), an NVIDIA Jetson Tegra X2 embedded computing board (containing a CPU and a powerful GP-GPU), two cameras (a "navigation camera", or NavCam, and a "cinematographic camera", or CinCam), a gimbal and a lightweight LiDAR. Multiple functionalities are implemented by on-board software components, such as autonomous UAV localization and control, gimbal/camera control and obstacle/collision avoidance.

The Jetson TX2 board is employed for on-board, on-the-fly semantic visual analysis of the captured video frames [26]. In general, a wide range of human-centered

[1] https://multidrone.eu/

visual analysis algorithms could be employed, although the emphasis of MULTIDRONE is on on-board object detection and tracking [35, 36] and on on-ground human crowd detection [37]. The Intel NUC computer is employed for executing on-board localization and control SW modules [31]. Overall, the majority of the platform's software components are implemented using the popular Robot Operating System (ROS) middleware [30], which provides the abstractions of *topics* (following a publisher/subscriber model) and *services*, to permit easy inter-process communication across devices.

Backup human pilots on stand-by are supported for safety reasons; the platform allows them to fully take manual control of the UAVs in case of emergency or serious error. The complete MULTIDRONE architecture is presented in detail in [21], while Figure 1 summarizes it at a high-level.

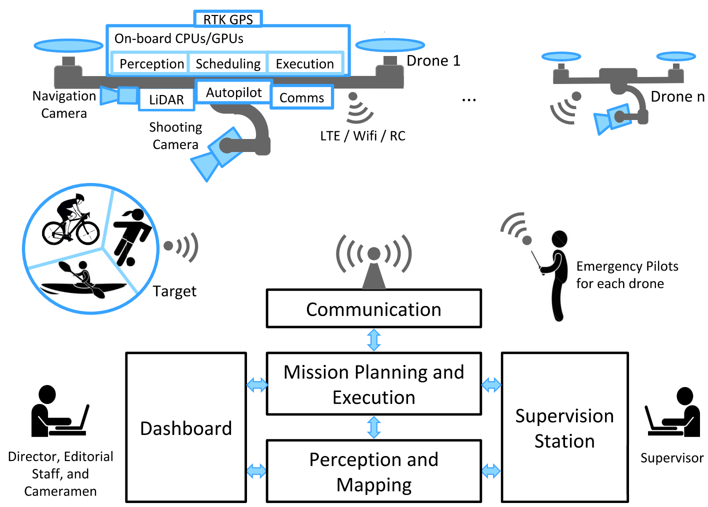


Fig. 1 High-level diagram of the MULTIDRONE architecture: on-board (top) and Ground Station (bottom).

4 MULTIDRONE Communications Module

The majority of the communication exchanges between the UAVs and the GS, including real-time live video streaming, are assured by an LTE system [24], composed of an LTE user equipment on-board and an LTE base station on-ground. Inter-UAV communications are assured by an auxiliary WiFi mesh (WiFi) [9]. This acts as: i) a redundancy feature, in case a UAV loses 4G/LTE access due to signal fluctuations, and ii) a medium of inter-UAV coordination for on-the-fly UAV formation

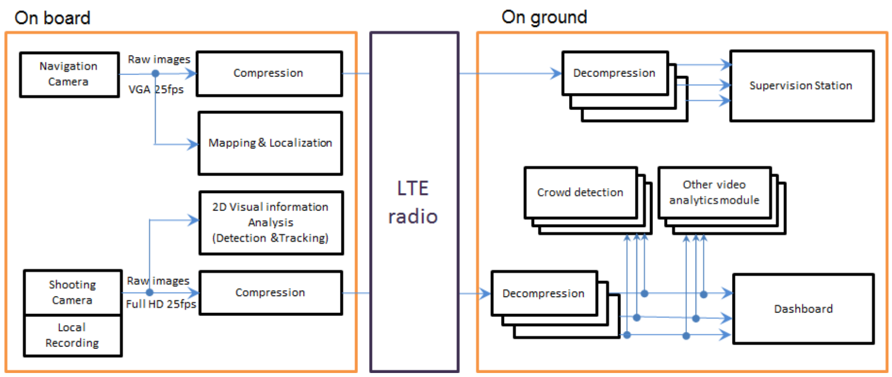


Fig. 2 Data flow for video streaming from the UAVs to the ground.

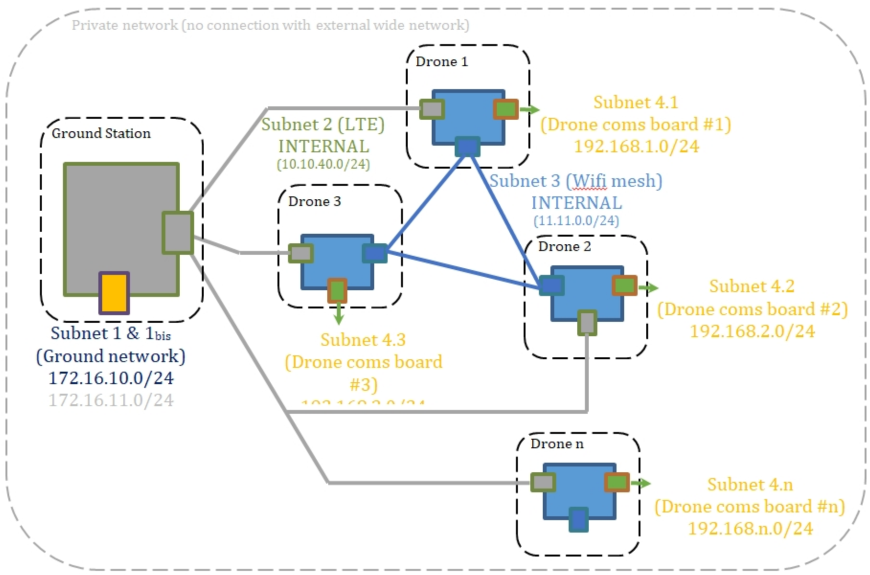


Fig. 3 Communication network addressing (complete).

control algorithms (e.g., to facilitate capturing multiview cinematic shots of moving targets). Each UAV carries on-board a dedicated *Communication Module* (CM) that is responsible for:

- Acting as a default IP communication gateway/router to the ground and to other UAVs.
- Scheduling IP flows depending on applications' precedence and assigned IP QoS.
- Traffic shaping / admission control when congestion occurs.
- Authentication, encryption and other security-related mechanisms.

