UAV Integration Into IoIT: Opportunities and Challenges

Mariana Rodrigues*, Daniel F. Pigatto†, João V. C. Fontes*,
Alex S. R. Pinto ‡, Jean-Philippe Diguet § and Kalinka. R. L. J. C. Branco*

*University of Sao Paulo (USP)
São Carlos, São Paulo, Brazil
e-mail: rodrigues.mariana@usp.br, joao.fontes@usp.br, kalinka@icmc.usp.br

†Federal University of Technology Parana (UTFPR)
Curitiba, Paran, Brazil
e-mail: pigatto@utfpr.edu.br

‡Federal University of Santa Catarina (UFSC)
Blumenau, Santa Catarina, Brazil
e-mail: a.r.pinto@ufsc.br

§Lab-STICC, UBS Research Center
Lorient, France
e-mail:jean-philippe.diguet@univ-ubs.fr

Abstract—**Unmanned Aerial Vehicles (UAVs) have been applied in many fields such as military, traffic management, natural disaster prevention and assistance, and agriculture. Due to their characteristics, they are natural candidates to integrate the Internet of Intelligent Things (IoIT), a network composed of devices that are autonomous and mobile and have both sensing and action taking capabilities. The insertion of UAVs into IoIT infrastructure brings new dimensions to UAV applications and at the same time introduces new challenges. In this paper, we outline some opportunities and challenges brought by the insertion of UAVs into IoIT.**

Keywords–Unmanned Aerial Vehicles; UAV; Unmanned Aircraft Systems; UAS; Internet of Intelligent Things; IoIT; Challenges

I. INTRODUCTION

Due to the development of processing, sensing and communication technologies, many once simple devices are now able to perform more complex tasks and communicate with other devices or systems. This is the base of the Internet of Things (IoT) paradigm, whose core concept revolves around ubiquitous, uniquely identifiable everyday objects equipped with sensing, networking and processing capabilities that communicating with each other to achieve a common goal [1][2].

The IoT paradigm is being applied in several study fields; it is easy to find in the literature many applications in healthcare, industry, smart farms and cities, environmental monitoring and others. In some cases, application-specific networks are considered IoT branches, such as the Internet of Vehicles [3] or the Internet of Mobile Things [4]. The Internet of Intelligent Things (IoIT) is said to be composed of devices that are autonomous and mobile and have both sensing and action taking capabilities [5].

Popularly known as drones, Unmanned Aerial Vehicles (UAVs) are natural candidates to integrate with IoIT. Their integration with other vehicles and systems enables more complex missions, in which acquired data is up-to-date and intelligent actions can be taken either remotely or locally in cooperation with other devices — all with remote supervision. This integration, however, brings new challenges to be addressed regarding public safety and privacy, standardisation and technical aspects.

In this paper, we present some UAV applications that can be boosted by being integrated with IoIT, as well as new opportunities brought by connected UAVs, and challenges that need to be addressed so that the integration can be done seamlessly. Section II brings background information on UAVs and IoT. Section III present some related work. Section IV presents the opportunities in inserting UAVs into IoIT. Section V outlines some challenges that arise by UAV and IoIT integration. Finally, Section VI presents the paper conclusion.

II. BACKGROUND

In this section, some background concepts covering Unmanned Aircraft Systems, Flying Ad hoc NETworks and the Internet of Things are presented.

A. *Unmanned Aircraft System (UAS)*

UAVs are gaining popularity in both military and civilian segments, with the technology being successfully used in applications such as surveillance, disaster control and response, infrastructure and environmental monitoring, among others. Usually, an Unmanned Aircraft System (UAS) is composed by UAVs, the Ground Control Station (GCS) and the communication links [6][7]. Despite UAVs being usually considered resource-constrained devices, they also benefited from technology development and are now able to provide more complex functionality that lead to more sophisticated missions.

In recent years, the use of multi-UAV solutions in civilian applications has increased [8] since it presents numerous advantages. Multi-UAV systems have higher scalability (larger covered area) and survivability (the mission can still be performed even if one UAV fails), usually complete missions faster than a single UAV and have lower acquisition and maintenance costs [8][9][10].

Establishing efficient communication in a multi-UAV system, however, is a major challenge. Opposed to single-UAV systems, in which the communication can easily be done through a GCS or satellite connection, multi-UAV systems that use the infrastructure for inter-vehicle communication can experience disturbances in link maintenance due to environmental conditions or terrain topology, and the mission target area is limited by the network coverage. Therefore, an ad hoc approach is generally applied for multi-UAV systems, forming a Flying Ad hoc NETwork (FANET) [11][10].

