Graduate Research in Engineering and Technology (GRET)

Volume 1
Issue 4 *Emerging Aerospace Technologies in Aerodynamics, Propulsion, and Materials.*

Article 9

January 2022

# Advancements in UAVs-A review

Sriram Sravya
*Institute of Aeronautical Engineering, Dundigal, Hyderabad*, sriramsravya77@gmail.com

Y. D. Dwivedi
*Institute of Aeronautical Engineering, Dundigal, Hyderabad*, yddwivedi@gmail.com



## Recommended Citation

Sravya, Sriram and Dwivedi, Y. D. (2022) "Advancements in UAVs-A review," *Graduate Research in Engineering and Technology (GRET)*: Vol. 1 : Iss. 4 , Article 9.
DOI: 10.47893/GRET.2022.1060
Available at: https://www.interscience.in/gret/vol1/iss4/9

# Advancements in UAV's-A review

Y D Dwivedi, S.Sravya

Department of Aeronautical Engineering, Institute of Aeronautical Engineering, Hyderabad , 500043, India

**Abstract**

Present decade has been observed that Unmanned Aerial Vehicles(UAVs) are occupying the sky to accomplish different missions. They became the popular area of interest due to their growing utility and relative cost. Increased demand of UAVs allowing the researchers for the optimized UAV as a major area of interest. They are providing new and better opportunities to cellular networks. UAV industry is undergoing a huge amount of advancements in it such as in navigation system, privacy and security ,mission management system, power system communication system etc. this article mainly focuses on the advancements regarding privacy and security of UAVs ,mission management system. The motivation behind the development of strategies for defending the breaches caused by data protection and public safety them are examined. This study gives an overview about past and how the present usage of UAVs is optimized by implementing the defense techniques. The major six criteria implemented to defend socio-technical concerns are explained. Few countries which adapted these regulations are discussed briefly .Ensuring security of the UAV system is studied considering physical security and cyber security as major aspects. The study also provides the techniques to defend these security threats. on Mission planning and mission management

Keywords : Privacy , Data protection, , Cyber Security, Mission management system, Cellular networks

## 1.INTRODUCTION

Drones which are also called as UAVs has tremendous value in various platforms. UAVs enable limitless aerial perspective. The UAVs are first documented in mid 1800's when Australian forces attacked the city of Venice using 200 explosions filled balloon carriers. From then, drones have been primarily in use in military , the advancements in UAVs from world war-II to present has led its interest in commercial fields. The physical parts of most UAVs are same. Complete UAS mainly consists of four parts[1] a baseline aircraft, optional manual control backup, which is realized via RC link for crash avoidance, a GCS system for remotely monitoring the UAV's in flight status and intervene the UAV's operation if needed, and an onboard flight control system (FCS) acting as the UAV's brain The nearly limitless visibility , data gathering and analyzing capabilities make automated drones valuable for several industry sectors. Drones and software together makes an autonomous solution. Advancements make the aerobatic solution a permanent part of the facility and integral to its operations. UAVs not only contribute for a beneficiary results but also result in privacy breach . contribution of new technologies in privacy and security are discussed clearly[1]**.** The six criteria applicability, technical requirements, operational limitations, administrative procedures, human resource requirements, implementation of ethical constraints are mentioned in the article[6]**.** The data principles [3] which has to be followed by the UAV systems are mentioned. The risk levels of various aspects in cyber security such s hijacking , eavesdropping , jamming, spoofing, denial of service (dos) along with the defense methodologies are described in the paper**[**18**][**19**][**20**][**21**].** On the other hand mission planning and management system of UAVs are examined. Recent advancements which optimizes the UAV are studied. This includes UAV system to work autonomously to work under changing environmental conditions, creating a mission plan , providing minimum execution time of

system, aligning the mission plan and a explanation regarding the percentage of failures[2] in various systems of mission management system are provided.

