Drone Security: Issues and Challenges

Rizwan Majeed¹, Nurul Azma Abdullah², Muhammad Faheem Mushtaq³, Rafaqut Kazmi⁴
Faculty of Computer Science and Information Technology¹,²
Universiti Tun Hussein Onn Malaysia (UTHM), Parit Raja 86400, Johor, Malaysia
Department of Computer Science³
The Islamia University of Bahawalpur, 63100 Bahawalpur, Pakistan
Department of Software Engineering⁴
The Islamia University of Bahawalpur, 63100 Bahawalpur, Pakistan

Abstract—Recent advancements in drone technology are opening new opportunities and applications in various fields of life especially in the form of small drones. However, these advancements are also causing new challenges in terms of security, adaptability, and consistency. This research discusses the drone technology, area of usages, citizen multi-objective uses, drones security, protection, and secrecy apprehensions, drone current intimidations and susceptibilities, existing approaches for drone cyber-security methods, security threats to drones and data sources for current literature review. Small drones are proving to be a new opportunity for the civil and military industries. The small drones are suffering from architectural issues and the definition of security and safety issues. The rapid growth of the Internet of Things (IoT) opens new dimensions for drone technology but posing new threats as well. The tiny flying intelligent devices are challenging for the security and privacy of data. The design of these small drones is yet not matured to fulfill the domain requirements. The basic design issues also need security mechanisms, privacy mechanisms and data transformations.

Keywords—Drone technology; security; internet of things; threats; privacy

I. INTRODUCTION

In this modern atomic world, drone technology is mainly used for military purposes and defensive areas. Drone technology is rapidly growing for defense purposes. These microdevices are flying in the air 200 feet above the ground. This range of height varies from device to device and purpose to purpose. This range can be in feet, meters, and kilometers. Flight time of these intelligent devices also varies from device to device [1][2]. The frequency variations and their properties are discussed in Table I.

### TABLE I. FREQUENCY VARIATIONS AND THEIR PROPERTIES

| Parameters      | 2GHz       | 5GHz       |
|-----------------|------------|------------|
| Frequency band  | Low speed  | High Speed |
| Cost            | Cheap      | Costly     |
| Range           | Extended range | Undersized range |
| Effect of noise | Noisy      | Less noisy |
| interference    | Prone to interference | Less prone to interference |
| Physical barriers| Overcome physical barriers | Unable to overcome physical barriers |
| Performances    | Disturb Wi-Fi speed | Don’t disturb Wi-Fi speed |

A. Rules and Guidelines

Many countries have strict rules and regulations for drone usage in civilian areas [16-18]. The rules and regulations issued advice for drone owners to use drones under government license. Drones must not enter private legacies without the permission of the owner. In Lebanon, strict rules are followed for drone usage. No person can fly drones in private areas, without the permission of the owner. To fly drones in private areas, the owner of the drone must get the permission certification for this act. Without this, one can face serious prosecutions. Following are some rules which must be followed by each drone owner in the USA.

- A drone must not reach 400 feet in height.
- A drone must not enter sensitive areas i.e. aircraft and airfields.
- A drone must be operated with safety and care to prevent face examination.
- A drone must not enter civilian areas.
- A drone must not be operated in gatherings and functions

Such rules are strictly followed by drone owners for safe drone flights. Heavy fines and punishments can be faced by the owners of the drone if such rules are violated.

B. Drone Structural Design

A UAV structure comprises three components. These components include Unmanned Aircraft, Ground Controller, and Communication link [3,19]. An explanation of these components is given below.

- The Flight Controller is the CPU of a drone.
- Ground station controller provides communication between the craft and controller.
- Data communication link provides information communication between ground controller and drone.

In [3] drones are categorized depending on their distance from the ground controller. These categories are given below.

- Line of sight distance drones use radio waves for communication.
Beyond line of sight distance, drones use satellite communications.

C. Drone Communications Categories

Drones are classified into different categories based on their communication styles. These categories are D2D, D2G, and D2N. This communication is described in Fig. 2.