B. Flying Ad hoc NETworks (FANETs)

An ad hoc network is a collection of nodes forming a temporary network with no infrastructure or centralised administration that is able to operate stand-alone or connected to the Internet. When nodes are mobile, the network is called MANET (Mobile Ad hoc NETwork). In this case, network topology is dynamic and may change as the nodes (or routers) move. If nodes are vehicles, the network is called VANET (Vehicular Ad hoc NETwork), and, if vehicles are UAVs, the network is called FANET.

Even though they may seem similar, FANETs have some characteristics that differ them from other types of ad hoc network [10]. Firstly, node mobility is usually much higher in FANETs due to node moving speed. Also, nodes in a FANET are usually kilometres apart and may have their course altered due to UAV movements, environmental changes or mission updates, resulting in a very uncharacteristic mobility model. All these facts contribute to a more frequently topology change due to UAV loss or UAV injection or even because of variations in the communication link/channel quality. Finally, some FANET protocols may need accurate localisation data faster than the one provided by a GPS (Global Positioning System). In these cases, the UAV must have other means to acquire this information (for instance, an Inertial Measurement Unit — IMU). Also, when considering small UAVs, computational capabilities and power consumption constraints must be taken into account. Routing and administration protocols must be energy-efficient to prolong the network lifetime [8].

C. Internet of Things (IoT)

Even though the Internet of Things theme has been vastly explored over the last few years, it still lacks a wide-accepted definition. The general idea of IoT is a large amount of everyday objects pervasively integrated in our environment, equipped with identifying, sensing, networking and processing capabilities, and able to communicate among themselves in order to complete a common task [1][2]. This results in a very distributed network system composed by entities that both provide and consume data from the physical world through sensors and actuators [12]. The application realm of IoT is really large, including areas such as health-care, smart environments (smart homes, factories or cities), environmental monitoring, and disaster alert and recovering [1][2][13][14][15].

Different technologies are involved in enabling IoT systems. *Identifying techniques* are crucial for uniquely address each connected device, ensuring the identification reliability and persistence. *Communication technologies* in general play a major role in these applications. New protocols and network strategies are necessary so that devices with both power and computational resources constrains can be integrated into the IoT. *Middleware* systems will be necessary to make the abstraction of all devices or *things* and make them available to users and applications. Also, it is expected that IoT systems will generate a large amount of data, making *data storage* a key technology for IoT and *Big Data* strategies essential for knowledge extraction [1][16][17]. *Cloud platforms* are being considered an important part of IoT systems and have gained interests in research recently [16][18]. The merge of IoT with cloud computing provides easy access to virtually unlimited processing and storage capabilities on demand and at a low cost, enhancing IoT scalability and performance [13][18]. Given its portability, the cloud is very suitable for IoT architecture, being able not only to aggregate, analyse and distribute collected IoT data continuously and securely but also to remotely manage and control systems. Moreover, it can concentrate services from different providers and bring them to the users in an easy, intuitive way [13][19].

Considering the amount of aspects and technologies involved, it is not surprising that IoT technology also comes with many challenges. *Scalability* can be considered a very onerous task given the large number of connected devices. How to locate, identify, authenticate, use and maintain them in a reliable manner is a hard problem to solve [12][16][20]. *Interoperability* issues will also arise due to a variety of devices supporting different protocols and platforms, or very resource-constrained devices that do not support any communication protocol. These problems must be considered by both developers and manufacturers since system inception so that device integration is done without compromising performance [12][16]. *Data sharing policies* among different applications also have to be considered. Deciding which data will be available to which application, as well as who has the higher priority has to be done carefully in order to ensure system trust and avoid application conflicts [12][20]. The *lack of standardisation* of both architecture and protocols is a major obstacle for IoT implementation, preventing both universal integration of devices — creating a “Babel Tower Effect” among them — and the creation of a competitive market in which all-size players can provide quality products for customers [16]. *Security and trust* of communication and data are a key challenge to address not only to guarantee system functionality, but also to have it accepted by the general public [12][16][20]. The *integration with the cloud* also brings its own challenges: the cloud must support a large number of users, providing at the same time real-time responses that meet system requirements; be prepared to deal with contextual and non-structured data, as well as resource-constrained devices and unreliable connectivity; and offer easy means for developing and deploying IoT applications. Data and communication security must also be addressed, as well as standardisation of IoT-supporting architecture, and device virtualization [16][17][18].