**2.**Emerging technologies helped the UAVs to meet its widespread use and operational requirements. In order to satisfy with the socio -technical concerns of drones such as privacy, data protection, public safety certain regulations are implemented. To know the motivation behind the implementation of criteria against socio- technical concerns are examine[1].
**2.1 PRIVACY**: It is major aspect observed to be affected with the usage of drones for both individuals and businesses. Surveillance UAVs can easily violate the businesses privacy. Employing UAVs for operations such as Multispectral/thermal/NIR cameras, aerial photography and Videography traffic monitoring can breach privacy even they are not intentionally equipped. Modern technologies permit the drones to facilitate privacy breach. For instance building a drone with low noise and high maneuvering capabilities and sensitive on-board instruments can create a trouble-fee environment to violate privacy. To defend these , every country has legislation to protect the privacy of public and citizen's such as the Commonwealth Privacy Act 1988 in Australia and the US Privacy Act of 1974.
**2.2 DATA PROTECTION** : To steal the personal data and business data is quite unchallenging for UAVs. they can take images ,videos as apart of 'invisible' data due to their aerial capabilities and they can easily share the information in various platforms. Invisible data refers to fact that drones can secretly collect data due to sensitive equipment on-board such as high resolution and night vision camera{1}. As a result of aerial capabilities of drones they can collect and store massive data which is against the data principles[3] . these complications motivate regulations to implement criteria for data protection.

**2.3 PUBLIC SAFETY** : High safety threats can be faced with the employment of UAVs. The accident rates for UAVs are significantly higher than those of manned aircraft . UAV collisions include collisions with manned aircraft or terrain [4] They result in hurting of civilians and damaging the airframes and various expensive equipments. Therefore, maximum allowed flight heights and minimum distances to airports for drones operation , for bidding drones to fly over certain areas such as specific urban areas with high population density are followed [5].

**3. CRITERIA**: Current UAV regulations are predominantly based on six criteria[6]

**Applicability** : It defines for which the regulations are applicable. Such as drones are classified in to groups based on operation and weight , which might be treated differently by UAV regulations.
**Technical requirements** :It describe the mandatory instruments or techniques for drones. Example: collision avoidance mechanism
**Operational limitations** : UAV is restricted in many factors in operation such as flight height, minimum distance to airport and individuals, prohibited areas etc.
**Administrative procedures**: it described the procedures and documents required before a UAV is allowed to operate which include registration, operational certificate and insurance
**Human resource requirements** : pilot needs to be qualified to operate UAV for various categories and purposes.
**Implementation of ethical constraints**: This criterion appoints the demands for data and privacy protection when operating drones.

## 4.. UAV COMMUNICATIONS REGULATION The advancements in communications are summarized here :

The Electronic Communications Committee (ECC) within the European Conference of Postal and Telecommunications Administrations (CEPT) formed a correspondence group on spectrum requirements for drones in Dec. 2015. This group produced the ECC 268 report discussing the technical, regulatory aspects and the needs for spectrum regulation for UAVs in Feb. 2018 [11] The use of cellular networks for UAV C&C communications is addressed in this report and is currently under further study . Additionally, ECC 268 discusses the communications requirements of both professional UAV use cases, which could benefit from using individual licensed spectrum, and non-professional UAV applications, where unlicensed bands may suffice for short range communications . (refer table 1.1,1.2, 1.3)
The Federal Communications Commission (FCC) in the U.S. received in Feb. 2018 a petition for rule-making from the Aerospace Industries Association (AIA) [12]**.** The petition is seeking to allow the secure communication of C&C and non-payload data between UAVs and licensed pilots in the 5030-5091 MHz band. The FCC has to gather public comment before adopting a decision

## 5. UAV FLYING REGULATION

PAST: The first UAV regulation was proposed in in1944. The first internationally recognized aviation regulation, the Chicago convention pointed out that

the operation of UAVs should be authorized to ensure the safety of manned civil aircraft [13]. In 21st century due to rapid development of UAV , regulations have progressed both nationally and internationally. In 2002, the United Kingdom and Australia first published their UAV regulations. In 2006, the International Civil Aviation Organization (ICAO) announced that it was necessary to issue an internationally acknowledged legislation for civil operations of UAVs. Since 2012, an increasing number of countries have established their own UAV regulations. [1]

PRESENT:Tables-1 describes the current UAV regulation frameworks of 3 countries based on the criteria . from the table -1 it is seen that every country has specific operational limitations to defend socio-technical concerns. currently only the UK is aware of protecting the data collected by UAV operations. Introducing new drone regulations is also considered to be worthy when we think about privacy and data protection. . Recently, waivers for regulations have been given to Apple, Microsoft and Uber for their drone-testing projects, which will help the Federal Aviation Authority (FAA) shape the future development of UAV regulations in the US [17].