1) Drone-to-drone: Drone to Drone communication is not yet legalized. Machine learning approaches can be used in such communication in a wireless environment. This is also known as peer-to-peer communication. Such communication is more prone to jamming and DoS attacks [20 – 23].

2) Drone-to-ground location: This type of communication is mainly standardized and based on specific protocols with 2 and 5 GHz frequencies. It can also be operated on Bluetooth and Wi-Fi. Many of such communications are not available in the public sector because of security and authentication issues. Such communication is more prone to eavesdropping and man-in-the-middle attacks as shown in Fig. 1.

3) Drone-to-network: Such communication allows network selection for control and transfer of information. Several Wi-Fi networks can be used at different frequencies in such types of communication.

4) Drone-to-satellite: GPS devices are involved to provide real-time communication in such types of drone communication. Drone communicates with the satellites for location measurement. This communication is more secure and safe as compared to other categories and is used in the military.

D. Unmanned Aerial Vehicles Types

All Unmanned Aerial Vehicles can be called drones. In this section, differences between drones, UAVs and UAS are described in detail. Fig. 7 explains this classification difference in detail.

1) Drones: Drones are remote-based air devices that can be used on earth and in ships for different purposes. Different types of drone categories are described below based on their technology.

   a) Multi-Blade Drones: Such drones are based on vertical landing and flying mechanisms. Such drones usually based on fixed operations and are easier to be attacked by external devices. This communication is very accurate but has less mobility because of the huge consumption of energy.

   b) Fixed-Blade Drones: These drones consume less energy and are most suitable as compared to multi-blade drones [33,34]. These drones are faster and can handle heavy payloads.

   c) Hybrid-Blade Drones: These drones have fixed as well as moving wings. These drone devices are speedy as compared to other types.
2) **UAVs**: These devices consist of a controller which can be a mobile or a computer. These devices can be operated independently and are classified into the following categories. A UAV can fly remotely/autonomously using a controller, mobile phone, computer, or even a tablet [24]. They are characterized into the following types [25]:

- Remote Pilot Control UAVs are based on the controller which is handled by a human on the ground.
- Remote Supervised Control UAVs work independently and can be handled by a human if needed.
- Full Autonomous Control drones work independently without any human intervention.

3) **UAS**: UAS is a combination of UAV and drone. A UAV is also a UAS that is controlled by a controller [38].

4) **RPA**: Remotely Piloted Aircraft works independently for a long time without any intervention. It is used in complex missions and flights [37].

II. **AREAS OF USAGE**

In the current era of technology, drone demand is increasing day by day. Drones help in delivering foods, items, and goods. Drones are also called flying riders. The main objective of using drones is to reach those areas where human access is limited. Drones usage is present in many areas of life [13][33]. This usage is discussed below in Fig. 3.

---

**A. Citizen Multi-Objective Uses**

Drone technology is used by civilians in many areas of daily life. These domains consist of life-saving, disaster management, etc. main uses of drones are discussed below.

a) **Camerawork**: Drones use is increasing in photography and video shooting in those areas where the human approach is difficult [34].

b) **Disaster Management**: Disaster monitoring and controlling is also possible using UAVs and UAS since the 2005 major disaster. It helps in evaluating the situation of destruction and damage.

c) **Exploration and Rescue**: UAVs are also used to explore and save the lives of people and other living beings.
d) **Tourism:** UAVs help in exploring different areas in tourism and traveling trips [35], which improves tourism revenue.

e) **Commercials:** Drones and UAVs are used to shoot commercials and Ads with HD cameras in minimum time. This saves time and cost for overall shooting.

f) **Emergency Supervision:** Extremist attacks and disasters can be handled and monitored using UAVs and drones [36].

g) **Quick Reaction:** Drones and UAVs as a first aid kit in many situations [37]. Drones were also used in the Covid-19 pandemic to provide disinfectant spray. Drones help in delivering foods and other items in this situation [38, 39 and 40].

h) **Ecological Management:** Drones provide different ecological measurement tasks including population calculation etc. it can also be used to calculate environmental parameters. It is also used to monitor crop parameters, air quality analysis, and weather measurement.

i) **Subsurface/Oceanic Devotions:** Underwater drones help in monitoring the underwater environment and operations [41]. Drones can provide live recording and monitoring.