III. Related Work

The integration of UAVs and the Internet/cloud is a fairly recent research topic and is primarily focused in providing UAV telemetry information though a cloud platform or a service-oriented architecture that virtualizes UAVs and make them accessible through a cloud/IoT infrastructure. Some examples are discussed in this section.

In [21], a cloud-supported UAV application framework in which a client hosted at the UAV responsible for image acquisition, which are sent to a server in the cloud for image processing and data storage. The results are sent to a control centre to be evaluated by a human operator.

Authors in [22] propose an emergency-management service. A cloud platform manage UAVs that can be invoked by threatened citizens through a smartphone app. When the UAV reaches the person, a real-time video streaming is provided to security authorities, which can remotely operate the UAV in order to assess the danger and take necessary actions.

In [23], a cloud-based architecture for mission control called Dronemap is proposed. The cloud infrastructure is used to realise UAV virtualization and perform resource-demanding computations. In this architecture, the user requests a mission, performed by one or more UAVs selected by the user or automatically by a cloud manager. While the mission is being executed, relevant data are reported real-time to the user.

Authors from [24] present a framework to offer UAV as a Service (UAVaaS), in which UAVs are hired by a different set of users trough an Internet interface to execute a task. While waypoints and video feeds are available to the users, control and navigation functionality are handled by UAV's on board flight controller. A cloud coordinator handles all communication between the users and UAVs in order to provide better security and optimize resource usage.

In [25], the authors propose a technique to control UAVs using the Cloud — the user inputs only the state of the flight (for instance, altitude, direction and speed) and the system makes the necessary control adjustments so that user requirements are met. The communication between UAVs and the cloud is made by the remote ground station, which has the ability to connect to the cloud through Internet and to the UAVs using a wireless communication link (radio system).

Authors in [26] propose an UAV-Cloud platform in a Resource-Oriented Architecture in which UAVs act as servers whose resources can be accessed by APIs, applying a broker architecture for scalability. A proof of concept is provided using Arduino devices as UAVs and RESTful APIs to access their resources.

The work presented in [27] present a softwarization of the network so that the UAV infrastructure is decoupled from control. A controller layer virtualizes the infrastructure to the higher layers, while an orchestration layer manages the mission. A loosely coupled architecture is used to connect UAVs and sensors, with a middle layer managing the cooperation between the two.

IV. UAVs into IoIT: Opportunities

So what happens when we integrate UAVs into IoIT and connect them to the cloud? First of all, UAVs will have at their disposal the virtually unlimited cloud processing and storing capabilities, allowing the use of smaller, cheaper UAVs in missions. One must be careful, however, about how much processing will be done within the cloud. Processing primary tasks as obstacle avoidance remotely will bring a latency for the system not acceptable for aircraft [28]. Therefore, the cloud must be used for tasks that demand high computational power and can afford a quasi-instantaneous response.

Also, UAV telemetry and captured data will be available to the user through the cloud, making new data readily available and enabling real-time operations and decision making from any location. Thus, the cloud can also be used for the execution of machine learning techniques and algorithms, improving the overall operation by using the acquired experience.

The connection of UAVs will also be boosted. Aircraft will be able to communicate among themselves and share data, network resources, and services even with no line-of-sight (LoS), enhancing UAS collaboration and cooperation.

UAVs are likely to be considered as systems of systems. Every internal aircraft module necessary to fly (e.g., motors, actuators) or perform missions (e.g., cameras, thermal sensors) can be considered a single system. Such a view leads to a next-level-approach where every aircraft module is a *thing* on an IoT network that is fully capable of providing real-time information and take actions. The UAV can be considered a network of things (1st order) connected to the IoIT infrastructure, and the UAV itself would also be a node on the IoIT network (2nd order). Moreover, such modules can be considered not simply *things*, but also smart and intelligent things that can be connected as an independent network node and even provide cloud-based services to users nearby, e.g., local sensing, computation and decisions capabilities or remote resources. That is a potential achievement that inherits important characteristics from the fly by wireless paradigm [29].

The integration of UAVs and IoIT and the consequent UAV availability to other systems in real-time can enhance UAV performance in many situations, as described in this Section. Moreover, the possibility of moving a set of sensors (such as a vehicle) to an area that lacks in IoIT coverage will provide more precise services delivery, improved Quality of Service (QoS) and better sensors positioning.

Regardless of the application, UAVs as intelligent things are able to perform self-diagnosis in order to verify whether they are capable of performing the required task or providing the requested service. If unexpected events during the mission generate failure or unavailability, the IoIT redundancy offers replacement possibilities.

