sensors

MDPI

Review

UAV IoT Framework Views and Challenges: Towards Protecting Drones as "Things"

Thomas Lagkas [1], Vasileios Argyriou [2], Stamatia Bibi [3] and Panagiotis Sarigiannidis [3,*]

[1] Computer Science Department, The University of Sheffield International Faculty, CITY College, 54626 Thessaloniki, Greece; t.lagkas@sheffield.ac.uk
[2] Department of Networks and Digital Media, Kingston University, Surrey KT1 2EE, UK; vasileios.argyriou@kingston.ac.uk
[3] Department of Informatics and Telecommunication Engineering, University of Western Macedonia, 50100 Kozani, Greece; sbibi@uowm.gr
* Correspondence: psarigiannidis@uowm.gr

Received: 20 October 2018; Accepted: 15 November 2018; Published: 17 November 2018

Abstract: Unmanned aerial vehicles (UAVs) have enormous potential in enabling new applications in various areas, ranging from military, security, medicine, and surveillance to traffic-monitoring applications. Lately, there has been heavy investment in the development of UAVs and multi-UAVs systems that can collaborate and complete missions more efficiently and economically. Emerging technologies such as 4G/5G networks have significant potential on UAVs equipped with cameras, sensors, and GPS receivers in delivering Internet of Things (IoT) services from great heights, creating an airborne domain of the IoT. However, there are many issues to be resolved before the effective use of UAVs can be made, including security, privacy, and management. As such, in this paper we review new UAV application areas enabled by the IoT and 5G technologies, analyze the sensor requirements, and overview solutions for fleet management over aerial-networking, privacy, and security challenges. Finally, we propose a framework that supports and enables these technologies on UAVs. The introduced framework provisions a holistic IoT architecture that enables the protection of UAVs as "flying" things in a collaborative networked environment.

Keywords: security; privacy; drones; IoT; UAV

1. Introduction

The applications of unmanned aerial vehicles (UAVs) are diverse, including areas related to civilian, military, commercial, and governmental sectors [1–5]. Examples include environmental monitoring (e.g., pollution, health of plants, and industrial accidents) in the civilian sector. In military and governmental areas, we mainly have surveillance and delivery applications aiming to acquire or provide information at locations after a disaster or attack, and to distribute medicine or other essential items. Commercial applications are focused on delivering products and goods both in urban and rural areas. UAVs, since they are dependent on sensors, antennas, and embedded software, are considered as part of the Internet of Things, providing a two-way communication for applications related to remote control and monitoring [6].

The Internet of Things (IoT) constitutes a rapidly emerging cutting-edge environment in which the focal concept lies in the orchestration of a large variety of smart objects in such a way that they can be utilized and operated globally, either directly by users or by special software that captures their behavior and objectives. IoT enables objects to become active participants of everyday activities, with numerous promising applications through various communication technologies in the context of the "smart-city" vision [7]. It is estimated that around 25 billion uniquely identifiable objects are expected

to be part of this global community by 2020. These projections are expected to substantially increase with the introduction of 5G technologies and networks.

IoT objects are becoming more complex, heterogeneous, and highly distributed [8]. This transformation comes with a cost: the IoT, as a fusion of heterogeneous networks, not only involves the same security problems with sensor networks, mobile communication networks, and the Internet, but also brings along specific privacy-protection challenges. As part of heterogeneous networks, things have to support advanced security concepts, such as authentication, access control, data protection, confidentiality, cyber-attack prevention, and a high level of authorization [9]. These security and privacy challenges are different from traditional Internet security issues, since the IoT presents unique features in handling and dealing with external and internal threats. In this context, a regulatory framework is needed for setting and applying rules and policies in commercial objects. This framework should provide regulation rules and procedures that all commercial things should pass for receiving a security and privacy license in terms of connectivity and intelligence, actuation, and control features.

In light of the aforementioned remarks, this paper:

- Overviews new UAV application domains enabled by IoT and 5G technologies.
- Analyzes the IoT sensor requirements for drones.
- Summarizes the privacy and security challenges of UAV applications.
- Overviews solutions for fleet management over aerial networking.

Furthermore, to address IoT security and privacy challenges for drones, an advanced framework for end-to-end security and privacy prevention in real, market-based dynamic IoT environments is introduced. The proposed framework includes cutting-edge holistic approaches for advancing the current security and privacy level into a robust, resilient, and high-protected trusted environment. The framework supports multilevel and multidomain defence mechanisms in protecting IoT objects (i.e., UAVs) from spoofing, signal-jamming, and physical attacks, RF and mobile-application hacking, protocol abusing, and firmware hacks/sabotage. Privacy preservation is accomplished by effective 'crowd of things' strategies, where the anonymity of the users and the information that the UAV carries are ensured. Vision techniques are considered as aiming to enhance the security of IoT by supporting computer-vision and machine-learning solutions.

In summary, the main contribution of this work is, on the one hand, conducting a targeted review that focuses on security issues and promising solutions associated with the inclusion of UAVs in the IoT ecosystem, considering the special characteristics of such devices and the related cutting-edge technologies. On the other hand, a new framework that involves UAV-specific security extensions is presented for addressing the identified issues, along with ambitious real-world use cases.

The rest of this paper is organized as follows. In Section 2, we discuss aspects of using UAVs for wireless networks, review prior UAV–IoT frameworks, overview IoT Sensors for UAVs over 5G networks, discuss security and privacy issues for drones, and analyze protection mechanisms focusing on aerial networks and fleet-management systems. In Section 3, we describe the proposed framework focusing on protecting drones. Suggestions and evaluation requirements are presented in Section 4, and we finally conclude the paper in Section 5.

2. Overview on UAVs as Members of IoT

2.1. UAVs for Wireless Networks

2.1.1. Use Cases for Wireless Networking with UAVs

The use of UAVs as key entities of next-generation wireless networks constitutes one of the most promising applications of the corresponding technologies. A number of promising use cases are thoroughly detailed in Reference [10] and presented below.

- UAV-carried flying base stations that complete heterogeneous 5G systems to enhance the coverage and capacity of existing wireless access technologies.
- UAV-based aerial networks that allow reliable, flexible, and fast wireless connections in public-safety scenarios.
- UAVs that support terrestrial networks for disseminating information and enhancing connectivity.
- UAVs as flying antennas that can be deployed on demand to enable mmWave communications, massive MIMO, and 3D network MIMO.
- UAVs that are used to provide energy-efficient and reliable IoT uplink connections.
- UAVs that form the backhaul of terrestrial networks to allow agile, reliable, cost-effective, and high-speed connectivity.
- UAVs able to cache popular content and efficiently serve mobile users by following their mobility patterns.
- UAVs that act as users of the wireless infrastructure for surveillance, remote-sensing, and virtual-reality cases, and package-delivery applications.
- UAVs that collect vast amounts of city data and/or enhance cellular network coverage in a smart-city scenario.

2.1.2. UAV Types and Classifications

Different types of UAVs with distinctive characteristics, such as supported altitude, speed, and energy autonomy, are suitable for different applications. Generally, UAVs are classified according to their supported altitudes into Low-Altitude Platforms (LAP) and High-Altitude Platforms [11]. Furthermore, UAVs can be classified into rotary-wing and fixed-wing. The former are appropriate for cases that require UAVs that can remain at steady positions, whereas the latter are suitable for applications that demand UAVs travelling at high speeds and covering large distances [12]. In an IoT environment, due to the limited energy capacity of the participating devices, suitable LAP UAVs of the rotary-wing type can be efficiently and dynamically positioned to allow IoT devices to transmit with minimum power. A related framework towards this direction is introduced in Reference [13], while authors in Reference [14] introduce a resource-allocation scheme for improving energy consumption at cluster heads that use aerial base stations.

2.1.3. Interference Management, Deployment, Path Planning, and Energy Consumption of UAVs in IoT Networks

The use of UAVs as flying relays for IoT networks has numerous advantages, such as energy conservation and reliability; however, there are also some significant challenges that need to be addressed. Among those challenges, interference management, UAV deployment, and path planning are considered of major importance. The authors in Reference [15] propose and analyze an efficient deployment scheme for multiple UAVs using circle parking theory.

Regarding interference management, the findings revealed that UAVs' altitude needs to be adjusted according to the coverage requirements and the beamwidth of their directional antennas. A related work presented in Reference [16] concluded on the optimum placement of UAVs as relay nodes that the decode-and-forward approach outperforms the amplify-and-forward one. A new heuristic algorithm for 3D UAV deployment was introduced in Reference [17], which minimizes the number of required UAVs to keep a specific level of service quality. To mitigate interference, the authors suggest lowering the altitude, but there is an obvious tradeoff between this and coverage. Similarly, the authors in Reference [18] analyze the tradeoff between delay and coverage, as far as the number of UAV stop points is concerned.

As far as path planning is concerned, it is directly related with trajectory optimization. In general, finding the optimal flight path for a UAV is considered a challenging goal, since it is affected by multiple factors, such as energy limitations, flight time, and obstacle avoidance. Hence, as explained

in Reference [10], path planning is usually approached as an optimization problem with various objectives depending on the criterion of interest.

Energy consumption, in particular, constitutes a critical issue for the deployment and mobility of UAVs. Because of their limited battery capacity, UAVs are not typically able of providing for long continuous wireless coverage in scenarios such as IoT networking. Their energy autonomy is highly affected by the UAV role and flight path, weather conditions, etc., and actually constitutes the main constraint for UAV adoption in many cases. There are several recent research endeavors toward improving UAV energy efficiency, focusing on various aspects, such as trajectory optimization [19], co-operative communications [20], energy harvesting [21], and resource allocation [22], et al.