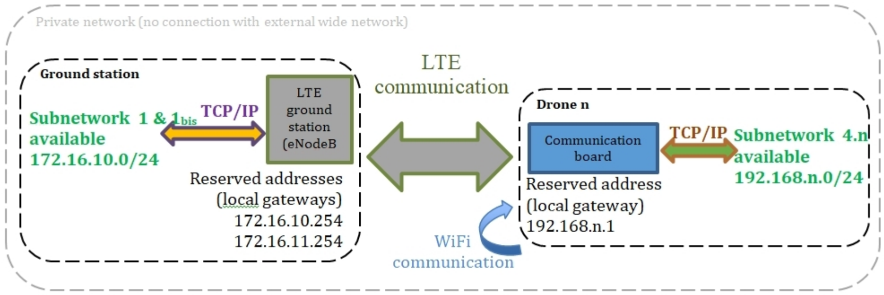


Fig. 4 Communication network addressing (user point-of-view).

The infrastructure is fully independent of any public LTE operator and provides a high level of real-time performance and cybersecurity: it offers plenty of available network bandwidth, long range of transmission, fine-grained QoS management and enhanced streams protection, with Virtual Private Network (VPN) tunneling and strong encryption.

The network topology provided for MULTIDRONE is designed to be as transparent as possible for the various software modules. LTE and WiFi subnetworks are routed to simplify the communication between each node, but certain constraints have been taken into account to ensure an efficient system behavior.

- All communications with the LTE system must be IP-based.
- IP addressing of on-board UAV computers and the GS conforms to the one detailed by Figures 3 and 4.

CM can be considered as a default IP router for the rest of the system. As such, it exposes an Ethernet interface to the computers on-board the UAV and implements a full IP protocol stack. Since it is fully independent from the other modules in the architecture, it has its own hardware and operating system (Linux OpenWRT). In addition, a separate *Video Streamer* (VS) module is necessary for video transmission and interacts heavily with CM. For each UAV, two video streams are generated: one by the NavCam (H.264 compressed, 4:2:0 chroma subsampling, 640x480 resolution), another one by the CinCam (H.264 compressed, 4:2:2 chroma subsampling, 1920x1080 resolution, @25fps).

A Blackmagic Micro Cinema Camera with a motorised Panasonic x3 lens was selected as the CinCam, supporting FullHD resolution. On the other hand, the NavCam does not require FullHD, since its main purpose is simply to provide the SS with good situational awareness. Compression takes place on-board the NVIDIA Jetson TX2 platform, which offers hardware-accelerated image/video compression. Video streams are then transmitted through the LTE radio network using RTP. The RTP Control Protocol (RTCP) is also used for on-ground synchronization of video streams coming from different UAVs. The RTP packets hold a 32-bit RTP timestamp. Several consecutive RTP packets may have equal timestamps if they are (logically) generated at once, e.g., they belong to the same video frame. The Sender Report

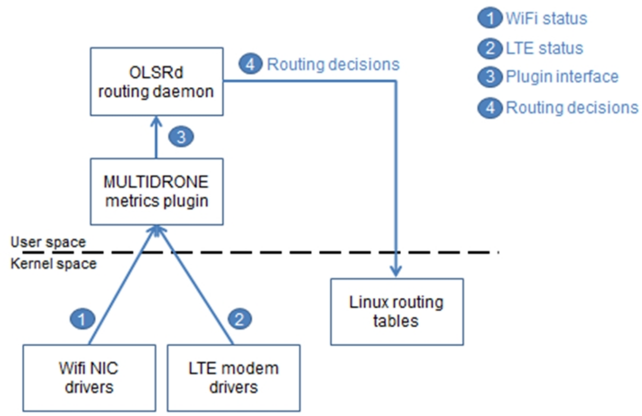


Fig. 5 Routing functional diagram.

packet holds the correspondence between the RTP timestamp and the absolute 64-bit timestamp (system hour), that is broadcasted through the LTE network thanks to NTP.

Figure 2 depicts the data flow for all video streams. It is assumed that 3 UAVs are connected to the GS. The CinCam video streams are transmitted to the Dashboard through the radio network. In parallel, the streams are also resized so that they can be processed on-board by the perception modules. VS can process either the images coming from the CinCam, or from the NavCam, depending on the situation. On-ground, these streams will be uncompressed to be displayed on the Dashboard and, also, resized to be processed by any video analysis modules.

Regarding system scalability, increasing the number of UAVs only implies updating the configuration and hardware of the LTE modules. Of course, the required bandwidth should be manageable by the communication base station. Apart from that, there is no other major impact on the overall communication architecture.

Redundant RF communications are also provided for safety, through additional links. An example would be in case of LTE streaming failure. The navigation stream is sent to the backup pilot via RF in manual mode, thus an analog signal is required. RF can also handle the commands to control the gimbal and the camera from a transmitter. The Pixhawk may receive at the same time commands coming from the RF receiver and from the on-board computer, which received it from the Dashboard through the LTE.

4.1 MULTIDRONE Routing and Link Monitoring

Multiple IP subnetworks are being used in MULTIDRONE, requiring IP routing between them to achieve end-to-end IP communications. While manual IP routing could be used, such a solution would be completely static and thus would not allow for dynamically and automatically changing the data transfer path. In order to introduce the required dynamics, the routing configuration is setup as depicted in Figure 5.

4.1.1 OLSRd Routing Daemon

The Optimized Link State Routing Protocol (OLSR) [6] is an IP routing protocol optimized for Mobile Ad Hoc Networks (MANETs). It is standardised at IETF under RFC 3626. OLSR is a proactive link-state routing protocol, which uses hello and topology control (TC) messages to discover and then disseminate link state information throughout the MANET. Individual nodes use this topology information to compute next hop destinations for all nodes in the network using shortest hop forwarding paths. The protocol is an optimization of the classical link state algorithm, tailored to MANET requirements. The key concept used is that of multipoint relays (MPRs). MPRs are selected nodes which forward broadcast messages during the flooding process. This substantially reduces the message overhead compared to a classical flooding mechanism, where every node retransmits each message when it receives its first copy. In OLSR, link state information is generated only by nodes elected as MPRs. Thus, a second optimization is achieved by minimizing the number of control messages flooded in the network. As a third optimization, an MPR node may choose to report only links between itself and its MPR selectors. Hence, contrary to the classic link state algorithm, partial link state information is distributed in the network and used for route calculation. OLSR provides optimal routes (in terms of number of hops). The OLSR Daemon (OLSRd) used in MULTIDRONE is the reference implementation of the IETF RFC 3626 from the OLSR.org association.