A. Emergency Applications

Emergency situations are always a trial for the city infrastructure. In some cases, the situation happens in an area of difficult access, delaying the emergency personnel response and in some cases jeopardising the victim's medical care. IoIT can improve emergency response by integrating UAVs and other devices in emergency situations.

UAVs in particular can be used to perform a first assessment sense and detect victims, specially in areas of difficult access such as mountains or very large areas like the ocean. Once the victim is located, the UAV can send through IoIT infrastructure the precise victim location to the emergency response team together with video feed for a quick evaluation of the situation. If needed, the same UAV or a different one can be used to deliver supplies such as bottled water or first-aid resources for immediate use until emergency personnel arrives.

Victim rescue can also benefit from IoIT. The UAV positioned near the victim can send weather conditions and terrain topology data so that the emergency response infrastructure can decide in advance if the rescue will be done by air or ground, optimising the emergency resources usage. In case of ground rescue, the UAV can also scout the area in order to identify blocked roads and other access difficulties, aiding the team to decide which path to take to reach the victim.

UAVs and other IoIT participants can also be used to improve the communication network in case it suffered damage during the emergency. Papers such as [30] and [28] propose the use of UAVs to build a temporary, mobile network infrastructure to be used by emergency personnel or the population in general until communication services are operating normally.

B. Smart Cities Applications

Smart Cities are becoming a topic of great interest in research. The objective of Smart Cities is to provide better quality of life with efficient infrastructure at reduced costs by integrating multiple assets such as transportation systems, power plants, law enforcement and others [31].

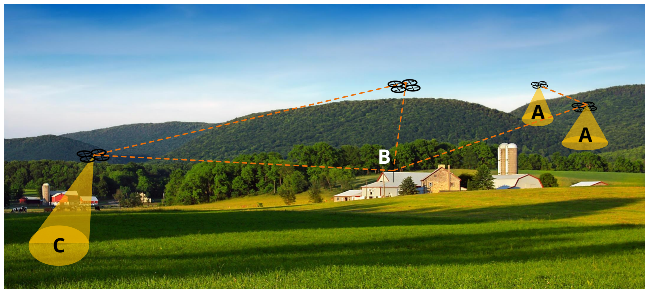

Figure 1. Smart Farm applications taken to the next level: (A) Surveillance in real-time; (B) Services integration; and (C) Identification of unexpected issues.

UAVs can perform several tasks in a smart city when connected to the IoIT. They can monitor in real-time the city infrastructure such as power lines, bridges, roads and railroads, reducing maintenance costs. Law enforcement can also be aided by patrolling, monitoring crowds or following a person of interest during a chase. They can also monitor the traffic flow and communicate the Intelligent Transportation System (ITS) about road accidents, as well as providing video images for emergency personnel. Finally, UAVs can also function as network infrastructure for city areas in which the connection link is limited, integrating them to the rest of the city and expanding the range of smart services.

C. Industry & Retail Applications

Industries have a lot to benefit from IoIT and its interface with other connected devices. The integration of smart machines in smart factories, smart storage facilities and smart supply chains will allow to automate the entire product chain, from production to delivery. For instance, a smart storage can detect if the sales of a particular product have increased and trigger a higher production so that this specific product is always available. In retail, smart supply chains will be able to provide real-time information for both suppliers and costumers, increasing the efficiency and customer experience.

In industries, UAVs can be used for real-time supervision of outdoor areas of the factory or for infrastructure inspection such as building structures or transportation ducts in oil and gas industry. When considering retail, UAVs are already being used in delivery of goods for major players such as Amazon [32], and can provide great customer experience by notifying the delivery and allowing it to be supervised in real-time.

D. Smart Farm Applications

Smart Farms also have great benefit potential from IoIT. The use of autonomous vehicles together with ubiquitous sensors for planting, monitoring crops and cattle and harvesting can increase efficiency of production by reducing its costs. Figure 1 presents examples of smart farm applications such as: (A) Surveillance in real-time; (B) Services integration; and (C) Identification of unexpected issues.

UAVs in particular can be used in many different ways in a smart farm [31]. UAVs can monitor farm borders for intruders or wildlife predators, promptly sending an alert for farm owner and calling law enforcement through IoIT infrastructure if necessary or dispersing the animals before they damage the crops or cattle. Monitor tasks can also extend to fields and cattle conditions, triggering suitable actions if a problem is encountered. They can also search for missing cattle and inspect the farm infrastructure such as silos or barn roofs. In plantation process, UAVs have been used for chemicals spraying, which can be optimised by the use of soil data gathered by IoIT connected sensors in the ground.