2.2. UAV–IoT Frameworks

Due to UAVs' high agility, they are now widely accepted as promising members of the IoT vision or even enablers of such a vision. They are capable of offering new value-added IoT services, while they can carry a variety of MTMC devices [23]. In more detail, according to the definition of IoT, "things" are expected to be able to be connected anywhere at any time providing any service. UAVs can fulfil this requirement, thanks to their autonomy, flexibility, and programmability. In this context, a number of UAV-enabled IoT frameworks supporting a variety of practical use cases have been proposed.

Authors in Reference [1] introduced and demonstrated a UAV-based IoT platform for crowd surveillance. The respective platform adopts and applies face recognition techniques and performs efficient offload of video processing to a Mobile Edge Computing (MEC) node, considering the limited processing power and energy capacity of a UAV. The developed testbed collects video-surveillance data and performs face recognition to identify suspicious individuals by utilizing the Local Binary Pattern Histogram (LBPH) algorithm of the Open Source Computer Vision (OpenCV) library. The proposed platform considers central management of a fleet of UAVs through a system orchestrator.

A communication framework for UAVs in urban IoT environments was proposed and evaluated in Reference [24]. It forms a multipath multihop infrastructure that is used to connect the UAVs to the ground control station. The conducted real-world experiments have shown that the introduced framework significantly enhances the control effectiveness and reliability against local congestion. It is noted that the specific work was inspired by the DARPA Hackfest on Software Defined Radios.

In Reference [25], a game-theory-based framework was introduced for allocating resources to UAVs, which enter the IoT ecosystems as platforms that assist terrestrial base stations. The access competition among the UAVs for bandwidth is modelled as a noncooperative evolutionary game. The evaluation of the two designed algorithms showed that Nash equilibrium can be quickly reached.

An optimization framework for aerial sensing in the context of an IoT infrastructure was designed and presented in Reference [26]. The goal is to allow remote users to navigate in specific scenes of interest by using augmented-reality (AR)/virtual-reality (VR) devices over the captured data. The corresponding scenario is likened to virtual human teleportation. The conducted experiments effectively demonstrated the advantages of the proposed methods on visual sensing.

Authors in Reference [27] conceived and presented a new MEC framework for IoT through an air–ground integration approach. Four use cases are presented to show how the proposed air–ground-integrated MEC framework supports high mobility, low latency, and high throughput for 5G applications. Through simulation-based and case-based evaluation, it was shown that the respective framework can support multiple IoT scenarios.

A novel framework for deploying and efficiently moving UAVs to gather information from ground IoT devices is proposed in Reference [28]. This work focuses on the optimal deployment and mobility of UAVs, as well as the optimal clustering of IoT devices, toward minimizing transmission power while retaining reliability. In this manner, it was shown that IoT devices' energy consumption can be significantly reduced, whereas UAVs can serve as ground devices for longer.

2.3. 5G and IoT Sensor Technologies for UAVs

The 5G technology is expected to enhance mobile broadband, enable applications that require ultrareliable very low latency and very high availability networks, improve traffic safety and control, support industrial applications, remote manufacturing, training, surgery, logistics, tracking, and fleet management. It will be utilized for smart agriculture, precision farming, smart buildings, smart meters, support of 4K/8K UHD broadcasting, virtual and augmented reality without range limitations, including homes, enterprises, and large venues offering massive and critical Machine-To-Machine-Type Communications (MTMC) [29]. This type of device communications can be integrated with typical Human-Type Communications (HTC) through suitable gateways in the context of a 5G architecture, as presented in Reference [30] and illustrated in Figure 1.

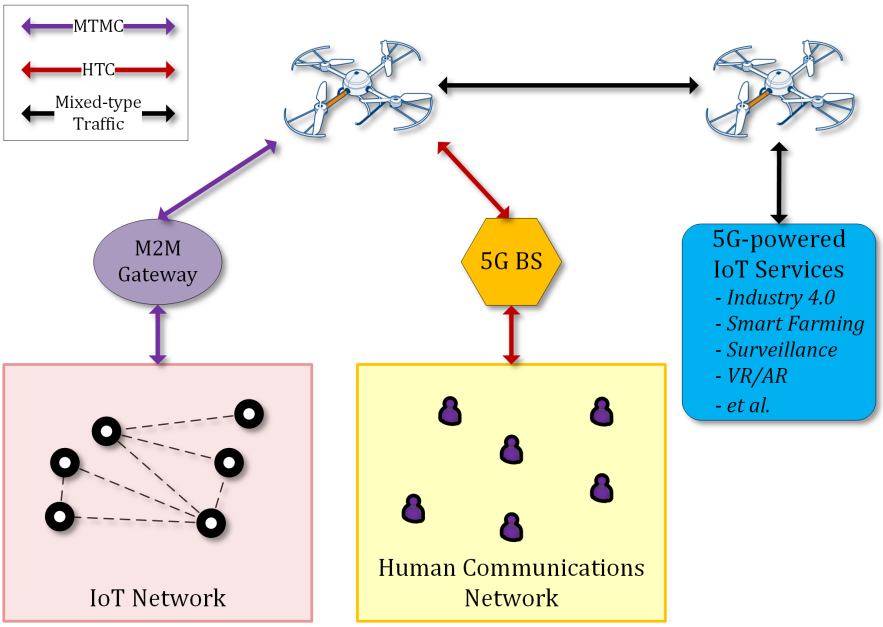

Figure 1. Unmanned aerial vehicle (UAV)-enhanced 5G-enabled Internet of Things (IoT) services.

Other 5G use cases that are linked to drones involve automation and robotics. Drones with the support of 5G networks would be able to offer a wide variety of tasks and applications providing new benefits to a wide range of industries. Among the top use cases of 5G-enabled drones, we consider applications related to construction, agriculture, insurance claims, police, fire, coast guard, border control, journalism, news, utilities, filmography, and logistics. All these applications will be feasible since autonomous and beyond line-of-sight control will be supported. In order to enable these use cases, specific minimum requirements for aerial vehicles are essential in terms of equipment and sensors.

The main types of sensor technologies that are supported and are a part of drones today can be separated into three main categories: (a) flight control, (b) data acquisition, and (c) communication sensors.

2.3.1. Flight Control Sensor for Internal State Evaluation

Accelerometers are used to determine position and orientation of the drone in flight. One type of technology senses the micromovement of embedded structures in an integrated circuit. Thermal sensing is another technology used in accelerometers, which does not include any moving parts but instead senses changes in the movement of gas molecules passing over a small integrated circuit [2]. Drones and UAVs manage to maintain flight paths and directions using inertial measurement units combined with GPS. The Inertial Measurement Units utilize multiaxis magnetometers (available in one to three axes). A magnetometer is basically a magnetic compass

that can measure the magnetic field of Earth. This mechanism helps in determining the direction of a compass and, consequently, of the drone, which is estimated with respect to the magnetic North. The flight-control system, in order to maintain level flight, obtains input from tilt sensors combined with accelerometers and gyroscopes. This is an essential element for UAVs, especially when the applications require high level of stability (e.g., surveillance, delivery, etc.). In certain drones we have Engine Intake Flow and current sensors [31]. These UAVs are powered with gas engines to effectively monitor the air flow and sensors to estimate the proper fuel-to-air ratio at a specified engine speed aiming to reduce emissions and the overall consumption. Current sensors are available in drones to monitor and optimize power consumption and detect faults with motors or other areas of the system.

2.3.2. Data-Acquisition Sensors

Drones are equipped with several sensors to capture information and data that are required to perform certain tasks. Depending on the application, the payload sensor suite can be arranged during the development of the drones.

- For military use cases, UAVs may be equipped with high-end electro-optical sensors, and radars for airborne systems providing resolutions from submillimeters to a few centimetres.
- In surveillance and monitoring applications, we can have sensors at the lower end of the spectrum, such as low- or high- (e.g., 4K) resolution RGB (Red Green Blue) cameras, NDVI (Normalized Difference Vegetation Index) cameras for precision farming, LIDAR (Light Imaging, Detection, And Ranging) for simultaneous localization and mapping, and ultrasonic sensors for sense and obstacle-avoidance methods.
- We can also have hyperspectral depth and thermal sensors [32]. Applications that monitor environmental and weather conditions and are deployed in disaster relief and management require sensors to measure or detect liquefied petroleum gas (LPG), butane, methane (CH4), hydrogen, smoke, oxygen, temperature, and humidity.

In all these applications, the IoT sensors collect data in real time and are either processed on board if enough power is available or transmitted to a base station.

2.3.3. Communication Systems

Managing and controlling tasks for UAVs are performed through communication systems and networks [33]. In the case of multiple drones, technologies are required to allow them to communicate with each other for safety reasons. There are different types of communications, and some of the main types used in UAVs are listed in Table 1. An extensive list of network protocols and communication techniques for generic IoT devices can be found in Reference [34]. Based on the coverage range, available data rates, and latency specifications, it is evident that 5G technology would impact drones' communications, enabling several worldwide applications. In such a conceptual model, UAVs can form infrastructureless dynamic network segments of the IoT architecture, which are interconnected to the core network for the provision of demanding services, such as surveillance multimedia streaming [35].

Table 1. Categories of communication technologies available to UAVs.

Category	Technology	Data Rate	Range	Latency
WPAN	Bluetooth 4.0	<1 Mbps	60 m	50
WPAN	Zigbee	<250 kbps	<100 m	50
WLAN	802.11a/b/g/n/ac	<600 Mbps	<250 m	75
WLAN	WAVE 802.11p	<27 Mbps	<1 km	50
LPWA	LoRA	<50 kbps	<15 km	82
LPWA	SigFox	<100 bps	<20 km	82
Cellular	NB-IoT	<250 kbps	World wide	75
Cellular	LTE-M	<1 Mbps	World wide	75
Cellular	LTE Advanced (4G)	<1 Gbps	World wide	50
Cellular	LTE D2D	-	World wide	25
Cellular	5G	<10 Gbps	World wide	3

2.4. Security for UAVs over IoT

Security provision in UAVs as part of the IoT environment is a complex task that requires the efficient integration of various techniques that are associated with different aspects of IoT networking and UAV operation. In the following two subsections, the security and privacy components for such an endeavor are discussed in detail. The main concept of the followed approach is the application of UAV-specific security extensions to various IoT technologies and security techniques, which can enable the required integration.