4.1.2 MULTIDRONE Metrics Plugin

The MULTIDRONE Metrics plugin has been developed in order to monitor link status (availability, performances) and report the results to the OLSRd routing daemon for route computation. The MULTIDRONE Metrics plugin comes as an OLSRd plugin. OLSRd supports loading of dynamically linked libraries (called plugins) for generation and processing of private package-types and any other custom functionality. The plugin design was chosen for, among others, the following reasons:

- No need to change any code in the OLSR daemon to add our MULTIDRONE custom metric or functionality.
- Plugins can be written in any language that can be compiled as a dynamic library.
- The plugin interface will always be backwards compatible.

Its interface with OLSRd is depicted in Figure 6.

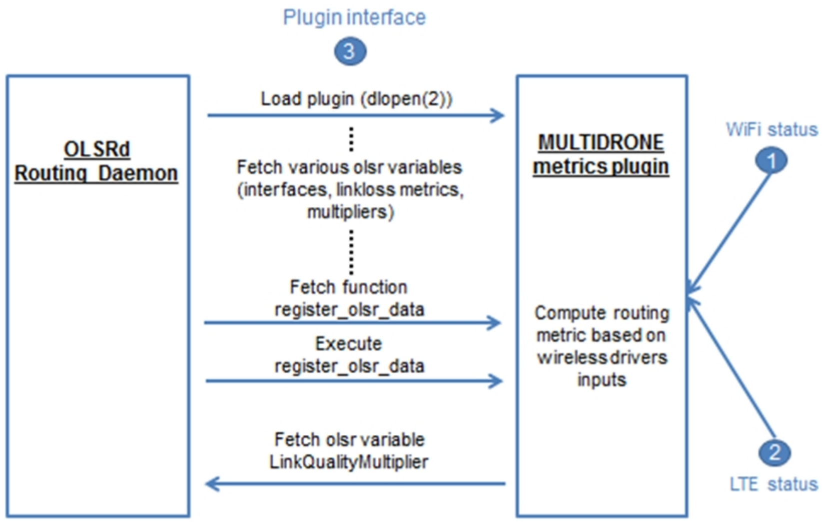


Fig. 6 The MULTIDRONE metrics plugin interface with OLSRd.

4.1.3 Metric computation

Computation of the routing metric injected into OLSR is based on the wireless link status/info provided from the LTE and WiFi drivers. The metric value is influenced by:

- Signal strengths ($SStrengthI_{LTE}$ and $SStrenghI_{WiFi}$) — By selecting paths with strong signal, paths which can support high-data rates with small error rates are typically preferred.
- Link status: down or up.
- LTE bias: a bias (α) is introduced into the routing metric computation in order to avoid changing path too frequently. Indeed, frequent metric changes will introduce routing instability and latency in the routing algorithm convergence time. This bias is intended to favour LTE in case both LTE and WiFi links are available.

The legacy sum of OLSR ETX [25] metric on path is evaluated by OLSRd itself ($\sum ETX_{WiFiPath}$). With these values and parameters, the OLSR routing metric is:

$$OLSR_{LQ_{WiFi}} = \sum ETX_{WiFiPath} * \alpha * \frac{SStrengthI_{LTE}}{SStrenghI_{WiFi}}. \quad (1)$$

We use non-intrusive methods for obtaining the signal strength, for both LTE and WiFi, and estimate bandwidths. We do not generate measurement overhead that could potentially hurt the active payload flows generated by the MULTIDRONE platform. These methods are based on passive monitoring, which allows a wireless node to intercept the transmission activities of its own radios by consulting the wireless drivers.

4.2 MULTIDRONE Security Functions

MULTIDRONE's CM is not only in charge of routing IP traffic, but also of enforcing security functions for secure communications. Indeed, even if 4G LTE used in MULTIDRONE uses symmetric-key cryptography to (1) authenticate the subscriber (phone), and (2) encrypt data sent over the 4G wireless link (128 bit encryption), potential threats that can be exploited by a malicious attacker still exist. Even if this risk is considered minimal, the criticality of UAV control commands and the value of cinematography content require additional security measures that are described in this Subsection.

4.2.1 IPsec deployment

In order to add end-to-end authentication and encryption on top of LTE, we chose the IPsec protocol [8] in a site-to-site configuration, in which each IPsec gateway is embedded into the MULTIDRONE CMs. IP flows are encrypted using AES-256 encryption on top of LTE's own encryption (based on AES 128 bit encryption). The designed IPsec security topology is based on site-to-site tunnelling used with the on-board and the ground CMs as tunnel end-points, thus efficiently encrypting all traffic generated by MULTIDRONE applications and expected to be transported by the LTE network.

The greatest advantage of IPsec is its transparency to MULTIDRONE applications. Since IPsec operates at OSI Layer 3 (IP), it has no significant impact on the higher network layers and no impact at all on the application layer. It is indifferent as to whether application traffic is being transported using TCP or UDP protocols. Consequently, IPsec is equally appropriate for securing real-time traffic (such as UAV video streams) and for traditional data applications using the ROS middleware.

IPsec is a suite of related protocols for cryptographically securing communications at the IP layer. IPsec also provides methods for the manual and automatic negotiation of *Security Associations* (SAs) and key distribution, with all the necessary attributes gathered in a *Domain of Interpretation* (DOI). The IPsec DOI is a document containing definitions for all the security parameters required for the successful negotiation of a VPN tunnel; essentially, all the attributes required for SA and Internet Key Exchange (IKE) negotiations. Additionally, since IPsec is deployed between the ground and the on-board CMs, it is not required for other MULTIDRONE computers to be IPsec capable.

4.2.2 Internet Key Exchange (IKEv2)

In order to establish the SAs required by IPsec between the ground and the on-board CMs, it is required to deploy a keying daemon. For this purpose, StrongSwan [34] is deployed on all CMs. StrongSwan is a keying daemon capable of using the *Internet Key Exchange* protocols (IKEv1 and IKEv2). IKE provides strong authentication of CMs and derives unique cryptographic session keys. Besides authentication and key material, IKE also provides the means to exchange configuration information (e.g., virtual IP addresses) and to negotiate IPsec SAs, which are often called CHILD-SAs. IPsec SAs define which network traffic is to be secured and how it has to be encrypted and authenticated. A CHILD-SA consists of two components:

- The actual IPsec SAs (there are two, one in each direction) describing the algorithms and keys used to encrypt and authenticate the traffic.
- The policies (there are at least two) that define which network traffic shall use such an SA.