E. Government Applications

Border protection and surveillance is a task performed by different means, from human surveillance to walls and monitoring cameras. With the use of IoIT, this task can be automated and performed by unmanned vehicles (ground, aerial and aquatic) in cooperation, responding real-time to a remote control station that can perform the necessary protocol when an anomaly is detected. Specifically, UAVs can also be used to monitor forests and areas of environmental protection to identify problems such as forest fire or areas of illegal logging and notify the competent authority so that proper actions can be taken.

F. Vehicular Sensors as a Service

The integration of mobile objects (flying, driving, floating, rolling, diving, walking, etc.) to IoIT networks will provide means of moving sensors to the right place at the right time. That leads to the possibility of enabling modules as potential providers of cloud-based real-time services to nearby networks and users, improving targeted information delivery. This approach has great potential on providing flexible intelligent mapping, efficient goods delivery, and search and rescue services with high precision.

G. Environmental monitoring

Environmental monitoring is another promising domain for unmanned vehicles connected to the IoIT. There is a growing necessity to monitor great barrier reef or pole ice regarding climate changes. The application of Unmanned Underwater Vehicles (UUV) and Unmanned Surface Vehicles (USV) directly connected to satellites or somehow supported by UAVs will provide IoIT connectivity that can improve such activities with real-time information and services both ways.

V. UAVs into IoIT: Challenges

As seen before, the integration of UAVs into IoIT brings a lot of opportunities. However, there are many challenges that need to be overcome — some of them well known by the unmanned vehicle community, others emerging due to the connection of vehicles to an infrastructure such as IoIT. In general, these challenges are classified in three categories: public safety and privacy, standardisation and technical.

A. Public Safety and Privacy Challenges

Confidentiality issues regarding the data acquired by UAVs is a major concern — particularly if there is critical information being collected — and will play a starring role in public acceptance of the technology. There is a tendency to store as much data as possible into the UAV main memory in order to ensure availability [33], which ends up being a critical security weakness [34]. If the UAV is stolen or has its control taken, it can be used as a gateway to probe sensitive information from the secured network it is authenticated in. IoIT could improve security by transferring sensitive data to the cloud. However, providing data distribution in a secure manner on UAVs or other resource-restricted devices is another challenge.

Another concern for the general population would be snooping — a UAV can take unauthorised video or photos and share them online, making them nearly impossible to be removed and very difficult to identify the perpetrator. It is likely that governments will enact legislation to UAV registration and to prevent privacy invasion, as done in some states in the US [35]. Moreover, providing vehicular sensors as a service will increase risks, leading to the demand for more precise information security approaches.

B. Regulation & Standardisation Challenges

Certification is a must for insertion of UAVs into the airspace and prevent the technology of being used for nefarious purposes, such as physical assault, drug smuggling and others [36]. UAV safety plays a major role in this regulations, since a UAV out of control can cause damage to property or harm people. Because of that, many regulation agencies such as FAA [37] and EASA [38] have started to regulate the UAV market.

As with IoT, standardisation is also a major challenge for IoIT, and must involve both the industry and governments. From a technical point of view, standardisation is necessary to ensure all devices are able to communicate, preventing a "Babel Tower Effect" in which devices become split into disjoint subsets (for instance, all devices from the same manufacturer) that can only talk to others from the same subset. From a social and economic point of view, standardisation will favour the entrance of small and medium companies in the market, stimulating entrepreneurship and competition, benefiting the final customer and spreading the use of the technology.

C. Technical challenges

There are many technical issues in UAVs being integrated into IoIT. For starters, UAVs are resource-constrained devices. Hardware and software design must take into account limited memory, storage and processing capabilities, as well as a limited power source. Thus, algorithms and communication protocols must be as energy-efficient as possible. This aspect demands a local intelligence to decide how to partition computation and data over local and remote resources that can also be temporally unreachable because of wireless connection outage.

Also, IoIT will be formed with a variety of devices developed for various platforms and using different communication protocols, which can lead to compatibility and interoperability issues. Furthermore, the inclusion of vehicular sensors as *things* on the IoIT network will increase the complexity of the entire system, since the communication links can be performed directly from sensors belonging to different vehicles. This heterogeneity will also extend to the acquired data, that will most likely be non-structured. How data is gathered, distributed, stored and recovered has to be planned carefully in order to ensure real-time and security requirements.