2.4.1. Security Component

IoT-based UAVs is a complex paradigm in which people and machines interact with the technological ecosystem based on smart objects through complex processes [36]. When studying security aspects in the IoT technological ecosystem, the study focused on four main layers that are, from top to bottom: the application, network, and link/adoption layers, and the perception. Figure 2 presents the IoT security techniques of each layer, along with UAV-oriented extensions (at the right side).

In the application layer, security mechanisms such as the Constrained Application Protocol (CoAP) [37], access control and user application security are included to enable secure messages and minimal configurations using the RESTful library, filtering and perimeter security with the Simple Object Access Protocol (SOAP) and data filtering and cloud support using application firewalls and Intrusion Detection Systems (IDS) [38]. The main UAV extensions in this layer are related with vision-based enhancements that support self-protection and path/destination identification by using video-processing and computer-vision techniques [39,40]. Novel solutions using deep learning and a combination of deep and shallow networks can be applied to enhance the security of mobile things.

In the network layer, mechanisms like IP Security (IPSec), secure routing, and transport security were suggested in Reference [36]. These mechanisms offer IP payload confidentiality and integrity using IPSec and the Encapsulated Security Payload (ESP) protocol. Trusted IoT drones and low-energy protocols can also be available with the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) according to the work in Reference [41]. The Datagram Transport Layer Security (DTLS) protocol, which is, in practice, TLS with added features to deal with the unreliable nature of User Datagram Protocol (UDP) communications, and Rivest Shamir Adelman (RSA) algorithms provide enhanced confidentiality, integrity, and authentication. These mechanisms, according to the work in Reference [42] can timely inform about potential threats (e.g., blackhole, wormhole, Sybil attack, and hello attack) in "flying" things while operating. Moreover, as UAV security extensions, novel routing and name service mechanisms can be developed based on the Named Data Networking (NDN) infrastructure, which is an evolution of the IP architecture that generalizes the role of this thin waist, such that packets can name objects other than communication endpoints [43]. NDN extensions can provide robust object identification and ensure the integrity of the things' records used in the naming architecture, in

order to defend against DNS, Man-in-the-Middle (MiM), and identification attacks using DNS Security Extensions (DNSSEC). Additionally, power-aware routing extensions can enhance drones' energy autonomy and increase flying time.

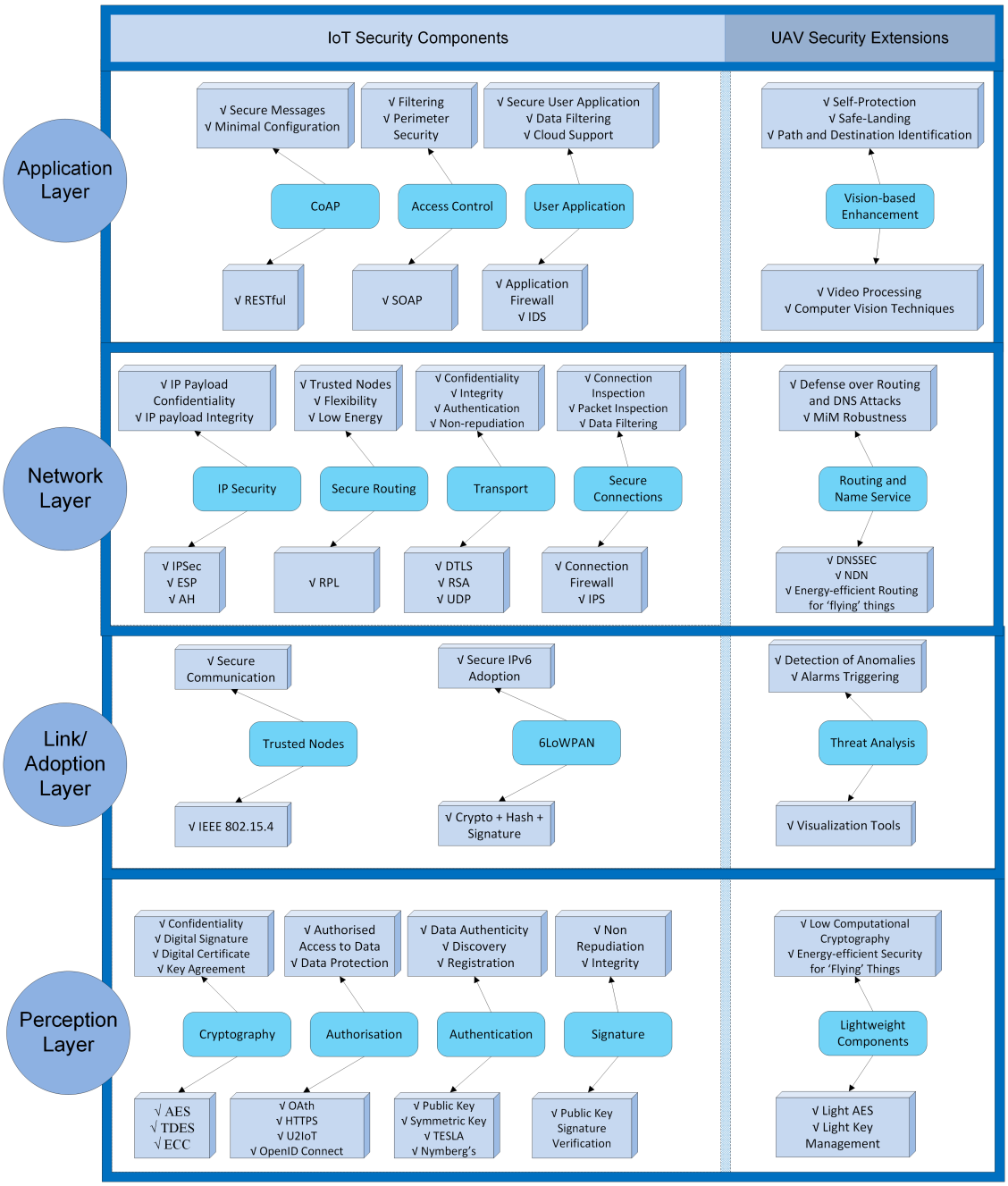

Figure 2. IoT security layers with UAV extensions.

In the link/adoption layer, important security services have to be applied in the 6LoWPAN adoption layer, including end-to-end security, continuous authentication schemes [44,45], trust verification/validation, and key management mechanisms [37]. To provide robust communication and endpoint security, secure and trusted channel protocols were proposed in Reference [46]. Furthermore, group key management techniques were considered in Reference [38], aiming to enable multicast communication using CoAP. To further strengthen the IoT drones, a trusted computing framework and execution architecture, were proposed in Reference [47]. Secure connections are enabled with connection firewalls and Intrusion Protection Systems (IPS) that can deeply inspect network

packets. In addition, firewalls, intrusion detection systems, and colocation proofs were suggested in Reference [48] that are necessary against routing attacks, such as selective forwarding, sinkhole, and wormhole attacks [44].

The primary security threats in the perception layer are physical damages, such as vandalism and weather challenges. Therefore, hardware mechanisms such as tamper-protection and -detection systems have to be employed, as was suggested in References [36,49]. In the perception layer, security is to ensure that only authorized users can have access to sensitive data that are produced by physical objects, and that's why authentication and authorization policies need to be defined. Authentication issues are addressed by combining light public and symmetric key mechanisms. According to Reference [50], RFC 6698 TLSA and Numberg's scheme are used to ensure data authenticity. The problem of authorization is addressed by combining open protocols such as Oath, HTTPS, U2IoT, and OpenID Connect [51]. In addition, lightweight cryptography and digital signature schemes are needed to ensure secure end-to-end communications. Light versions of existing algorithms such as the Advanced Encryption Standard (AES), the RSA, and Elliptic Curve Cryptography (ECC) can be customized to be applied on mobile things.

2.4.2. Privacy Component

Privacy protection in the IoT domain is divided into two main directions: (a) protection of collecting, acquiring, and distributing sensitive information such as faces, body silhouettes, objects, and license plates, by "flying" things such as drones; and (b) protection of observing and eliciting patterns, such as the number, duration, and diversity of connections, all of which can be used as signatures of IoT devices. The former direction is also referred as "user privacy", while the latter one is known as "thing privacy".

Privacy protection is a challenging goal in many research fields where measuring devices take place. For example, in Reference [52] a wide range of sensors measure various types of information; however, the concept fully protects the privacy of all registered users. To ensure anonymity, the group signature and data of all devices are communicated via TLS protocol with an authentication mechanism. The integrated group signature method appears to be efficient to protect the identity of the measuring devices. A group signature is used to encrypt all data in order to avoid the reception of dummy data by the reporting service. Similarly, in Reference [53], the proposed work provides identity confidentiality of both parties (the end user who requests data and the owner of the mobile device). In that manner, the end user cannot associate the mobile device and measured data.

Current solutions for "user privacy" in "flying" things are focused on filters aiming to remove sensitive information. Most of these systems are based on computer vision analyzing video content [54]. In the case of mobile things, such as drones, since they can get close to targets and capture the same scene from different points of view, they are able to gather sensitive personal data, adding a new dimension to issues related with privacy and protection solutions. Several state-of-the-art privacy filters were introduced, aiming also to keep a balance between privacy issues and surveillance effectiveness. Privacy filters include simple filters such as pixelization, masking blurring, as well as more advanced morphing [55] and reversible warping [56] filters. Recently, several researchers [57–60] proposed new features and approaches for drone-based surveillance that affect visual privacy. Regarding the acquired audiovisual data, a number of approaches have been proposed that employ encryption techniques [61–63]. However, such techniques cause the corruption of large parts of the original image, making the intelligibility task practically impossible. Other solutions use reversible scrambling applied in the compression-specific domain of a particular video format [64–66], improving the visual result, but heavily depending on the employed compression algorithm.