## 6.SECURITY

It is the most predominant issue to be considered while operating UAVs . since UAV is equipped with wireless communication system security is the most serious issue to be considered. if a flying cellular BS is compromised by attackers, then its serving UEs are more likely to lose cellular connections since the UAV may directly crash . Moreover, cellular UEs served by terrestrial BSs might suffer from strong interference due to LOS links, if a UAV is manipulated by attackers. Therefore, it is essential to ensure security of UAVs when used for cellular communications. It includes cyber security and physical security.

**6.1 Physical Security:** Obtaining access to UAVs is the major aspect to launch physical attacks. Accessing can be done on the ground(damaged or ran out of battery) or capture a flying drone. Enemies also can control drones by launching cyber attacks which will be discussed later. Here attack paths and respective counter measures according to the attackers are discussed.[23]

**6.1a** LOW: To capture the internal data attackers disassemble the drones. e.g. telemetry data via common interfaces such as USB . to defend this attacks, self destruction mechanisms could be applied on drones which will be enabled under pre-defined circumstances. However self destruction mechanism should only be implemented when necessary due to the reasons of public safety , loss of data and drone .

**6.1b** MEDIUM : Attackers could access data through higher standard interfaces such as Joint Test Action Group (JTAG). In this case, information stored on the drone needs to be encrypted. However, encryption may only delay the time taken by adversaries to obtain their desired data

**6.1c** HIGH: Advance attacks such as side-channel attacks, fault injection attacks and software attacks are used to retrieve desired information from a drone. To deal with such attacks, superior cryptographic mechanisms and secure key management should be equipped by drones.

**6.2 Cyber Security:** Cyber attacks has been increasing on UAV systems due to its widespread use it is reported that since 2007 more number of cyber attacks have occurred on drones [18]. Enemies mainly target on the radio links of UAV systems which carry information such as data requested by cellular UEs, control signals and global positioning system (GPS) signals for UAVs' navigation. By capturing these information enemies can easily steal the data carried by UAVs. Manipulating the control signals and using for their own advantage is not big challenge for attackers. Since UAV works on wireless communication ensuring its security has a significant importance to protect the data and control signals. Here we analyze potential attack paths and respective defense strategies(FIG-1)&(table 2)

**6.2a** JAMMING : generating interference signals in the same frequency band can disrupt the reception process. s. For example, GPS jamming has become a critical threat for drones. It was reported that in 2012 a small drone crashed and led to casualties, which was suspected to be caused by GPS jamming for the legitimate receiver [19]. For jamming attacks, increasing the signal to noise ratio (SNR) could be a defense solution. However it is dependent on the transmitter power

**6.2b** EAVESDROPPING: Wireless channels such as Wi-Fi connections and cellular communications provide a favorable open environment for the enemies to obtain the information. It breaches the confidentiality aspect of security. Eavesdropping breaches the confidentiality aspect of security.

Encryption and physical layer security techniques could be used as a protective mechanism

**6.2c** HIJACKING : when enemies takeover the radio link it is referred as hijacking. Radio links are Wi-Fi connections. Hijacking process takes place with the "de authentication" management frames to disconnect radio links. Then the UAV will come under the enemies control via 802.11 protocols[1]. Effective detection algorithms could be applied and transmitted frames could be encrypted. For example, WPA2 (802.11i-2004) encryption mechanism with proper key length is recommended as a countermeasure [19] And dynamic key generation could provide even stronger protection [20]

**6.2d** SPOOFING: It can be done by transmitting the GPS signals with the higher power than the authentic one's. Enemies use this technique to take over the drones. To defend GPS spoofing attacks, defense solutions such as jamming-to-noise sense and multi-antenna defense could be employed [21] [22]. In [7], authors successfully disconnected a drone from its controller by continuously sending spoofed ARP replies with the valid controller's MAC address.