Apart from certification, there is also a rising concern with GPS security. GPS spoofing attacks have become more frequent. Such attacks can cause the aircraft to completely lose control, which is a very critical issue. The GPS spoofing may help attackers to hijack UAVs, another issue that is strongly related to man-in-the-middle attacks.

Security is always a challenge in any communicating system and relate to all other aspects aforementioned. Limited resources demand efficient security algorithms that do not compromise performance or resource/power consumption; heterogeneity defies the idea of implementing a global security policy for all devices and data storage must also be covered by security in case the communication is interrupted or the physical integrity of the device compromised. Therefore, security solutions must permeate all layers of the architecture — reducing the breaches throughout the layers will consequently reduce the overall chances of attacks to the network.

Safety is another important aspect for the devices, which must be able to determine the "health" and the authenticity of both its internal and external components [11] — something even more challenging if the internal components are also connected wirelessly.

VI. CONCLUSION

IoIT is a network composed of autonomous and mobile devices equipped with both sensing and action taking capabilities. UAVs are natural candidates to be integrated into IoIT, which enable a new degree of collaboration between devices and real-time supervision of missions. One promising opportunity is the use of vehicles and sensors as services allowing a better integration of all *things*, leading to an environment composed by everything, updated every-time and available everywhere. This integration, however, introduces new challenges to be addressed regarding public safety and privacy, standardisation and technical aspects. Despite the challenges, the integration of UAVs into IoIT is a promising research topic with high chances of applicability. In this paper, we presented how UAV integration to IoIT can improve applications, as well as the current challenges.

By proposing solutions to the identified challenges, the development of IoIT integrated with autonomous vehicles should be facilitated in order to achieve relevant advances in this research area. Moreover, the challenges presented here are only a sampling of potential issues that might be faced in this new paradigm. Besides the number of challenges, the several different missions and applications pointed out that can be performed in the near future are exciting. This is why not only the military but also the civilians, the academics, and the industry are enthusiastic about novel uses and applications of autonomous vehicles and IoIT.

ACKNOWLEDGEMENTS

The authors acknowledge the support granted by CAPES and FAPESP under processes 2012/16171-6.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," Computer Networks, vol. 54, no. 15, 2010, pp. 2787–2805, ISSN: 13891286.

[2] A. Whitmore, A. Agarwal, and L. Da Xu, "The Internet of Things A Survey of Topics and Trends," Information Systems Frontiers, vol. 17, no. 2, 2015, pp. 261–274, ISSN: 1387-3326.

[3] O. Kaiwartya et al., "Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges and Future Aspects," IEEE Access, vol. PP, no. 99, 2016, ISSN: 21693536.

[4] L. E. Talavera et al., "The Mobile Hub concept: Enabling applications for the Internet of Mobile Things," in International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops), March 23-27, 2015, St. Louis, USA. IEEE, Mar 2015, pp. 123–128, ISBN: 978-1-4799-8425-1, URL: http://dx.doi.org/10.1109/PERCOMW.2015.7134005 [accessed: 2017-01-09].

[5] Y. Chen and H. Hu, "Internet of intelligent things and robot as a service," Simulation Modelling Practice and Theory, vol. 34, 2012, pp. 159–171, ISSN: 1569190X.

[6] K. P. Valavanis and G. J. Vachtsevanos, Handbook of Unmanned Aerial Vehicles. Dordrecht: Springer Netherlands, 2015, ISBN: 9789048197064.

[7] S. G. Gupta, M. M. Ghonge, and P. M. Jawandhiya, "Review of Unmanned Aircraft System (UAS)," International Journal of Advanced Research in Computer Engineering & Technology, vol. 2, no. 4, 2013, pp. 1646–1658, ISSN: 2278-1323.

[8] L. Gupta, R. Jain, and G. Vaszkun, "Survey of Important Issues in UAV Communication Networks," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, 2016, pp. 1123–1152, ISSN: 1553-877X.

[9] O. K. Sahingoz, "Mobile networking with UAVs: Opportunities and challenges," in International Conference on Unmanned Aircraft Systems (ICUAS), May 28-31, 2013, Atlanta, USA. IEEE, May 2013, pp. 933–941, ISBN: 9781479908172, URL: http://dx.doi.org/10.1109/ICUAS.2013.6564779 [accessed: 2016-03-31].

[10] I. Bekmezci, O. K. Sahingoz, and S. Temel, "Flying Ad-Hoc Networks (FANETs): A survey," Ad Hoc Networks, vol. 11, no. 3, 2013, pp. 1254–1270, ISSN: 15708705.