"Thing-privacy" breaches arise because it is still possible to observe patterns such as the number, duration, and diversity of connections, all of which can be used as the signatures of IoT devices. Existing schemes that preserve privacy in identity management are mostly centralized solutions [67].

Data provenance can provide data trackability, not just for data privacy but also for data-quality assurance and data-management transparency [68,69].

2.5. Protection for UAVs

One of the main challenges in the design of co-operative applications involving Multiple UAVs (Multi-UAVs) is the formulation of a network that can provide connectivity among the different types of employed vehicles, protecting at the same time the vehicles and the fleet mission from failures [70]. Therefore, it is very important to protect the life cycle of a fleet by (a) establishing and maintaining flexible aerial networks, and (b) by applying effective fleet-management techniques.

2.5.1. Aerial Networking

Multi-UAV networks should demonstrate highly dynamic behavior on complex operating scenarios baring all the constraints related to energy consumption and connectivity that may jeopardize the fleet mission. Research on aerial networks focuses on the definition of routing protocols that ensure quick communication recovery by employing flexible aerial nodes and energy-consumption management techniques that enable increased flight lifetime.

At the moment, configurations like Mobile Ad-hoc NETworks (MANETs) that are destined for mobile-device communications, Vehicle Ad-hoc NETworks (VANETs) that mainly consider land vehicles, and Flying Ad-hoc NETworks (FANETs) are adopted, each of them presenting certain advantages and disadvantages in context-specific deployments [71]. All of the above adopt ad hoc routing protocols that allow the exchange of data from one node to another without any direct links. There are three main types of routing protocols, namely, proactive, reactive, and geographic [70].

- Proactive protocols [72] incorporate tables for each node that are periodically updated to store routing information for all other nodes of the topology. The main advantage of proactive protocols is that the tables of each node contain up-to-date information on routes due to continuous message exchanges; a fact, though, that causes bandwidth constraints.
- Reactive protocols [73] search and store routing paths between two nodes only when the need for communication between them arises. These types of protocols present the advantage of consuming low bandwidth, but there are many cases, specifically in large topologies, where route-path calculation is very slow, causing high latency.
- Geographic protocols [74] assume that the source node is aware of the geographic position of the receiving node and therefore sends the message directly without the need for searching for a route path. This protocol is very effective in terms of latency, bandwidth, and throughput, though localization information should be available. Such information can be very challenging to obtain in GPS-denied environments; however, this is quite unlikely to occur in the case of FANETs, while signal-based tracking methods (such as the one introduced in Reference [75]) can be additionally adopted.

Energy conservation in UAV networks is also very important in protecting network continuity and increasing the carried payload. In terms of networking, saving energy in UAVs can be achieved [76] by (a) data reduction, (b) network coding, and (c) energy-efficient routing. Data reduction is possible by adopting aggregation schemes that perform data fusion, combining data derived from nodes on the same path. In this direction, adaptive data sampling is also an option for data-gathering tasks performed by UAVs by adjusting the sampling rate (images, videos, etc.) without compromising the required information precision. Network Coding (NC) is also used to reduce data traffic in broadcast scenarios by sending a linear combination of several packets instead of a copy of each packet.

On the other hand, energy conservation can also be enabled through the appropriate energy-routing mechanisms that take into consideration metrics relevant to power utilization and load distribution. Power utilization is related to the remaining battery of a node, while load distribution refers to the queue status of a node measured as the number of packets received and waiting to

be transmitted. To this end, there are three main energy-aware routing protocols: multipath-based protocols, node-based protocols, and cluster-based protocols [70]. Multipath-based protocols balance energy consumption among nodes by alternating forwarding nodes. These protocols discover multiple node-disjoint routes utilizing a cost function based on the hop distances and the energy levels of the nodes, and allocate the traffic rate to each selected route. Node-based protocols do not only consider the shortest paths, but select the next candidate hops based on their residual energy. Cluster-based protocols organize the network into clusters, where each cluster is managed by the cluster head (CH), which is responsible for co-ordination and aggregation operations. Sleep/wake-up protocols that save power by setting as many nodes in idle mode for as long as possible.

2.5.2. Fleet Management

Fleet management in autonomous moving objects is a challenging research field that focuses on defining the optimal formation configuration (positioning, speed, height) of a fleet of heterogeneous aerial objects, including decision making in the case of collisions or accretions [77]. Fleet-management techniques may offer various Levels of Automation (LOA) that can range from fully automated flights (no human involvement) to fully human-operated flights. Many works proposed automation architectures [78,79], but human operations are still usually required [80–82].

Fleet-management techniques can be classified into centralized and decentralized schemas [83].

- In the centralized schema, a formation manager that can be one of the aerial vehicles of the fleet or a ground-based station [82], acts as a supervisor for all aerial vehicles and manages their topology. Centralized schemas present the advantage that important decisions are performed at a higher level, by centralized high-power computer systems, where humans can also interfere. On the other hand, the major disadvantage of this schema is that it requires frequent ground communications, which can be energy consuming and, in case of disruptions/failures, ground management can cause delays [83].
- In the decentralized schema [4], each aerial vehicle has a certain freedom in decision making, while the whole formation must be capable of reconfiguring, making decisions, and achieving mission goals. This schema is energy-efficient and presents reduced reaction times, though it may produce conflicting decisions, jeopardizing the fleet formation and, in cases of critical formation updates, it may require ground-control assistance [83].

3. Proposed Framework and Methodology

3.1. Overall Concept and Methodology

The fundamental concept of the proposed framework to protect drones lies in the fact that mobile semiautonomous devices are expected to enter the IoT architecture as another type of smart devices and, due to their significant impact on several everyday activities (sensitive/critical or not), they require well-established and high-quality security support. On this ground, the proposed framework envisions to provide the necessary security components that would facilitate the process of interconnecting drones and UAVs under the umbrella of the IoT, while exhibiting advanced intelligence and self-management characteristics.

In more detail, considering the use of drones for different types of scenarios as representative application, the current state is actually characterized by separated, isolated, and custom approaches. As illustrated at the top of Figure 3, each operator currently uses their control center to communicate and control drone flight based on their own perceived processes. The adoption of security tools is, in fact, optional, their quality is questionable and not certified, as well as not compatible (in the general case) with security measures applied by other operators. The flight license (wherever required, based on local regulations) is also separate and difficult to verify compliance. Moreover, there are no fleet-management processes and no interdrone communications.

The introduced framework actively inserts drones in the IoT architecture by properly securing them both at device and network level.

- At device level, the proposed framework enhances drones with embedded lightweight security, privacy, and safety based on cutting-edge vision-based techniques, which also enable advanced scene/path identification.
- At network level, drones become part of the IoT architecture and they are accessed/controlled through it. Furthermore, agile communications among drones are enabled, providing self-organizing capabilities that set the basis for innovative features, namely, device registration, flight dynamic monitoring, trust establishment through a distributive reputation point system, enforcement and verification of flight-plan regulations, and extensive fleet management via advanced interoperability.

For achieving the aforementioned security and privacy goals, the proposed framework introduces: (a) a lightweight security toolbox, (b) vision-based solutions, and (c) privacy prevention and anonymity techniques for mobile things.