The policies work both ways, that is, only traffic matching an inbound policy is allowed after decryption. Policies are derived from the *Traffic Selectors* (TS) negotiated via IKE when establishing a CHILD-SA. Unprotected traffic that the kernel receives and for which there is a matching inbound IPsec policy are dropped for security reasons. The actual IPsec traffic is not handled by strongSwan, but instead by the network and the IPsec stack of the operating system kernel.

Generally, IPsec processing and routing are two different topics. For the purpose of MULTIDRONE, IPsec is bumped into the stack and the original routing decision for the unprotected packet also applies to the protected packet. In this sense, IPsec was configured to be deployed in a policy-based manner, instead of route-based which is a less flexible mode.

Authentication is required to ensure that the peer with an IKE-SA is really who it claims to be. StrongSwan provides several methods to do this:

- Public Key Authentication
- Pre-Shared-Key (PSK)
- Extensible Authentication Protocol (EAP)
- eXtended Authentication (XAuth)

In the context of MULTIDRONE, Pre-Shared Key (PSK) was used for its ease of deployment, although it comes at the "cost" of requiring strong secrecy to be secure.

4.2.3 Advanced Encryption Standard (AES-256) and Cryptographic Hardware Acceleration

The purpose of cryptographic hardware acceleration is to offload the computation-intensive tasks of IP packet encryption/decryption and compression/decompression. Acceleration is achieved by executing any arithmetic calculations required by the AES-256 algorithm on dedicated hardware, instead of having the CPU in charge of it. A Cryptographic Hardware Accelerator can be:

- integrated into the System-on-Chip (SoC) as a separate, special-purpose processor.
- integrated in a co-processor on the circuit board.
- contained on a chip on an extension circuit board, that can be connected to the mainboard via some bus, e.g., PCI.

The i.MX6 Processors used in the MULTIDRONE on-board CM offer hardware encryption through Freescale's Cryptographic Accelerator and Assurance Module (CAAM, also known as SEC4). It offers the following support:

- Security Control.
- Advanced High Assurance Boot (A-HAB) System (HAB with embedded enhancements).
- SHA-256, 2048-bit RSA key.

For AES-256 encryption, the MULTIDRONE on-board CM is set-up to make use of the hardware cryptographic accelerators on-board the i.MX6 processors. The latter leverage a CAAM driver to make use of the above features, via the Linux CryptoAPI. The driver itself is integrated with the Crypto API kernel service, in which the algorithms supported by CAAM can replace the native software implementations. The Cryptodev module is implemented as an out-of-kernel module and, therefore, must be compiled against the i.MX6 kernel.

4.3 MULTIDRONE Quality-of-Service

In order to exploit the full capacity of the wireless links provided by the CMs, QoS is deployed. It is based on the Diffserv model and uses DSCP marking and different LTE radio bearers in order to classify, mark, and then enforce QoS on each IP flow depending on its Class-of-Service (COS). Table 2 provides the classification and mapping of each data stream (according to the protocols used) to a dedicated LTE QoS bearer:

Table 2 MULTIDRONE QoS specifications.

Service Type	Protocol	Precedence	QoS QCI	QoS Priority	Max Latency (ms)	Max Packet Loss
Telemetry	MAVLink	High	5	1	100	10^{-6}
Control and signalling	ROS	High	2	4	150	10^{-10}
NavCam video stream	RTP/RTCP/UDP	Medium	3	3	50	10^{-10}
NTP	NTP	Medium	7	7	100	10^{-3}
CinCam video stream	RTP/RTCP/UDP	Low	Best effort	Best effort	Best effort	Best effort

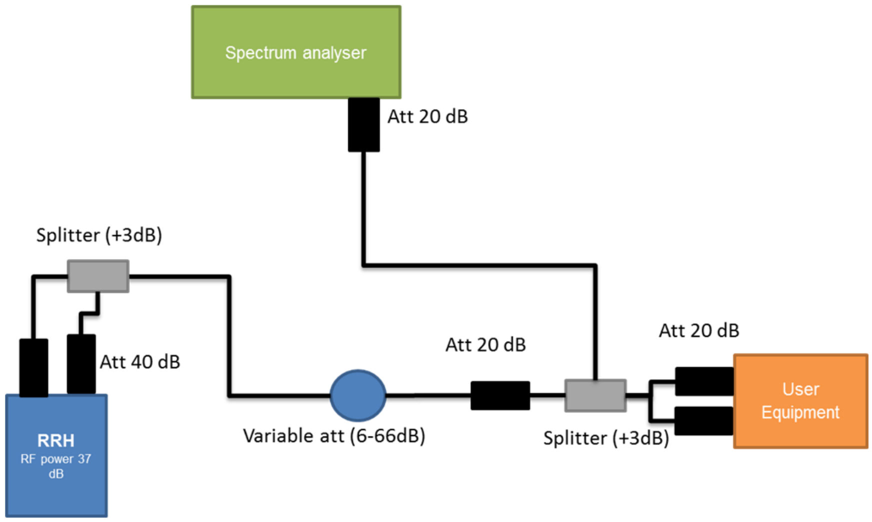


Fig. 7 LTE testbed setup.

The CinCam video stream has its precedence set to Low and a best-effort method, due to the higher criticality of the other streams. Without an optimal control/command and safety services (such as ROS) the UAVs are not able to fly. The NavCam video stream needs the QoS with the lowest latency to allow the backup pilot to have the best control of the vehicle if needed (only one QoS bearer allows a latency with a maximum of 50ms).

The different ROS messages cannot be separated in different QoS classes without a specific DSCP marking. The approach chosen for MULTIDRONE was to aggregate all the ROS messages into the same QoS class, thanks to the UDP/TCP port management. Alternatively, one could employ ROS proxies with a dedicated ROS node per UAV and a dedicated ROS node on-ground that subscribes to all ROS topics, using TCP sockets to transport the messages over-the-air.

5 MULTIDRONE Communications Evaluation

The MULTIDRONE communications infrastructure was evaluated with regard to performance compared to the attenuation, i.e., understanding the impact of distance between the LTE ground station and the UAVs on QoS and the IPsec tunnel.