[11] D. F. Pigatto et al., "HAMSTER - Healthy, Mobility and Security-based Data Communication Architecture for Unmanned Aircraft Systems," in International Conference on Unmanned Aircraft Systems (ICUAS) May 27-30, 2014, Orlando, USA. IEEE, May 2014, pp. 52–63, ISBN: 9781479923762, URL: http://dx.doi.org/10.1109/ICUAS.2014.6842238 [accessed: 2016-05-10].

[12] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Networks, vol. 10, no. 7, 2012, pp. 1497–1516, ISSN: 15708705.

[13] A. Botta, W. de Donato, V. Persico, and A. Pescapé, "Integration of Cloud computing and Internet of Things: A survey," Future Generation Computer Systems, vol. 56, 2016, pp. 684–700, ISSN: 0167739X.

[14] H. Arasteh et al., "Iot-based smart cities: A survey," in 16^{th} International Conference on Environment and Electrical Engineering (EEEIC) June 7-10, 2016, Florence, Italy. IEEE, Jun 2016, pp. 1–6, ISBN: 9781509023202, URL: http://dx.doi.org/10.1109/EEEIC.2016.7555867 [accessed: 2016-09-14].

[15] R. Kumar and A. Pandey, "A Survey on Security Issues in Cloud Computing," International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), vol. 2, no. 3, 2016, pp. 506–517, ISSN: 2394-4099.

[16] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," IEEE Communications Surveys & Tutorials, vol. 17, 2015, pp. 2347–2376, ISSN: 1553-877X.

[17] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," Future Generation Computer Systems, vol. 29, no. 7, 2013, pp. 1645–1660, ISSN: 0167739X.

[18] E. Cavalcante et al., "On the Interplay of Internet of Things and Cloud Computing: A Systematic Mapping Study," Computer Communications, vol. 89-90, 2016, pp. 17–33, ISSN: 01403664.

[19] J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers, "Twenty Security Considerations for Cloud-Supported Internet of Things," IEEE Internet of Things Journal, vol. 3, no. 3, 2016, pp. 269–284, ISSN: 2327-4662.

[20] J. A. Stankovic, "Research Directions for the Internet of Things," IEEE Internet of Things Journal, vol. 1, no. 1, 2014, pp. 3–9, ISSN: 2327-4662.

[21] C. Luo, J. Nightingale, E. Asemota, and C. Grecos, "A UAV-Cloud System for Disaster Sensing Applications," in 81^{st} Vehicular Technology Conference (VTC Spring), May 11-14, 2015, Glasgow, Scotland. IEEE, May 2015, pp. 1–5, ISBN: 9781479980888, URL: http://dx.doi.org/10.1109/VTCSpring.2015.7145656 [accessed: 2016-04-23].

[22] G. Ermacora et al., A Cloud Based Service for Management and Planning of Autonomous UAV Missions in Smart City Scenarios. Springer International Publishing, 2014, pp. 20–26, ISBN: 9783319138237_3.

[23] B. Qureshi, A. Koubaa, M.-F. Sriti, Y. Javed, and M. Alajlan, "Dronemap - A Cloud-based Architecture for the Internet-of-Drones," in International Conference on Embedded Wireless Systems and Networks (EWSN) February 15-17, 2016, Graz, Austria, Feb 2016, pp. 255–256, ISBN: 9780994988607, URL: http://www.ewsn.org/file-repository/ewsn2016/255_256_qureshi.pdf [accessed: 2016-04-02].

[24] J. Yapp, R. Seker, and R. Babiceanu, "UAV as a service: Enabling on-demand access and on-the-fly re-tasking of multi-tenant UAVs using cloud services," in 35^{th} Digital Avionics Systems Conference (DASC), September 25-19, 2016, Sacramento, USA. IEEE, Sep 2016, pp. 1–8, ISBN: 9781509025237, URL: http://dx.doi.org/10.1109/DASC.2016.7778007 [accessed: 2017-01-20].

[25] S. Majumder and M. S. Prasad, "Cloud Based Control for Unmanned Aerial Vehicles," in 3^{rd} International Conference on Signal Processing and Integrated Networks (SPIN), February 11-12, 2016, Noida, India. IEEE, Feb 2016, pp. 421–424, ISBN: 9781467391979, URL: http://dx.doi.org/10.1109/SPIN.2016.7566731 [accessed: 2016-12-19].