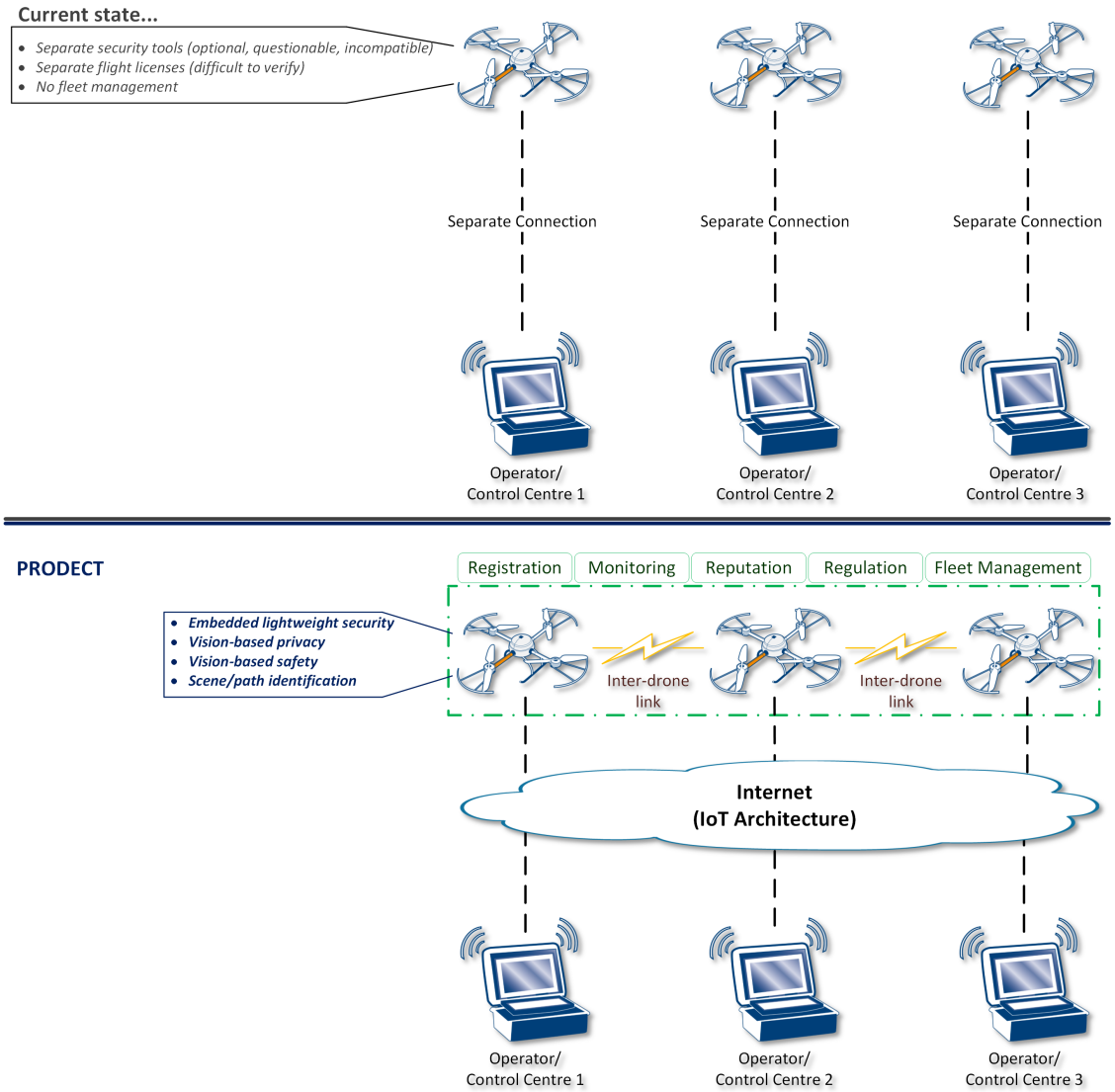

Figure 3. Proposed framework for "flying" things' secure connectivity in the IoT.

3.1.1. Lightweight Security Toolbox in "Flying" Things

In the context of the introduced framework, a novel lightweight security toolbox is proposed designed for "flying" things. The security toolbox supports open-source end-to-end security, authentication, and key management mechanisms in the adoption/network layer, firewalls and intrusion detection systems in both the adoption/network and application layers, and access control and selective disclosure in the application layer. The proposed security toolbox is lightweight and flexible since it is embedded in the drone's firmware as a part of the core software. Furthermore, the novel security framework incorporates physics and deep-learning mechanisms to allow the estimation of anomalies and security threats (e.g., hijacking).

3.1.2. Vision-Based Novel Solutions as Security Enhancement

Another issue addressed in the proposed framework is related to human's or drones' safety and self-protection. There are many scenarios (e.g., hackers take control of a drone, damaged and attached drones, etc.) in which drones may be a potential threat for humans or extra safety is required for the sensitive items they may carry. In order to overcome these issues, scene analysis and understanding using computer vision have been considered. Therefore, semantic segmentation is supported in this framework, aiming to offer complete forms of visual scene understanding, mainly for outdoor scenarios.

3.1.3. Privacy Prevention and Anonymity in "Flying" Things

In the introduced framework, we addressed both "user privacy" and "thing privacy" challenges in the "flying" things domain. To this end, user-privacy prevention is obtained by allowing mobile things to collect information that describe a user in detail, but preserving the privacy of the collected data. The "UAV privacy" concept is applied in mobile things supporting further anonymity techniques, such as k-anonymity, group signature, and crowd of things, customized for drone IoTs. A community of mobile things, configured as IP-based drones, are formed to apply anonymous authentication using Anonymous Access Credentials (AACs).

3.2. Proposed UAV IoT Architecture

As shown in Figure 4, the introduced architecture supports multiple solutions for security, safety, and privacy for mobile IoT toward the provision of services to different users through a set of distributed systems. In this way, end users can deploy and query their "flying" things, such as drones, in a secure and safe ecosystem respecting existing privacy regulations. In the proposed architecture, we have three main entities: the control center, the distributed systems, and the embedded solutions on the UAVs. The system is based on a drone-to-drone communication utilizing rooting algorithms, while communication with the control center takes place through the Internet. The Control Center (CC) is responsible for the management and orchestration of the proposed ecosystem. For that purpose, the CC shown in Figure 4 is responsible for end-to-end communication with the "things". It integrates all traditional IoT management elements and novel functional blocks to realize searching, information retrieval, and group instruction administration. Distributed Systems (DSs) are focused mainly on three areas: monitoring, management, and reputation. In more detail, the monitoring system is responsible for the registration processes and information authentication. In the case of the reputation system, we consider ranking functionalities for all drones, whereas the last component provides fleet-management solutions. The third entity represents all components integrated in the "flying" things.

In the proposed architecture, we focused mainly on the security and privacy components supported by vision-based systems. One component targets on security, protecting the drone from attackers aiming to hijack it and take control using network and wireless channel exploitation techniques. A second component is related to the privacy of the payload that incorporates advanced encryption and anonymity solutions. A third computer-vision component is included that provides

support and solutions both for security and privacy. This component introduces mechanisms for destination and path verification for security, as well as behavior analysis and scene understanding for privacy and safety, respectively. Finally, components for monitoring and drone-to-drone communication supporting registration and routing algorithms are part of the embedded system on the mobile IoT devices.

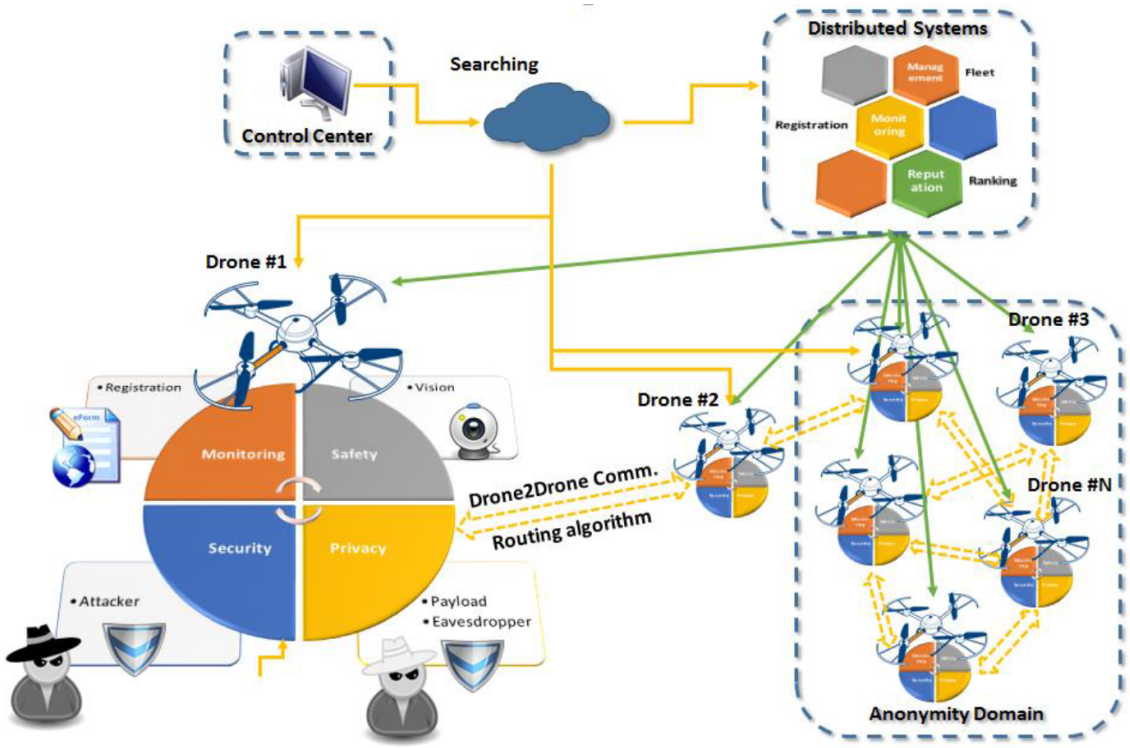

Figure 4. Proposed UAV IoT architecture.

3.3. Potential Security-Sensitive UAV IoT Applications

The deployment of the proposed UAV IoT framework/architecture for the protection of drones enables the realization of innovative security-sensitive applications. In this subsection, two such applications are presented and discussed.

3.3.1. Power-Line Monitoring

In this case, we exploit topics related to anonymity of IoT mobile devices, vision-based security using scene analysis, secure communications, and safe landing locations. The proposed scenario involves power-line monitoring and inspection, mainly over rural areas, as illustrated in Figure 5. Power-line monitoring is essential for all high- and medium-power operators/distributors. Today, most inspections are carried out with aerial methods with the use of helicopters, while sometimes terrestrial methods are used as well (e.g., ground patrols). Both methods are expensive and time consuming without guaranteeing successful results. Operators spend a lot of time and money to repair damages that were not detected during inspections. According to the proposed application, unmanned multicopters would be equipped with a set of visual, infrared, and localization sensors. All data would be acquired simultaneously, and a flight path would be scheduled based on power-pylon positions. This includes X, Y, and Z co-ordinates that would be used as a reference for the calculation of mission waypoints. A flight route would be designed in a way that multicopter flies several meters above the power pylons, several meters beside them in one direction, and then back to the other side of the power line. This would allow for capturing oblique inspection images of both sides of the power infrastructure, as well as point clouds and nadir images with a large side overlap, resulting in doubled density of point

clouds and images suitable for accurate orthophoto building and stereoscopic analyses. After landing, all acquired data and flight logs would be downloaded. They would be analyzed for quality and completeness. The following flights would be planned retaining a buffer in order to allow overlapping with the previous mission to assure continuity of data along the power lines.