Bandwidth 20MHz (no QoS)														
notes	UE side					RRH side								
						DL					UL			
	attenuation	TX Power (dBm)	RSSI (dBm)	RSRP (dBm)	SNR (dB)	cqi	mcs	retx	txok	brate (Mb/s)	mcs	rxko	rxok	brate (Mb/s)
WITHOUT TRAFFIC	90	0	-58	-85	30	15	-	0	0	0	-	0	0	0
	90	5	-52	-85	28,8	15	28,0	0	400	14,700	22,6	13	1187	27,5
	93	10	-56	-89	28	15	28,0	0	400	14,700	22,7	13	1187	27,7
	96	13	-59	-92	27,2	15	28,0	0	400	14,700	22,4	13	1182	27
	99	14	-62	-95	26	15	28,0	0	400	14,700	22,6	12	1188	27,5
	102	17	-65	-98	25,6	15	28,0	0	400	14,700	22,7	12	1188	27,6
	103	18	-66	-99	25,2	15	28,0	0	400	14,700	22,7	12	1188	27,6
(FULL THROUGHPUT)	105	19	-68	-101	23,8	15	28,0	0	400	14,700	22,7	13	1187	27,6
(THROUGHPUT START DECREASING)	108	22	-70	-103	22,1	15	28,0	0	400	14,700	22,3	12	1188	26,9
	111	22	-73	-106	20	15	28,0	0	400	14,700	21,5	11	1189	25,3
	114	22	-76	-109	17,4	15	28,0	2	398	14,600	16,0	11	1189	17
	117	22	-79	-112	14,6	13	27,3	4	396	12,900	12,9	11	1189	12,5
	120	23	-82	-115	11	12	14,7	58	342	4,750	7,0	293	870	2,23
	123	23	-85	-119	7,6	10	13,4	104	296	3,670	7,0	388	779	0,869
	124	23	-86	-120	6,4	9	11,6	178	284	2,810	7,0	399	767	0,685
	125	23	-87	-121	5,6	10	11,5	231	295	2,860	7,0	418	746	0,526
	126	23	-88	-122	4,2	9	9,5	172	289	2,390	7,0	414	752	0,41
	127	23	-89	-123	3,8	8	9,0	230	302	2,220	7,0	418	745	0,361
	128	23	-90	-124	2,6	8	9,2	162	303	2,280	7,0	389	775	0,257
	129	23	-91	-126	1,8	7	6,4	180	347	1,980	7,0	405	757	0,216
(RECONNECTION)	131	23	-92	-128	0,6	6	5,0	212	324	1,290	6,2	473	688	0,0972
	133	23	-93	-130	-2,2	5	2,9	141	322	0,800	5,4	404	768	0,0765
	134	23	-94	-131	-4	4	0,7	154	243	0,387	5,2	535	633	0,0591
(BORDER CELL)	135													

Fig. 8 LTE attenuation tests.

5.1 LTE evaluation

All tests were performed with an RF cabled test bed (no over-the-air communication) to keep the environment under control by minimizing interference. The testbed, which is depicted in Figure 7, was composed of:

- 1 Base Band Unit server
- 1 Remote Radio Head
- 1 User Equipment (UE)

Figure 8 depicts the results of the attenuation tests. **UE-ID** is the S1 eNodeB UE identity (unique among all cells), **CQI** is the Channel Quality Indicator (between 0, i.e., bad, and 15, i.e., very good), **mcs** is the Average Modulation and Coding Scheme, **Retx** is the number of transport blocks retransmissions, **txok** is the number of successfully transmitted transport blocks, while **Brate** is the average bitrate (in bits per second).

The conclusion is that a maximum throughput of around 15Mb/s in downlink and 30Mb/s in uplink are available until 108dB of attenuation. It is possible to extrapolate from this attenuation result an approximate distance. To calculate it (assuming free environment, Line-of-Sight condition, no RF loss), the following equation is useful:

$$a = 32.45 + 20log(f) + 20log(d), \tag{2}$$

where a is attenuation in dB, f is center frequency in MHz and d is distance in km. Then, to approximately calculate the distance according to the attenuation and the frequency:

$$d = 10\left[\frac{a - 32.45}{20} - log(f)\right] \tag{3}$$

Thus, according to the tests results and Eqs. (2)-(3), it is possible to achieve approximately 2.55 km with a full throughput, using a center frequency at 2350MHz.

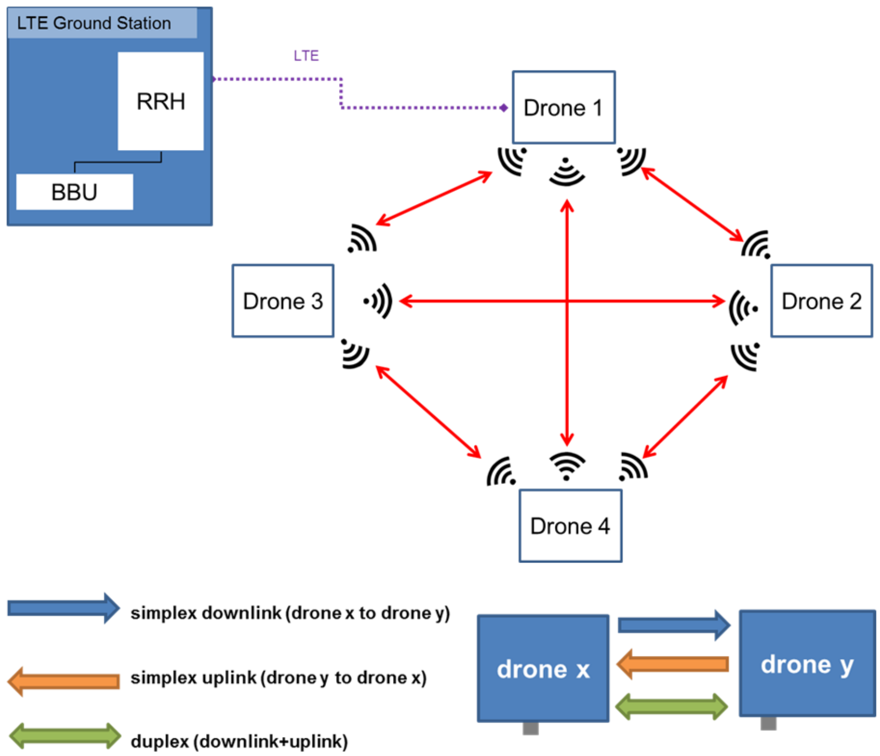


Fig. 9 WiFi mesh testbed setup.