[26] S. Mahmoud and N. Mohamed, "Toward a Cloud Platform for UAV Resources and Services," in Fourth Symposium on Network Cloud Computing and Applications (NCCA), June 11-12, 2015, Munich, Germany. IEEE, Jun 2015, pp. 23–30, ISBN: 9781467377416, URL: http://dx.doi.org/10.1109/NCCA.2015.14 [accessed: 2016-04-23].

[27] S. Mahmoud, I. Jawhar, and N. Mohamed, "A Softwarization Architecture for UAVs and WSNs as Part of the Cloud Environment," in International Conference on Cloud Engineering Workshop (IC2EW), April 4-8, 2016, Berlin, Germany. IEEE, apr 2016, pp. 13–18, ISBN: 9781509036844, URL: http://dx.doi.org/10.1109/IC2EW.2016.17 [accessed: 2016-09-25].

[28] M. Cochez, J. Periaux, V. Terziyan, K. Kamlyk, and T. Tuovinen, "Evolutionary Cloud for Cooperative UAV Coordination," Department of Mathematical Information Technology, University of Jyväskylä, Jyväskylä, Finland, Tech. Rep., 2014, ISBN: 9789513957292, URL: http://www.cs.jyu.fi/ai/papers/UAV_report.pdf [accessed: 2016-04-16].

[29] D.-K. Dang, A. Mifdaoui, and T. Gayraud, "Fly-By-Wireless for next generation aircraft: Challenges and potential solutions," in IFIP Wireless Days (WD), November 21-23, 2013, Dublin, Ireland, Nov 2012, pp. 1–8, ISBN: 9781467344043, URL: http://dx.doi.org/10.1109/WD.2012.6402820 [accessed 2017-01-22].

[30] S. Morgenthaler, T. Braun, Z. Zhao, T. Staub, and M. Anwander, "UAVNet: A Mobile Wireless Mesh Network Using Unmanned Aerial Vehicles," in IEEE Globecom Workshops, December 3-7, 2012, Anaheim, USA. IEEE, Dec 2012, pp. 1603–1608, ISBN: 9781467349413, URL: http://dx.doi.org/10.1109/GLOCOMW.2012.6477825 [accessed: 2016-04-02].

[31] F. Mohammed, A. Idries, N. Mohamed, J. Al-Jaroodi, and I. Jawhar, "UAVs for smart cities: Opportunities and challenges," in International Conference on Unmanned Aircraft Systems (ICUAS) May 27-30, 2014, Orlando, USA. IEEE, May 2014, pp. 267–273, ISBN: 9781479923762, URL: http://dx.doi.org/10.1109/ICUAS.2014.6842265 [accessed: 2017-01-20].

[32] "Amazon makes its first drone delivery in the U.K." URL: http://money.cnn.com/2016/12/14/technology/amazon-drone-delivery/ [accessed: 2017-01-17].

[33] K. Hartmann and C. Steup, "The vulnerability of UAVs to cyber attacks - An approach to the risk assessment," in 5^{th} International Conference on Cyber Conflict (CyCon) June 4-7, 2013, Tallinn, Estonia. Tallinn, Estonia: IEEE, Jun 2013, pp. 1–23, ISBN: 9781479904501, URL: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6568373 [accessed: 2016-04-16].

[34] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," Wireless Networks, vol. 20, no. 8, 2014, pp. 2481–2501, ISSN: 1022-0038.

[35] Y. Kim, J. Jo, and S. Shrestha, "A Server-Based Real-Time Privacy Protection Scheme against Video Surveillance by Unmanned Aerial Systems," in International Conference on Unmanned Aircraft Systems (ICUAS) May 27-30, 2014, Orlando, USA. IEEE, May 2014, pp. 684–691, ISBN: 9781479923762, URL: http://dx.doi.org/10.1109/ICUAS.2014.6842313 [accessed: 2016-08-12].

[36] N. Hossein Motlagh, T. Taleb, and O. Arouk, "Low-Altitude Unmanned Aerial Vehicles-Based Internet of Things Services: Comprehensive Survey and Future Perspectives," IEEE Internet of Things Journal, vol. 3, no. 6, 2016, pp. 899–922, ISSN: 2327-4662.

[37] "Unmanned Aircraft Systems," URL: https://www.faa.gov/uas/ [accessed: 2017-01-20].

[38] "Unmanned Aircraft Systems (UAS) and Remotely Piloted Aircraft Systems (RPAS)," URL: https://www.easa.europa.eu/unmanned-aircraft-systems-uas-and-remotely-piloted-aircraft-systems-rpas [accessed: 2017-01-20].