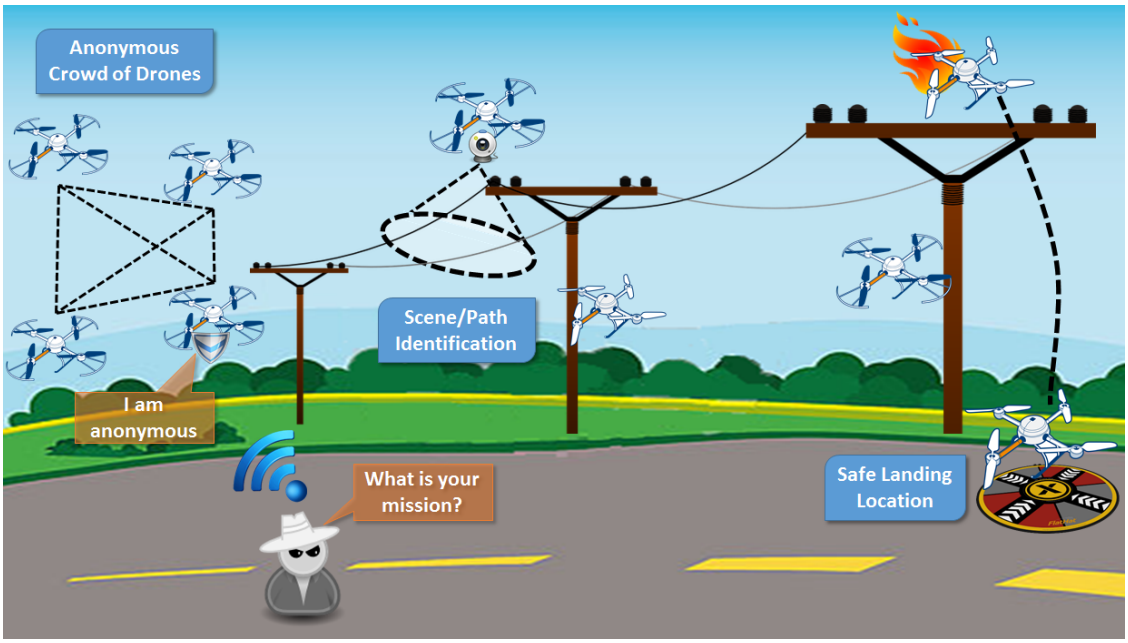

Figure 5. Power-line monitoring application.

3.3.2. Human Blood Delivery

In this case, we exploit topics related to payload privacy and monitoring, advanced security topics, thing anonymity, and embedded security tools. The proposed scenario involves hospitals and medical vans delivering human blood between them, which is an extremely vulnerable and high-demand task, as depicted in Figure 6. Delivering human blood is an assignment of high demand and risk. There are also certain requirements and restrictions imposed regarding temperature, time, and exposure. The payload in this case contains further sensitive and private information that may be vulnerable to external threats and attacks. This delivery scenario would provide solutions for many security and privacy issues, mainly related to the payload, considering approaches to provide a secure and robust routing protocol. It involves precise flights over urban areas following preselected and precalculated paths, payload protocols for security and privacy, and safe landing and dropping of the blood in a specified location (from medical vans to hospitals or vice versa). The multicopters, which would be equipped with a high-resolution camera, localization sensors, and cargo container, would fly to the predefined destination using a direct root, minimizing the required time. Regarding the container, it would ensure all required conditions for the human blood (e.g., temperature, exposure, etc.). All recorded data would be filtered based on privacy regulations and the proposed solutions would be integrated. Furthermore, computer vision and machine learning would help to identify safe landing locations, minimizing the risk of hijacking.

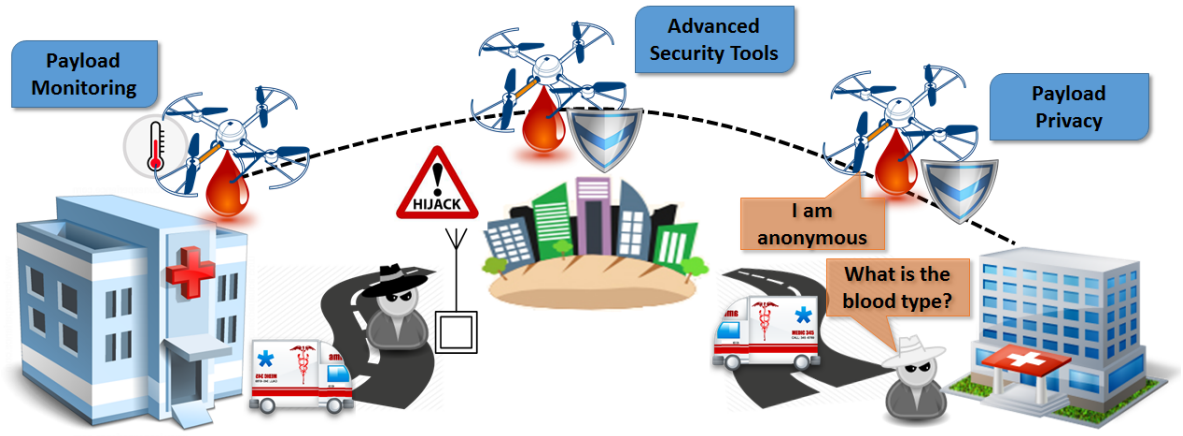

Figure 6. Human blood delivery application.

4. Requirements, Suggestions, and Evaluation

In this section, we present the necessary prerequisites for the successful deployment of the proposed framework, we discuss possible enhancements, and close with future evaluation plans.

The effective use of the provisioned architecture requires the deployment of a Universal UAV CC (UUCC) that would act as a single point of access for identifying mobile flying objects while they are operating in real environments. The existence of a UUCC would be the first step to establish a well-defined global process for registering and identifying all UAV flights. Additionally, the proposed framework provisions interdrone communication, a fact that requires certain mechanisms to control autonomous flights' interoperability and co-operation. Interoperability mechanisms set the grounds for defining the types of communications between drones (exchange of data, fleet formulation). For example, the exchange of data between two independent UAVs operating at the same time in two neighbor areas would help in maximizing the area covered, while achieving energy conservation.

The proposed framework, presented in Section 3, supports the management and control of UAV and multi-UAV systems, while preserving the security and privacy of the different stakeholders participating in mobile IoT missions without being differentiated across different application domains. Enhancement of the proposed framework would include variations of the suggested security and privacy mechanisms based on the context of the UAV application and the hardware/mechanical characteristics of the participating UAVs. A classification of the UAVs based on their hardware attributes and their application domain would be particularly useful in filtering security and privacy measures, both at device and network level, ensuring the smooth operation of the mission without overloading the UAV device and the aerial network with procedures that, in some cases, could be out of scope.

The suggested framework, along with the corresponding architecture, is formulated but not yet validated. Therefore, the next logical step would be to build a simulation model as proof of concept of the proposed UAV secure-connectivity framework. Metrics related to security, privacy, and connectivity would be employed in order to evaluate framework and communication effectiveness. Based on the findings, the involved security and privacy techniques would be tuned to adjust to the needs of real-world applications.

5. Conclusions

In this survey, the applications of UAVs were reviewed presenting IoT sensors that are essential for the related scenarios and use cases. Considering the drones as IoT devices and the support from emerging technologies such as 5G networks, we analyzed the sensor requirements for the corresponding applications and overview solutions for fleet management over aerial networking. The issues related to privacy and security were presented, focusing on users' and drones' privacy. Finally, we proposed a framework that supports and enables these technologies on UAVs, providing advanced

security and privacy by incorporating novel vision-based solutions for scene analysis. According to the proposed framework, a hybrid centralized–distributed framework controls UAV flights, handling operations like the registration, identification, ranking, and management of moving objects. As future work, we plan to evaluate the proposed framework, both within laboratory settings and in real-world scenarios, in order to adjust it for context-specific application domains.

Author Contributions: The presented work was carried out with the collaboration of all authors, who have equally contributed.

Funding: This research was co-funded by the European Union and Greek national funds through the Operational Program Competitiveness, Entrepreneurship, and Innovation, grant number T1EDK-04759