III. **Drones Security, Protection, and Secrecy Apprehensions**

Drones technology provides several advantages and benefits for human beings. It helps in day-to-day activities as well as the military and monitoring of weather. However, several privacy and safety concerns are associated with their advantages. Security and privacy breaches should be addressed properly. Recording and image capturing by drones must be done keeping in mind the privacy and confidentiality of people’s concerns [42]. For sanctuary and risk examination of drones, several studies are present in which risk associated with it is considered and discussed.

It is important to maintain secrecy, reliability, obtainability, verification, and non-denial possessions above message-passing networks are fulfilled. This can be achieved through AAA procedures and progressions:

- Authorization is achieved by providing access to the control unit of the drone/UAV.
- Verification can be obtained by using multi-level authentication using knowledge (specific key), identity verification and biometric verification.

Security threats are associated with drones which can be physical or cyber-attacks. It is important to limit drone usage in civilian areas and properties. The negative use of drones is also increasing day by day. This usage also creates problems for the citizens and civilians. Drone owners use Bluetooth or Wi-Fi channels to control their drones in restricted areas. This can lead to financial loss. Drones are used to breach Wi-Fi connections and Bluetooth signals. Such breach causes so many privacy and security concerns for peoples. Fig. 4 shows the important security threats to drones. Solutions to prevent these threats are also discussed. A summary of present and upcoming safety apprehensions is given below.

![Fig. 4. Drone Threats Taxonomy.](image-url)
A. Safety Apprehensions

A drone is tiny, lightweight, and has high mobility characteristics. It can be used to monitor criminal activities which are done at a high level of privacy. It can also be used by criminals to perform their illegal activities.

Drones can be equipped with dangerous objects to perform criminal acts. Such acts can create damage to civilians. It is a matter of concern to overcome such extremist activities for the wellbeing of peoples. Several terrorist groups can associate armed objects with a drone to perform their illegals activities.

Security doesn’t constantly deliver protection. There are chances of damage done by the civilians in civilian areas which can result in financial loss [43]. The following list provides the safety concerns in detail.

- Minimum safety features in architecture can lead to control drone usage. This can result in damage and loss [44].
- Minimum mechanical and operative ethics include smashing avoidance techniques which can lead to drone’s incapability to identify airliners [45].
- Absence of Administrative knowledge: especially it mainly occurs when people have less knowledge of safety features [46].

B. Confidentiality Apprehensions

Privacy is also the main factor to be considered for people. Drones must be kept out of those areas which are private. One must know the level of privacy of people before capturing or entering a private legacy. Three types of privacy threats are discussed below.

- Flying drones over someone’s property is considered a major issue because of the risks associated with this act. Because such data can be used by scammers for negative purposes.
- Monitoring somebody’s location must be avoided without their permission [47].
- Monitoring someone’s acts and doings is also another unethical act which is also a matter of concern [48].

IV. DRONES CURRENT INTIMIDATIONS & SUSCEPTIBILITIES

Several security threats are associated with drones and UAVs. Many design and architecture issues of drones cause such threats and vulnerabilities. Data and information protection must be addressed in drones to overcome these issues [49].