**6.2e** DENIAL OF SERVICE (DoS) : To cause network congestion, enemies will send excessive requests to the server. s a result, the legitimate users will lose their service.

## 7.MISSION PLANNING AND MANAGEMENT SYSTEMS AND THEIR COMPONENTS

In military based applications, UAVs has to perform specific tasks which are predefined and characterized in advance and they are provided to the vehicle in series of command formats. Vehicles are designed depending up on the tasks to be carried out by them. Some are designed for longer missions and easier tasks and other for smaller missions and so on.. a system has to make use of its resources effectively to make a successful mission. The availability of resources on the system restricts the mission profile in the aspects of range and endurance A typical autonomous mission management system constitutes of : mission planning (task/resource allocation, motion planning), mission execution (navigation, task execution, intelligent decision making), mission monitoring (mission progress evaluation, situational awareness, contingency and anomaly detection), and mission re-planning (re-tasking, resource reallocation, re-routing).

## .8.MISSION PLANNING AND MISSION MANAGEMENT SYSTEMS OF UAVs

Present article focuses on the drawbacks of the current UAV technologies such as vehicle's structure, perception, rapid adaption and reflexive response which results in poor performance when compared with the manned aircrafts. The study describes the reasons for failure of mission management system by comparing the failures in various mission management system accordingly.[2]

Emergency procedures(26%) parts quality/suitability (16%), testing (16%), SW configuration control (13%), redundancy of critical systems (10%), design problems (6%) and assembly errors (3%)

**(**Johnson et.al 2001)argued that by providing optimized mission management system, failures can be avoided up to 30%. Allowing UAVs to monitor autonomously , forecasting future state and allowing them to address their own problems can be a better solution to decrease failure in mission management. Robust and reusable software architectures allow UAVs to meet all the above requirements.

Johnson et al. (2001) proposed an autonomous control executive(ACE) in mission management architecture called TRAC which is responsible for managing the real-time execution of the mission plane in a step-by-step manner with the following functionalities

segment completion. - Reacting to unexpected events during a mission segment. - Managing start-up and shutdown. - Logging Issuing mission segment commands-monitoring mission events and data.

Sullivan et al. (2004) mainly focuses on the mission success by making UAV system to redirect the flight with different environmental conditions and goals of the flight. To this end, an on-board Intelligent Agent Architecture (IAA) and a ground-based Collaborative Decision Environment (CDE) are employed. The CDE system provides SA, collaboration, and decision-making tools for UAV in order to furnish its mission plan, schedule monitoring, direct the payload system, integrate sensing goal to the mission plan, and provide visualization. Te system uses MAPGEN (Mixed Initiative Activity Planning Generator) which is a ground-based decision support which allows human operators to operate manually automatically generated plan and to take required steps for keeping system within the boundary[6].

(Linegang et al. 2006) in mission planning aligning the operator's conceptualization is the most important task to be performed accurately for the development of intelligent autonomy. The author in this article suggests to use the interface displays which allow the operators to focus on the aspects of the plan which influence the automation system's functioning and made use of Mission Displays for Autonomous Systems (MiDAS) that uses Cognitive Work Analysis (CWA) in its analysis of the ISR (Intelligence, Surveillance, and Reconnaissance) work domain

(Saska et.al 2013) introduced an approach based on utilizing pairs of virtual leaders that are controlled by an optimization process . the resultant solution of the optimized process includes a complete control plan in addition to controlling inputs of individual UAVs. Virtual leaders have resulted in the increased maneuverability of UAVs

JAPAN:

Applicability : classification: weight/purpose

Operational Limitations :

- daytime only
- by VLOS only
- minimum distance to people, other UAVs, ground properties and water surface: 30m
- cannot fly over event sites
- cannot carry hazardous materials
- cannot drop any objects
- prohibited airspace:
  - 150m above ground level
  - airspace around airports
  - densely inhabited districts (DI

Administrative Procedures
permission required for operation in the prohibited airspace
[25]

TABLE 1.1

AUSTRALIA:

Applicability: classification: weight/purpose

Operational limitations :
- Minimum distance to people: 30m
-Height limit:120m
- Minimum distance to airport:5.5km
-Daytime only(not for sunset)
- By visual line of sight(VLOS)only
-cannot operate over popular areas

Administrative procedures: insurance strongly recommended
Human resources:>2kg:pilot's license required

Ethical constraints: respect personal privacy[2]

TABLE 1.2

UK

Applicability: classification: weight/purpose

Technical Requirements:
beyond visual line of sight (BVLOS):
collision avoidance required

Operational Limitations:
- minimum distance to people: 50m
- height limit: 122m
- minimum distance to congested area: 150m
- by VLOS only (up to 500m)
-

Administrative Procedures :approvals vary for different operations

Human Resources :pilot competency required

Ethical Constraints: protect data integrity and confidentiality [2]

TABLE 1.3

| THREAT | LIKELIHOOD | IMPACT |
|---|---|---|
| JAMMING | HIGH | LOW |
| EAVESDROPPING | HIGH | MEDIUM |
| HIJACKING | MEDIUM | HIGH |
| SPOOFING | MEDIUM | HIGH |
| DoS | HIGH | HIGH |

TABLE -2 THREAT ANALYSIS[1]


FIG-1

| Technique | Highlights |
|---|---|
| Real-time adaptive mission planning approach [8] | Allow to reassess the environment continuously to identify the change and to appropriate action. Facilitates continuous mission plan adaption and maintains a window to take actions. |
| TITAN (Tactical Information Technologies for Assured Networks ) [ Manousakis et al. (2011)][9] | Focuses on mission networking requirements. Re-planning process is facilitated using a Mission to Policy Translation (MPT) mechanism |
| Phase mission analysis [24] | Each phase of the mission analysis is performed to identify the failures in every phase. It is performed through the use of library of probable failure causes of all potential phases. |
| B-Spline point-by-point Path Planner[ Keller et al. (2013)][10] | Aims to provide minimum execution time by approach post-processes the point-by-point path planner's output |

TABLE-3:FEW APPROACHES TO UAV-BASED MISSION PLANNING AND MISSION MANAGEMENT SYSTEM

**9.CONCLUSIONS :**

We have studied that the Criteria to defend socio-technical concerns are very important to maintain personal as well as business privacy and security. Implementing Regulations in operations of UAVs protects the information, security and privacy. We have studied clearly about socio-economic concerns and the reasons to defend them . We have discussed few countries and regulations followed by them. They restrict the flying of UAVs by implementing regulations to ensure successful mission. There is chance to implement new regulations in future which can be acceptable to carry when we consider safety and privacy aspects.

On the other hand mission planning and mission management of UAV systems are explained in this study clearly. Various ideologies to carry out autonomous mission profile are discussed. Advancements in mission management system allow the UAV system to create own mission profile , take necessary actions for changing environment conditions. Recent advancements optimize the mission management system in the aspects of execution time, failure analysis, networking requirements, mission plan adaption, aligning the operator's conceptualization , virtual leaders etc.

In future, implementation of new regulations are expected to ensure the successful defense of socio-technical concerns. And also optimized mission management system will introduce to avoid the mission failures. As we have studied better mission management system can reduce the mission failures up to 30%.

**10.REFERENCES:**

1)Azade Fotouhi,Haoran Qiang, Ming Ding, Lorenzo Galati Giordano,Mahbub Hassan, Adrian Garcia-Rodriguez,Jinhing Yuan. Survey on UAV cellular communications: Practical Aspects, Standradization Avancements, Regulation, and Securtiy challenges.

2)Adham Atyabia , Somaiyeh MahmoudZadehb,∗ , Samia Nefti-Meziani. Current advancements on autonomous mission planning and management systems: An AUV and UAV perspective.2018

3) Rachel L Finn, David Wright, L Jacques, and P De Hert. Study on privacy, data protection and ethical risks in civil remotely piloted aircraft systems operations: Final report. Retrieved February, 27:2015, 2014.

4) Christopher Bolkcom and Elizabeth Bone. Unmanned aerial vehicles: Background and issues for congress, report for congress, congressional research service. In Library of Congress, 2003.