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Motlagh, N.H.; Bagaa, M.; Taleb, T. UAV-based IoT platform: A crowd surveillance use case. *IEEE Commun. Mag.* **2017**, *55*, 128–134.
2. Kersnovski, T.; Gonzalez, F.; Morton, K. A UAV system for autonomous target detection and gas sensing. In Proceedings of the Aerospace Conference, Big Sky, MT, USA, 4–11 March 2017; pp. 1–12.
3. Kumbhar, A.; Guvenc, I.; Singh, S.; Tuncer, A. Exploiting LTE-Advanced HetNets and FeICIC for UAV-assisted public safety communications. *IEEE Access* **2018**, *6*, 783–796.
4. Bupe, P.; Haddad, R.; Rios-Gutierrez, F. Relief and emergency communication network based on an autonomous decentralized UAV clustering network. In Proceedings of the SoutheastCon, Fort Lauderdale, FL, USA, 9–12 April 2015; pp. 1–8.
5. Merwaday, A.; Guvenc, I. UAV assisted heterogeneous networks for public safety communications. In Proceedings of the Wireless Communications and Networking Conference Workshops (WCNCW), New Orleans, LA, USA, 9–12 March 2015; pp. 329–334.
6. Luo, C.; Nightingale, J.; Asemota, E.; Grecos, C. A UAV-cloud system for disaster sensing applications. In Proceedings of the 2015 IEEE 81st Vehicular Technology Conference (VTC Spring), Glasgow, 2015, pp. 1–5.
7. Zanella, A.; Bui, N.; Castellani, A.; Vangelista, L.; Zorzi, M. Internet of Things for Smart Cities. *IEEE Internet Things J.* **2014**, *1*, 22–32. doi:10.1109/JIOT.2014.2306328.
8. Eleftherakis, G.; Pappas, D.; Lagkas, T.; Rousis, K.; Paunovski, O. Architecting the IoT paradigm: A middleware for autonomous distributed sensor networks. *Int. J. Distr. Sens. Netw.* **2015**, *11*, 139735.
9. Solomitckii, D.; Gapeyenko, M.; Semkin, V.; Andreev, S.; Koucheryavy, Y. Technologies for efficient amateur drone detection in 5G millimeter-wave cellular infrastructure. *IEEE Commun. Mag.* **2018**, *56*, 43–50.
10. Mozaffari, M.; Saad, W.; Bennis, M.; Nam, Y.H.; Debbah, M. A Tutorial on UAVs for Wireless Networks: Applications, Challenges, and Open Problems. *arXiv* **2018**, arXiv: 1803.00680.
11. Al-Hourani, A.; Kandeepan, S.; Jamalipour, A. Modeling air-to-ground path loss for low altitude platforms in urban environments. In Proceedings of the 2014 IEEE Global Communications Conference, Austin, TX, USA, 8–12 December 2014; pp. 2898–2904. doi:10.1109/GLOCOM.2014.7037248.
12. Zeng, Y.; Zhang, R.; Lim, T.J. Wireless communications with unmanned aerial vehicles: Opportunities and challenges. *IEEE Commun. Mag.* **2016**, *54*, 36–42. doi:10.1109/MCOM.2016.7470933.
13. Mozaffari, M.; Saad, W.; Bennis, M.; Debbah, M. Mobile Unmanned Aerial Vehicles (UAVs) for Energy-Efficient Internet of Things Communications. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 7574–7589. doi:10.1109/TWC.2017.2751045.
14. Soorki, M.N.; Mozaffari, M.; Saad, W.; Manshaei, M.H.; Saidi, H. Resource Allocation for Machine-to-Machine Communications with Unmanned Aerial Vehicles. In Proceedings of the 2016 IEEE Globecom Workshops (GC Wkshps), Washington, DC, USA, 4–8 December 2016; pp. 1–6. doi:10.1109/GLOCOMW.2016.7849026.
15. Mozaffari, M.; Saad, W.; Bennis, M.; Debbah, M. Efficient Deployment of Multiple Unmanned Aerial Vehicles for Optimal Wireless Coverage. *IEEE Commun. Lett.* **2016**, *20*, 1647–1650. doi:10.1109/LCOMM.2016.2578312.
16. Chen, Y.; Feng, W.; Zheng, G. Optimum Placement of UAV as Relays. *IEEE Commun. Lett.* **2018**, *22*, 248–251. doi:10.1109/LCOMM.2017.2776215.

17. Kalantari, E.; Yanikomeroglu, H.; Yongacoglu, A. On the Number and 3D Placement of Drone Base Stations in Wireless Cellular Networks. In Proceedings of the 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall), Montreal, QC, Canada, 18–21 September 2016; pp. 1–6. doi:10.1109/VTCFall.2016.7881122.
18. Mozaffari, M.; Saad, W.; Bennis, M.; Debbah, M. Unmanned Aerial Vehicle With Underlaid Device-to-Device Communications: Performance and Tradeoffs. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 3949–3963. doi:10.1109/TWC.2016.2531652.
19. Zeng, Y.; Zhang, R. Energy-Efficient UAV Communication With Trajectory Optimization. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 3747–3760. doi:10.1109/TWC.2017.2688328.
20. Tran, T.X.; Hajisami, A.; Pompili, D. Cooperative Hierarchical Caching in 5G Cloud Radio Access Networks. *IEEE Netw.* **2017**, *31*, 35–41. doi:10.1109/MNET.2017.1600307.
21. Anton, S.R.; Inman, D.J. Performance modeling of unmanned aerial vehicles with on-board energy harvesting. In *Active and Passive Smart Structures and Integrated Systems*; International Society for Optics and Photonics: Bellingham, WA, USA, 2011; Volume 7977, p. 79771H. doi:10.1117/12.880473.
22. Ceran, E.T.; Erkilic, T.; Uysal-Biyikoglu, E.; Girici, T.; Leblebicioglu, K. Optimal energy allocation policies for a high altitude flying wireless access point. *Trans. Emerg. Telecommun. Technol.* **2017**, *28*, e3034. doi:10.1002/ett.3034.
23. Motlagh, N.H.; Taleb, T.; Arouk, O. Low-Altitude Unmanned Aerial Vehicles-Based Internet of Things Services: Comprehensive Survey and Future Perspectives. *IEEE Internet Things J.* **2016**, *3*, 899–922. doi:10.1109/JIOT.2016.2612119.
24. Shaikh, Z.; Baidya, S.; Levorato, M. Robust Multi-Path Communications for UAVs in the Urban IoT. In Proceedings of the 2018 IEEE International Conference on Sensing, Communication and Networking (SECON Workshops), Hong Kong , China, 11–13 June 2018; pp. 1–5. doi:10.1109/SECONW.2018.8396356.
25. Yan, S.; Peng, M.; Cao, X. A Game Theory Approach for Joint Access Selection and Resource Allocation in UAV Assisted IoT Communication Networks. *IEEE Internet Things J.* **2018**. doi:10.1109/JIOT.2018.2873308.
26. Chakareski, J. Aerial UAV-IoT sensing for ubiquitous immersive communication and virtual human teleportation. In Proceedings of the 2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Atlanta, GA, USA, 1–4 May 2017; pp. 718–723. doi:10.1109/INFCOMW.2017.8116465.
27. Zhou, Z.; Feng, J.; Tan, L.; He, Y.; Gong, J. An Air-Ground Integration Approach for Mobile Edge Computing in IoT. *IEEE Commun. Mag.* **2018**, *56*, 40–47. doi:10.1109/MCOM.2018.1701111.
28. Mozaffari, M.; Saad, W.; Bennis, M.; Debbah, M. Mobile Internet of Things: Can UAVs Provide an Energy-Efficient Mobile Architecture? In Proceedings of the 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, USA, 4–8 December 2016; pp. 1–6. doi:10.1109/GLOCOM.2016.7841993.
29. Wang, D.; Bai, L.; Zhang, X.; Guan, W.; Chen, C. Collaborative relay beamforming strategies for multiple destinations with guaranteed QoS in wireless machine-to-machine networks. *Int. J. Distr. Sens. Netw.* **2012**, *8*, 525640.
30. Sarigiannidis, P.; Lagkas, T.; Bibi, S.; Ampatzoglou, A.; Bellavista, P. Hybrid 5G optical-wireless SDN-based networks, challenges and open issues. *IET Netw.* **2017**, *6*, 141–148.
31. Klepac, L.; Rozehnal, D. Scavenging simulation of small two-stroke engine with low-pressure fuel injection for usage in unmanned aerial vehicle (UAV). In Proceedings of the 2017 International Conference on Military Technologies (ICMT), Brno, Czech Republic, 31 May–2 June 2017; pp. 457–461.
32. Honkavaara, E.; Eskelinen, M.A.; Plnen, I.; Saari, H.; Ojanen, H.; Mannila, R.; Holmlund, C.; Hakala, T.; Litkey, P.; Rosnell, T. Remote sensing of 3-D geometry and surface moisture of a peat production area using hyperspectral frame cameras in visible to short-wave infrared spectral ranges onboard a small unmanned airborne vehicle (UAV). *IEEE Trans. Geosci. Remote Sens.* **2016**, *54*, 5440–5454.
33. Zhang, C.; Zhang, W. Spectrum sharing for drone networks. *IEEE J. Sel. Areas Commun.* **2017**, *35*, 136–144.
34. Triantafyllou, A.; Sarigiannidis, P.; Lagkas, T.D. Network Protocols, Schemes, and Mechanisms for Internet of Things (IoT): Features, Open Challenges, and Trends. *Wirel. Commun. Mobile Comput.* **2018**, *2018*. doi:10.1155/2018/5349894.
35. Bellavista, P.; Giannelli, C.; Lagkas, T.; Sarigiannidis, P. Quality Management of Surveillance Multimedia Streams Via Federated SDN Controllers in Fiwi-Iot Integrated Deployment Environments. *IEEE Access* **2018**, *6*, 21324–21341.
36. Altawy, R.; Youssef, A.M. Security, privacy, and safety aspects of civilian drones: A survey. *ACM Trans. Cyber-Phys. Syst.* **2017**, *1*, 7. doi:10.1145/3001836.