- Susceptible to Spoofing: several weak points are present which are related to architecture and control of UAVs and drones which may result in spoofing of information shared by the drone. Spoofing can be of several types [50, 51, 52, 53]. GPS spoofing is the easiest way to capture information and do modifications to it.
- Susceptible to Viruses: there are chances of malware and virus threats in the information shared by drones via a communication device which can be a mobile or a computer. This communication is also insecure because of poor wireless connection.
- Susceptible to data interruption: drones are more susceptible to data interruption and interception. Which may result in various threats associated with data vulnerability [54]. Such type of data interruption also causes malicious data insertion from drone to controller device [55].
- Susceptible to handling: drone devices are tiny objects which have building programming and control instructions, these instructions are more prone to manipulation which may change their operation and cause serious destructions [56].
- Susceptible to machine-driven problems:
  - Many technical problems may occur during flight operations which may result in damage and destruction of data. Such failures may include unstable control connection [57,58].
  - Susceptible to functioning problems: such issues include poor knowledge of control and command of a drone. Such lack of functioning information causes accidents and damage [59]. Many times, the drone also gets crushed in such incidents [60].
  - Susceptible to environmental problems: Environmental factors include, wind speed, rain, heat, humidity result in problems for drone flight [61, 62].
  - Susceptible to signal congestion: drones can also be spoofed using a signal loss mechanism which may transfer the control to a third party. Such situations also cause problems. This problem occurs by using device microcontrollers i.e. Arduino and raspberry-pi [63].

V. EXISTING APPROACHES FOR DRONE CYBER-SECURITY METHODS

Major security methods for drone cybersecurity are categorized into the following types. Such classification is based on the attacker’s aim and purpose. The following section discusses the existing approaches to prevent drone security issues.

A. Drone Network Security

Several security problems occur during drone flights and communication with a base station. To overcome such problems, and intrusion detection method was identified which can recognize illegal activities. Intrusion detection methods capture network flow and detect abnormal activities. Several intrusion detection methods are present which are used to analyze anomalies. These methods include rule-based, signature-based, and anomaly-based intrusion detection methods.

B. Drone Information Safety

Drone communication must be transformed into packet data to prevent load on the communication network. Such packaging allows safe communication to some extent. However such packaging also produces many problems. In one study [64],
Cipher security is discussed, which can protect data from attackers.

C. Scientific Resolutions

Scientific methods are present in the drone domain which works by analyzing the network flow using forensic methods of monitoring. Such monitoring provides identification and detection of illegal access and capturing.

VI. Security Threats to Drones

Drone security has many layers and types according to its size, use, and controlling mechanism. The drone control in many cases using Wi-Fi with IEEE 802.11 communication protocol [65]. The typical designs of drones using the communication network are Wi-Fi networks with its ground stations. These networks are vulnerable to security breaches. Professional drones may be hijacked due to no proper encryption on their chips [66]. The second hijacking mechanism known to the research community was the man-in-middle attacks which is possible up to 2 KM only. The bottleneck so far emerged was with no encryption drones may be hijacked by individuals [67].

The novice trend in drone security is the Internet of Drones (IoD). The concept is equally popular in defense and industry drones [68]. The wide range of applications of IoD is in civilian and military drones simultaneously. The basic problem with drones was that they will design without security mechanisms in mind. There were fundamental security and privacy issues in drone technology regarding its design. The major issues identified in the domain of IoD security are privacy leakage, data confidentiality, data protection, data flexibility, data accessibility, and data encryption and decryption strategies [69].

In many studies in the last few years, various security and data privacy threats are identified by various researchers. The identified cybersecurity attacks are divided into four categories such as protocol-based attacks, sensors-based attacks, compromised components attacks, and jammers attacks. An account of such identified possible threats under these four cybersecurity attacks, found in the literature review, is given in Table II.

Table II shows that the majority of the available work in cybersecurity and data privacy of industrial drones is just the identification of possible threats. The solution to these threats does not exist. An attempt was made to use encryption to secure data transmission of a drone to a base station by using a Key Encryption algorithm for secure packet delivery [11].

Small drones and their usage are gaining the attention of the research community in recent years. These drones are popular because they have fewer wingspan and lightweight as well. The security and privacy of individuals and governments under threat due to these small drones as well [74]. Some other studies are also highlighting common challenges and threats to drone security [14-19].

Tian presented an efficient privacy-preserving authentication framework for edge-assisted internet of drones that was capable of ensuring the privacy of the drones Network [20]. Similarly, Hell presented a drone system for the security and surveillance purpose of a factory [21]. This system was capable of monitoring a defined area of a factory for security purposes. A similar application was also presented by Tosato in 2019, where he introduced an autonomous application of a swarm of drones for sensing industrial gas [22]. These types of drones are getting popular these days to monitor and surveillance the industrial area or an agriculture farm for the sake of security management.