UE + direction		Average throughput (60 sec duration tests)		signal strength		comment
UE	**direction**	**DL (Mb/s)**	**UL (Mb/s)**	**left UE (dBm)**	**right UE (dBm)**	Throughput can't exceed 95,7Mb/s because of PoE switch limitation
1-2	simplex	95.7	95.7	-41	-44	
1-2	duplex	52.4	50.6	-41	-44	
2-3	simplex	95.7	95.6	-47	-37	
2-3	duplex	47.4	48.9	-47	-37	
3-4	simplex	95.7	80.2	-34	-48	
3-4	duplex	54.1	34.4	-34	-48	
1-4	simplex	95.6	95.6	-46	-52	
1-4	duplex	53.1	50.0	-46	-52	
4-2	simplex	95.6	95.6	-45	-43	
4-2	duplex	56.4	53.7	-45	-43	
3-1	simplex	72.5	78.5	-41	-51	
3-1	duplex	33.2	38.5	-41	-51	

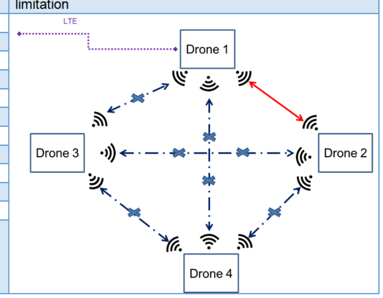
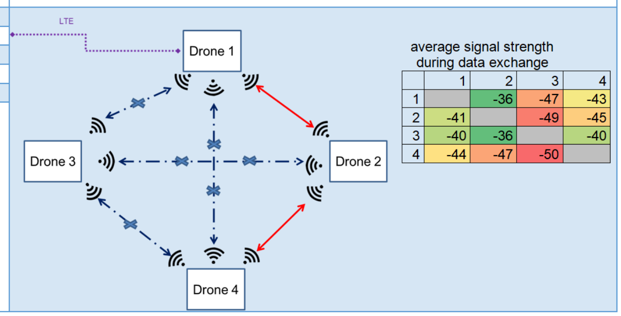


Fig. 10 WiFi mesh evaluation.

5.2 WiFi mesh evaluation

The main goal of these tests is to compare and measure the capacity and performances of the WiFi mesh (IEEE 802.11s protocol) with multiple UEs. Due to the number of

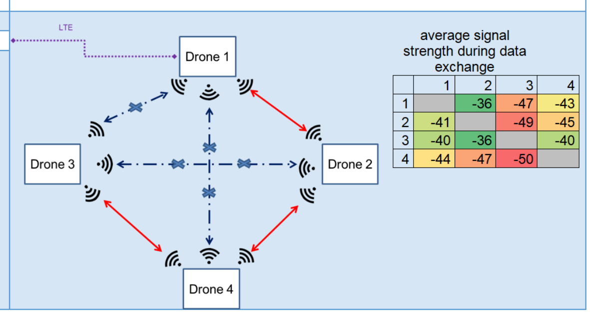
UE + direction		Average throughput (60 sec duration tests)		comment
UE	direction	DL (Mb/s)	UL (Mb/s)	Throughput can't exceed 95,7Mb/s because of PoE switch limitation
1-2-3	simplex	48.5	43.6	
1-2-3	duplex	13.8	10.9	
2-3-4	simplex	45.4	42.9	
2-3-4	duplex	15.6	13.9	
3-4-1	simplex	45.0	33.2	
3-4-1	duplex	9.21	10.1	



	1	2	3	4
1		-36	-47	-43
2	-41		-49	-45
3	-40	-36		-40
4	-44	-47	-50	

Fig. 11 WiFi mesh evaluation.

UE + direction		Average throughput (60 sec duration tests)		comment
UE	direction	DL (Mb/s)	UL (Mb/s)	Throughput can't exceed 95,7Mb/s because of PoE switch limitation
1-2-3-4	simplex	25.5	30.2	
1-2-3-4	duplex	9.26	10.2	



	1	2	3	4
1		-36	-47	-43
2	-41		-49	-45
3	-40	-36		-40
4	-44	-47	-50	

Fig. 12 WiFi mesh evaluation.

UEs, it was not possible to test with RF cable. All these tests are done "over-the-air" in real radio conditions. Compared to wired tests, interference and RF multipaths may occur. The testbed is depicted in Figure 9, while evaluation results are depicted in Figures 10, 11 and 12.

5.3 Overall evaluation

More generally, the overall prototype MULTIDRONE platform evaluation requirements demanded the ability to handle a fleet of three UAVs, with each one transmitting live through LTE a FullHD video stream (H.264 @ 30 Frames Per Second, from the cinematographic camera, at a maximum latency of 100 ms) plus a standard-definition video stream (640x480 pixels, H.264 @ 30 Frames Per Second, from the navigation camera, at a maximum latency of 50 ms). Thus, the system should be demonstrated as able to robustly handle a required bandwidth of about 10 Mbps per UAV. Final evaluation of the overall MULTIDRONE platform indeed confirmed that the system met these goals, achieving a combined uplink throughput of 31 Mbps.

6 Conclusions

Communication issues (networking, security, and data flow) are especially challenging when using autonomous UAV fleets for media production/cinematography applications. The presented innovative, domain-specific, secure and robust communications architecture handles them, while emphasizing the more general and difficult filming scenario, i.e., live outdoor coverage. The designed communications infrastructure (utilizing both 4G/LTE and a WiFi mesh) for a partially autonomous UAV fleet coordinated by a central ground station was described in detail and the rationale behind the choices made was explained in the context of the presented platform. An empirical evaluation demonstrates the latter's effectiveness.

The MULTIDRONE communications platform can serve as a baseline prototype for facilitating research on improved alternatives. Current developments, such as the advent of 5G and recent advances in FANET research (e.g., cluster-based and bio-inspired routing protocols) may be exploited for further augmenting similar platforms with improved Quality-of-Service and enhanced scalability in terms of UAV fleet size, UAV formation range when capturing multiview shots, streamed video resolution, coverage area, etc. An interesting research avenue would be to explore the interplay of such improvements with aesthetic cinematographic constraints.

Acknowledgements The research leading to these results has received funding from the European Union's European Union Horizon 2020 research and innovation programme under grant agreement No 731667 (MULTIDRONE). This publication reflects only the author's views. The European Union is not liable for any use that may be made of the information contained therein.