5) Bill Canis. Unmanned aircraft systems (UAS): Commercial outlook for a new industry. Congressional Research Service Washington, 2015

6) Claudia Stöcker, Rohan Bennett, Francesco Nex, Markus Gerke, and Jaap Zevenbergen. Review of the current state of uav regulations. Remote sensing, 9(5):459, 2017.

7) Michael Hooper, Yifan Tian, Runxuan Zhou, Bin Cao, Adrian P Lauf, Lanier Watkins, William H Robinson, and Wlajimir Alexis. Securing commercial wifi-based uavs from common security attacks. In Military Communications Conference, MILCOM 2016-2016 IEEE, pages 1213– 1218. IEEE, 2016

8) http://refhub.elsevier.com/S1367-5788(18)30025-7/sbref0068

9) http://refhub.elsevier.com/S1367-5788(18)30025-7/sbref0060

10) http://refhub.elsevier.com/S1367-5788(18)30025-7/sbref0042

11)ECC Report 268. Technical and Regulatory Aspects and the Needs for Spectrum Regulation for Unmanned Aircraft Systems (UAS). Feb. 2018.

12)FCC Petition for Rulemaking. Aerospace Industries Association (AIA) Petition for Rulemaking on Unmanned Aircraft Systems (UAS). Feb. 2018.

13)WM Sheehan. Air cabotage and the chicago convention. Harvard Law Review, 63(7):1157–1167, 1950.

14)https://doi.org/10.1016/j.ejcon.2012.10.003( Saska, Mejia, Stipanovic, and Vonasek (2013))

15)https://doi.org/10.1177/154193120605002304(Lin egang et al. (2006))

16)https://doi.org/10.1117/12.582446 (Sullivan et al. (2004) (121-131) )

17 ) The Guardian. Apple, Microsoft and Uber test drones approved but Amazon left out in cold. url:https://www.theguardian.com/technology/ 2018/may/ 10/ apple-microsoft-uber-drones-approved-testing-amazon, May 2018.

18 ) Ahmad Y Javaid, Weiqing Sun, Vijay K Devabhaktuni, and Mansoor Alam. Cyber security threat analysis and modeling of an unmanned aerial vehicle system. In Homeland Security (HST), 2012 IEEE Conference on Technologies for, pages 585–590. IEEE, 2012

19) CG Leela Krishna and Robin R Murphy. A review on cybersecurity vulnerabilities for unmanned aerial vehicles. In Safety, Security and Rescue Robotics (SSRR), 2017 IEEE International Symposium on, pages 194–199. IEEE, 2017.

20) Daojing He, Sammy Chan, and Mohsen Guizani. Communication security of unmanned aerial vehicles. IEEE Wireless Communications, 24(4):134–139, 2017.

21) [Chitra Javali, Girish Revadigar, Ming Ding, and Sanjay Jha. Secret key generation by virtual link estimation. The 10th EAI International Conference on Body Area Networks, pages 301–307, Sep. 2015.
22)Daniele Borio and Ciro Gioia. Real-time jamming detection using the sum-of-squares paradigm. In Localization and GNSS (ICL-GNSS), 2015 International Conference on, pages 1–6. IEEE, 2015

23) Kamesh Namuduri, Serge Chaumette, Jae H Kim, and James PG Sterbenz. UAV Networks and Communications. Cambridge University Press, 2017.

24) http://refhub.elsevier.com/S1367-5788(18)30025-7/sbref0004

25) Civil Aviation Bureau. Japan's safety rules on Unmanned Aircraft (UA)/Drone, 2015. http://www.mlit.go.jp/en/koku/uas.html (accessed on 29 October 2018).

26) YD Dwivedi, YB Sudhir Sastry An experimental flow field study of a bio-inspired corrugated wing at low Reynolds number- 2019, journal-INCAS Bulletin,volume 11,pages 55-65

27) YD Dwivedi, V Bhargava . .aerodynamic characterization of bio inspired corrugated wings-2019-journal-MOJ App Bio Mech,pages 1-10

28) V Sridhar, YD Dwivedi.effect of peak shape in bio inspired corrugated wing.2017,journal-International conference on advances in thermal systems, materials and design engineering (ATSMDE2017),