37. Granjal, J.; Monteiro, E.; Silva, J.S. Security for the internet of things: a survey of existing protocols and open research issues. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1294–1312.
38. Wallgren, L.; Raza, S.; Voigt, T. Routing Attacks and Countermeasures in the RPL-based Internet of Things. *Int. J. Distr. Sens. Netw.* **2013**, *9*, 794326.
39. Bloom, V.; Makris, D.; Argyriou, V. Clustered spatio-temporal manifolds for online action recognition. In Proceedings of the 2014 22nd International Conference on Pattern Recognition (ICPR), Stockholm, Sweden, 24–28 August 2014; pp. 3963–3968.
40. Bloom, V.; Argyriou, V.; Makris, D. Hierarchical transfer learning for online recognition of compound actions. *Comput. Vis. Image Underst.* **2016**, *144*, 62–72.
41. Winter, T.; Thubert, P.; Brandt, A.; Hui, J.; Kelsey, R.; Levis, P.; Pister, K.; Struik, R.; Vasseur, J.P.; Alexander, R. *RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks*; Technical report; Internet Engineering Task Force (IETF): Fremont, CA, USA, 2012.
42. Tsitsiroudi, N.; Sarigiannidis, P.; Karapistoli, E.; Economides, A.A. EyeSim: A mobile application for visual-assisted wormhole attack detection in IoT-enabled WSNs. In Proceedings of the 2016 9th IFIP Wireless and Mobile Networking Conference (WMNC), Colmar, France, 11–13 July 2016; pp. 103–109.
43. Zhang, L.; Afanasyev, A.; Burke, J.; Jacobson, V.; Crowley, P.; Papadopoulos, C.; Wang, L.; Zhang, B. Named data networking. *ACM SIGCOMM Comput. Commun. Rev.* **2014**, *44*, 66–73.
44. Leloglu, E. A review of security concerns in Internet of Things. *J. Comput. Commun.* **2016**, *5*, 121.
45. Shepherd, C.; Akram, R.N.; Markantonakis, K. Towards Trusted Execution of Multi-modal Continuous Authentication Schemes. In *Proceedings of the Symposium on Applied Computing*; ACM: New York, NY, USA, 2017; pp. 1444–1451. doi:10.1145/3019612.3019652.
46. Akram, R.N.; Markantonakis, K.; Mayes, K.; Bonnefoi, P.F.; Sauveron, D.; Chaumette, S. An efficient, secure and trusted channel protocol for avionics wireless networks. In Proceedings of the 2016 IEEE/AIAA 35th Digital Avionics Systems Conference (DASC), Sacramento, CA, USA, 25–30 September 2016; pp. 1–10.
47. Markantonakis, K.; Akram, R.N.; Holloway, R. A secure and trusted boot process for avionics wireless networks. In Proceedings of the Integrated Communications Navigation and Surveillance (ICNS), Herndon, VA, USA, 19–21 April 2016; pp. 1C3–1.
48. Gurulian, I.; Akram, R.N.; Markantonakis, K.; Mayes, K. Preventing relay attacks in mobile transactions using infrared light. In Proceedings of the Symposium on Applied Computing, Marrakech, Morocco, 3–7 April 2017; pp. 1724–1731.
49. Akram, R.N.; Bonnefoi, P.F.; Chaumette, S.; Markantonakis, K.; Sauveron, D. Secure Autonomous UAVs Fleets by Using New Specific Embedded Secure Elements. In Proceedings of the Trustcom/BigDataSE/ISPA, Tianjin, China, 23–26 August 2016; pp. 606–614.
50. Yao, X.; Han, X.; Du, X.; Zhou, X. A lightweight multicast authentication mechanism for small scale IoT applications. *IEEE Sens. J.* **2013**, *13*, 3693–3701.
51. Ning, H.; Liu, H.; Yang, L. Cyber-entity security in the Internet of things. *Computer* **2013**, *46*, 46–53. doi:10.1109/MC.2013.74.
52. Trojak, D.; Komosny, D. System for Anonymous Data Collection Based on Group Signature Scheme. *Acta Univ. Agric. Silvicult. Mendel. Brun.* **2016**, *64*, 1785–1795.
53. De Cristofaro, E.; Soriente, C. Short paper: PEPSI-privacy-enhanced participatory sensing infrastructure. In Proceedings of the Fourth ACM Conference on Wireless Network Security, Hamburg, Germany, 14—17 June 2011; pp. 23–28.
54. Senior, A.; Pankanti, S.; Hampapur, A.; Brown, L.; Tian, Y.L.; Ekin, A.; Connell, J.; Shu, C.F.; Lu, M. Enabling video privacy through computer vision. *IEEE Secur. Privacy* **2005**, *3*, 50–57.
55. Korshunov, P.; Ebrahimi, T. Using face morphing to protect privacy. In Proceedings of the 2013 10th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Krakow, Poland, 27–30 August 2013; pp. 208–213.
56. Korshunov, P.; Ebrahimi, T. Using warping for privacy protection in video surveillance. In Proceedings of the 2013 18th International Conference on Digital Signal Processing (DSP), Fira, Greece, 1–3 July 2013; pp. 1–6.
57. Villasenor, J. Observations from above: unmanned aircraft systems and privacy. *Harv. JL Pub. Pol'y* **2013**, *36*, 457.

58. Finn, R.L.; Wright, D. Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications. *Comput. Law Secur. Rev.* **2012**, *28*, 184–194.
59. Clarke, R. The regulation of civilian drones' impacts on behavioural privacy. *Comput. Law Secur. Rev.* **2014**, *30*, 286–305.
60. Wilson, R.L. Ethical issues with use of drone aircraft. In Proceedings of the IEEE 2014 International Symposium on Ethics in Engineering, Science, and Technology, Chicago, IL, USA, 23–24 May 2014; p. 56.
61. Boult, T.E. PICO: Privacy through invertible cryptographic obscuration. In Proceedings of the Computer Vision for Interactive and Intelligent Environment, Lexington, KY, USA, 17–18 November 2005; pp. 27–38.
62. Carrillo, P.; Kalva, H.; Magliveras, S. Compression independent reversible encryption for privacy in video surveillance. *EURASIP J. Inf. Secur.* **2009**, *2009*, 5. doi:10.1155/2009/429581.
63. Rahman, S.M.M.; Hossain, M.A.; Mouftah, H.; El Saddik, A.; Okamoto, E. Chaos-cryptography based privacy preservation technique for video surveillance. *Multimed. Syst.* **2012**, *18*, 145–155.
64. Dufaux, F.; Ebrahimi, T. Video surveillance using JPEG 2000. In *Applications of Digital Image Processing XXVII*; International Society for Optics and Photonics: Bellingham, WA, USA, 2004; Volume 5558, pp. 268–276.
65. Martinez-Ponte, I.; Desurmont, X.; Meessen, J.; Delaigle, J.F. Robust human face hiding ensuring privacy. In Proceedings of the International Workshop on Image Analysis for Multimedia Interactive Services, Montreux, Switzerland, 13–15 April 2005; Volume 4.
66. Dufaux, F.; Ebrahimi, T. Scrambling for privacy protection in video surveillance systems. *IEEE Trans. Circ. Syst. Video Technol.* **2008**, *18*, 1168–1174.
67. Alcaide, A.; Palomar, E.; Montero-Castillo, J.; Ribagorda, A. Anonymous authentication for privacy-preserving IoT target-driven applications. *Comput. Secur.* **2013**, *37*, 111–123.
68. Akram, R.N.; Ko, R.K. Unified model for data security-A position paper. In Proceedings of the 014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Beijing, China, 24–26 September 2014; pp. 831–839.
69. Suen, C.H.; Ko, R.K.; Tan, Y.S.; Jagadpramana, P.; Lee, B.S. S2logger: End-to-end data tracking mechanism for cloud data provenance. In Proceedings of the 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Melbourne, VIC, Australia, 16–18 July 2013; pp. 594–602.
70. Gupta, L.; Jain, R.; Vaszkun, G. Survey of important issues in UAV communication networks. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 1123–1152.
71. Bekmezci, I.; Sahingoz, O.K.; Temel, A. Flying ad-hoc networks (FANETs): A survey. *Ad Hoc Netw.* **2013**, *11*, 1254–1270.
72. Cheng, B.N.; Moore, S. A comparison of MANET routing protocols on airborne tactical networks. In Proceedings of the MILCOM 2012 - 2012 IEEE Military Communications Conference, Orlando, FL, USA, 29 October—1 November 2012; pp. 1–6.
73. Shirani, R.; St-Hilaire, M.; Kunz, T.; Zhou, Y.; Li, J.; Lamont, L. Combined reactive-geographic routing for unmanned aeronautical ad-hoc networks. In Proceedings of the 2012 8th International Wireless Communications and Mobile Computing Conference (IWCMC), Limassol, Cyprus, 27–31 August 2012; pp. 820–826.
74. Yu, Q.; Zhang, B.; Liu, C.; Mouftah, H.T. Energy-Efficient Geographical Forwarding Algorithm for Wireless Ad Hoc and Sensor Networks. In Proceedings of the Wireless Communications and Networking Conference, Las Vegas, NV, USA, 31 March–3 April 2008; pp. 2468–2473.
75. Lagias, A.E.; Lagkas, T.D.; Zhang, J. New RSSI-Based Tracking for Following Mobile Targets Using the Law of Cosines. *IEEE Wirel. Commun. Lett.* **2018**, *7*, 392–395.
76. Rault, T.; Bouabdallah, A.; Challal, Y. Energy efficiency in wireless sensor networks: A top-down survey. *Comput. Netw.* **2014**, *67*, 104–122.
77. Maza, I.; Ollero, A. Multiple UAV cooperative searching operation using polygon area decomposition and efficient coverage algorithms. In *Distributed Autonomous Robotic Systems 6*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 221–230.
78. Dixon, S.R.; Wickens, C.D.; Chang, D. Mission control of multiple unmanned aerial vehicles: A workload analysis. *Hum. Fact.* **2005**, *47*, 479–487.
79. Ruff, H.A.; Calhoun, G.L.; Draper, M.H.; Fontejon, J.V.; Guilfoos, B.J. *Exploring Automation Issues in Supervisory Control of Multiple UAVs*; Technical report; Sytronics Inc.: Dayton, OH, USA, 2004.

80. Cummings, M.L.; Bruni, S.; Mercier, S.; Mitchell, P.J. *Automation Architecture for Single Operator, Multiple UAV Command and Control*; Technical report; Massachusetts Inst Of Tech Cambridge: Cambridge, MA, USA, 2007.
81. Arslan, O.; Inalhan, G. Design of a decision support architecture for human operators in UAV fleet C2 applications. In Proceedings of the 14th International Command and Control Research and Technology Symposium (ICCRTS), Washington, DC, USA, 15–17 June 2009.
82. Lee, J.; Kim, K.; Yoo, S.; Chung, A.Y.; Lee, J.Y.; Park, S.J.; Kim, H. Constructing a reliable and fast recoverable network for drones. In Proceedings of the 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 22–27 May 2016; pp. 1–6.
83. Giulietti, F.; Pollini, L.; Innocenti, M. Autonomous formation flight. *IEEE Control Syst.* **2000**, *20*, 34–44.