References

1. Alcantara, A., Capitan, J., Cunha, R., Ollero, A.: Optimal trajectory planning for cinematography with multiple Unmanned Aerial Vehicles. Robotics and Autonomous Systems **140**, 103778 (2021)
2. Alcantara, A., Capitan, J., Torres-Gonzalez, A., Cunha, R., Ollero, A.: Autonomous execution of cinematographic shots with multiple drones. IEEE Access pp. 201300–201316 (2020)
3. Boyle, S., Zhang, F., Bull, D.R.: A subjective study of viewing experience for drone videos using simulated content. In: Proceedings of the IEEE International Conference on Image Processing (ICIP) (2019)
4. Cabecinhas, D., Brás, S., Cunha, R., Silvestre, C., Oliveira, P.: Integrated visual servoing solution to quadrotor stabilization and attitude estimation using a pan and tilt camera. IEEE Transactions on Control Systems Technology (99), 1–16 (2017)

5. Caraballo, L.E., Montes-Romero, A., Diaz-Bañez, J.M., Capitan, J., Torres-Gonzalez, A., Ollero, A.: Autonomous planning for multiple aerial cinematographers. In: Proceedings of the International Conference on Intelligent Robots and Systems (IROS) (2020)
6. Clausen, T., Jacquet, P., Adjih, C., Laouiti, A., Minet, P., Muhlethaler, P., Qayyum, A., Viennot, L.: Optimized link state routing protocol (OLSR). Tech. rep. (2003)
7. Cunha, R., Malaca, M., Sampaio, V., Guerreiro, B., Nousi, P., Mademlis, I., Tefas, A., Pitas, I.: Gimbal control for vision-based target tracking. In: Proceedings of the European Signal Processing Conference (EUSIPCO), Satellite Workshops (2019)
8. Davis, C.R.: IPSec: Securing VPNs. McGraw-Hill Professional (2001)
9. Guillen-Perez, A., Sanchez-Iborra, R., Cano, M.D., Sanchez-Aarnoutse, J.C., Garcia-Haro, J.: WiFi networks on drones. In: Proceedings of ITU Kaleidoscope: ICTs for a Sustainable World (ITU WT). IEEE (2016)
10. Kakaletsis, E., Mademlis, I., Nikolaidis, N., Pitas, I.: Bayesian fusion of multiview human crowd detections for autonomous UAV fleet safety. In: Proceedings of the European Signal Processing Conference (EUSIPCO). IEEE (2020)
11. Kakaletsis, E., Mademlis, I., Nikolaidis, N., Pitas, I.: Multiview vision-based human crowd localization for UAV fleet flight safety. Signal Processing: Image Communication **99**, 116484 (2021)
12. Kakaletsis, E., Symeonidis, C., Tzelepi, M., Mademlis, I., Tefas, A., Nikolaidis, N., Pitas, I.: Computer vision for autonomous UAV flight safety: An overview and a vision-based safe landing pipeline example. ACM Computing Surveys (CSUR) **54**(9), 1–37 (2021)
13. Karakostas, I., Mademlis, I., Nikolaidis, N., Pitas, I.: UAV cinematography constraints imposed by visual target tracking. In: Proceedings of the IEEE International Conference on Image Processing (ICIP) (2018)
14. Karakostas, I., Mademlis, I., Nikolaidis, N., Pitas, I.: Shot type constraints in UAV cinematography for target tracking applications. Information Sciences **506**, 273–294 (2019)
15. Karakostas, I., Mademlis, I., Nikolaidis, N., Pitas, I.: Shot type feasibility in autonomous UAV cinematography. In: IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (2019)
16. Mademlis, I., Mygdalis, V., Nikolaidis, N., Montagnuolo, M., Negro, F., Messina, A., Pitas, I.: High-level multiple-UAV cinematography tools for covering outdoor events. IEEE Transactions on Broadcasting **65**(3), 627–635 (2019)
17. Mademlis, I., Mygdalis, V., Nikolaidis, N., Pitas, I.: Challenges in Autonomous UAV Cinematography: An Overview. In: Proceedings of the IEEE International Conference on Multimedia and Expo (ICME) (2018)
18. Mademlis, I., Nikolaidis, N., Tefas, A., Pitas, I., Wagner, T., Messina, A.: Autonomous unmanned aerial vehicles filming in dynamic unstructured outdoor environments. IEEE Signal Processing Magazine **36**(1), 147–153 (2018)
19. Mademlis, I., Nikolaidis, N., Tefas, A., Pitas, I., Wagner, T., Messina, A.: Autonomous UAV cinematography: A tutorial and a formalized shot type taxonomy. ACM Computing Surveys **52**(5), 105:1–105:33 (2019)
20. Mademlis, I., Torres-Gonzalez, A., Capitan, J., Cunha, R., Guerreiro, B., Messina, A., Negro, F., Le Barz, C., Goncalves, T., Tefas, A., Nikolaidis, N., Pitas, I.: A multiple-UAV software architecture for autonomous media production. In: Proceedings of the European Signal Processing Conference (EUSIPCO), Satellite Workshops (2019)
21. Mademlis, I., Torres-González, A., Capitán, J., Montagnuolo, M., Messina, A., Negro, F., Le Barz, C., Gonçalves, T., Cunha, R., Guerreiro, B., Zhang, F., Boyle, S., Guerout, G., Tefas, A., Nikolaidis, N., Bull, D., Ollero, A., Pitas, I.: A multiple-UAV architecture for autonomous media production. Multimedia Tools and Applications pp. 1–30 (2022)
22. Meier, L., Tanskanen, P., Fraundorfer, F., Pollefeys, M.: Pixhawk: A system for autonomous flight using onboard computer vision. In: Proceedings of the IEEE International Conference on Robotics and Automation (ICRA) (2011)
23. Montes-Romero, A., Torres-González, A., Capitán, J., Montagnuolo, M., Metta, S., Negro, F., Messina, A., Ollero, A.: Director tools for autonomous media production with a team of drones. Applied Sciences **10**(4) (2020)

24. Muruganathan, S.D., Lin, X., Maattanen, H.L., Zou, Z., Hapsari, W., Yasukawa, S.: An overview of 3GPP release-15 study on enhanced LTE support for connected drones. arXiv preprint arXiv:1805.00826 (2018)
25. Ni, X., Lan, K.C., Malaney, R.: On the performance of expected transmission count (ETX) for wireless mesh networks. In: Proceedings of the 3rd International Conference on Performance Evaluation Methodologies and Tools. ICST (2008)
26. Nousi, P., Mademlis, I., Karakostas, I., Tefas, A., Pitas, I.: Embedded UAV real-time visual object detection and tracking. In: Proceedings of the IEEE International Conference on Real-time Computing and Robotics (RCAR) (2019)
27. Nousi, P., Triantafyllidou, D., Tefas, A., Pitas, I.: Re-identification framework for long-term visual object tracking based on object detection and classification. Signal Processing: Image Communication **88**, 115969 (2020)
28. Papaioannidis, C., Mademlis, I., Pitas, I.: Autonomous UAV safety by visual human crowd detection using multi-task deep neural networks. In: Proceedings of the IEEE International Conference on Robotics and Automation (ICRA) (2021)
29. Patrona, F., Nousi, P., Mademlis, I., Tefas, A., Pitas, I.: Visual object detection for autonomous UAV cinematography. In: Proceedings of the Northern Lights Deep Learning Workshop (2020)
30. Quigley, M., Conley, K., B.P., G., J., F., T., F., Leibs, J., Wheeler, R., Ng, A.: ROS: an open-source Robot Operating System. In: Proceedings of the IEEE International Conference on Robotics and Automation (ICRA) Workshop on Open Source Software (2009)
31. Real, F., Torres-González, A., Ramón-Soria, P., Capitán, J., Ollero, A.: UAL: An Abstraction Layer for Unmanned Aerial Vehicles. In: Proceedings of the International Symposium on Aerial Robotics (2018)
32. Real, F., Torres-González, A., Ramón Soria, P., Capitán, J., Ollero, A.: Unmanned aerial vehicle abstraction layer: An abstraction layer to operate unmanned aerial vehicles. International Journal of Advanced Robotic Systems **17**(4), 1–13 (2020)
33. Sabetghadam, B., Alcantara, A., Capitan, J., Cunha, R., Ollero, A., Pascoal, A.: Optimal trajectory planning for autonomous drone cinematography. In: Proceedings of the European Conference on Mobile Robots (2019)
34. Steffen, A.: StrongSwan: the opensource IPsec-based VPN solution (2005). URL https://www.strongswan.org
35. Symeonidis, C., Mademlis, I., Nikolaidis, N., Pitas, I.: Improving neural Non-Maximum Suppression for object detection by exploiting interest-point detectors. In: Proceedings of IEEE International Workshop on Machine Learning for Signal Processing (MLSP) (2019)
36. Triantafyllidou, D., Nousi, P., Tefas, A.: Fast deep convolutional face detection in the wild exploiting hard sample mining. Big Data Research **11**, 65 – 76 (2018)
37. Tzelepi, M., Tefas, A.: Graph-embedded convolutional neural networks in human crowd detection for drone flight safety. IEEE Transactions on Emerging Topics in Computational Intelligence (2019)

Author Biographies

Ioannis Mademlis

Dr. Ioannis Mademlis is a computer scientist, specialized in artificial intelligence. He received a M.Sc. degree in intelligent/cognitive systems (2014) and a Ph.D. in machine learning and computer vision (2018) from the Aristotle University of Thessaloniki, Greece (AUTH). Presently, he is employed as a postdoctoral research associate at AUTH. He has participated in 5 European Union-funded R&D projects, having co-authored more than 50 publications in academic journals and international conferences. He is an IEEE Senior Member and a committee member of the International AI Doctoral Academy (IAIDA). His current research interests include machine learning, computer vision, autonomous robotics and intelligent cinematography.

Paraskevi Nousi

Paraskevi Nousi obtained her B.Sc. and Ph.D. degree in Informatics from the Aristotle University of Thessaloniki in 2014 and 2021 respectively. She is currently a post-doctoral researcher in the Artificial Intelligence and Information Analysis Laboratory in the Department of Informatics at the Aristotle University of Thessaloniki. Her research interests include deep learning for computer vision, robotics, timeseries forecasting and gravitational waves analysis.

Damien Lavaux

Damien Lavaux is an advanced studies engineer at Thales Communications & Security, France. He received his engineering degree from ESME-Sudria Paris engineering school, specializing in telecommunications networks in 2006. He has been involved in collaborative R&D projects since 2007. His current research topics cover wireless, mobile and ad hoc networks, from the software and IP protocol perspective, with a focus on mission-critical communications. He has participated in multiple different EC-funded R&D projects, having coordinated the awarded FP-7 HIT-GATE European R&D project and been technical manager of PPDR-TC.

Thomas Aubourg

Thomas Aubourg received a M.Eng. on computer systems and networks from ESME Sudria in 2015. Since then, he has been working as an engineer with Thales Group in France, specializing in telecommunication networks and aeronautics.

Cedric Le Barz

Cédric Le Barz, Ph.D., is a computer vision research engineer. In 2000, he first joined the imaging group of Philips Semiconductor Company, where he participated in R&D of algorithms for an ASIC dedicated to digital still cameras. He then joined Thales Company, where he initially worked in the Signal Processing team and acquired an expertise in image and video codecs (JPEG2000 & H.264), streaming over wireless networks and video analytics. In 2009, he joined the "Vision Lab" laboratory, a Common CEA/Thales endeavour focused on video analytics. In 2015 he received a Ph.D. on computer vision for UAVs, in collaboration with the French Aerospace Lab (ONERA) and the machine learning team of Paris Sorbonne University. He is now a research engineer with active interests in video streaming/processing and AI for autonomous systems. He has participated in, or coordinated several national or European R&D projects related to computer vision.

Ioannis Pitas

Ioannis Pitas (IEEE Fellow, IEEE Distinguished Lecturer, EURASIP Fellow) received the Diploma and PhD degree in Electrical Engineering, both from the Aristotle University of Thessaloniki (AUTH), Greece. Since 1994, he has been a Professor at the Department of Informatics of AUTH and Director of the Artificial Intelligence and Information Analysis (AIIA) lab. He served as a Visiting Professor at several Universities. His current interests are in the areas of computer vision, machine learning, autonomous systems, intelligent digital media, image/video processing, human-centred interfaces, affective computing, 3D imaging and biomedical imaging. He has published over 906 papers, contributed in 47 books in his areas of interest and edited or (co-)authored another 11 books. He has also been member of the program committee of many scientific conferences and workshops. In the past he served as Associate Editor or co-Editor of 9 international journals and General or Technical Chair of 4 international conferences. He participated in 70 R&D projects, primarily funded by the European Union and is/was principal investigator/researcher in 42 such projects. He has 31600+ citations to his work and h-index 87+ (Google Scholar). Prof. Pitas leads the International AI Doctoral Academy (IAIDA) of the European H2020 R&D project AI4Media https://ai4media.eu/. He coordinates the HE project “TEMA” (g.a.n. 101093003).