TABLE II. TYPICAL CYBERSECURITY AND DATA PRIVACY THREAT TO SMART DRONES

| Threats Identified Citations | Countermeasures Citations |
|------------------------------|---------------------------|
| Security of Communication Link | [70], [71], [72], [73] |
| Data Confidentiality Protection | [1] |
| Replay Attack | [34], [35] |
| Privacy Leakage | [1], [23] |
| De-authentication Attack | [8], [10], [36] |
| GPS Spoofing/Jamming Attack | [4], [37], [38] |
| Motion Sensors Spoofing | [41] |
| UAV Spoofing/Jamming Attack | [4] |
| IoT Security Threats | [4], [5], [18] |
| Control/Data Interception | [4], [6] |
| Denial of Service | [4], [8], [10], [39], [40] |
| Stop Packet Delivery | [11] |
The contributions to the identification of cybersecurity threats to drones are the healthy research area in the recent past. In 2016, Vattapparamban discussed a study on the application of drones for smart cities where he also discussed basic issues of Cybersecurity and privacy [23]. A few of these issues are also highlighted in Table I. A similar study to identify the possible security attacks along with the limitations of drone systems with a set of recommendations was also presented in 2020 by Yaacoub [24]. There are various studies [25], [26], and [27] that closely study the problems and challenges in drone security and its applications in business, commerce, etc. A few of them also propose the use of blockchain for secure data delivery using 5G and IoT enables drones [27]. However, this system heavily relies on manual identification of threats type and intensity. There is a need for a smart and intelligent system for drone security that can analyze data of security breach attempts and attacks and adopt a proactive measure to ensure the security of the drones.

There are a few other survey-based studies [28], [29], [30], and [31] to identify common challenges and solutions to security threats and issues to drones used for industrial and commercial purposes. A few tried to address the problem of device authentication with lightweight authentication using key agreement [28] and key-enabling technique [30] for safe drones. The application of IoT drones in agriculture is also getting very common and recent contributions are discussed [9][32-33].

The problem of hacking and hijacking of drones and UAVs is a common threat to commercial drones that are specifically studied in [34], [35], [36], and [37]. The countermeasures problem of hacking and hijacking of drones and other UAV machines is proposed in [36] and [37]. Another common issue of drones is the capturing of the drones [38] and UAV machines are GPS spoofing that also needs a secure and authentic solution. A few other studies on the hijacking of drones and intercepting control of a drone are also discussed in [39], [40], [41], and [42].

A. Gap Analysis of Drone Security using Machine Learning

There are a few basic types of machine learning techniques such as supervised learning, unsupervised learning, semi-supervised learning and reinforcement learning, deep learning, etc. During the literature survey, it was found in the recent past that, various attempts have been made to use machine learning solutions to handle cybersecurity attacks for mobile networks [45], wireless sensor networks [46], cloud computing [48], IoT systems [53][7][12], etc. An account of previous attempts to use machine learning for the security of various types of wireless networks is given in Table III.

However, there is no previous work is found to use machine-learning-based cybersecurity solutions for drone security threats. Additionally, we propose to use a machine-learning-based security solution with Blockchain to improve authentication and access control mechanisms in drone security.

In the detailed survey of literature from 2010 to 2020 in the area of drone and UAVs security, safety, and privacy concerns, more than 30 contributions were found in the form of research papers mainly published in IEEE and ACM journals. Majority of these papers highlight challenges and problems in the area of cybersecurity, device interception, data privacy, GPS spoofing, IoT spoofing, hijacking drones, and many similar cybersecurity threats in recent times. However, the majority of the literature is just highlighting identified key threats and issues to the security of drones but a majority of them are not giving solutions and countermeasures to handle security threats to drones. Only, in [27], blockchain is proposed for secure data delivery using 5G and IoT enables drones. However, this system heavily relies on manual identification of threats type and intensity. Other attempts are also relying on key-based authentication of devices that are not authentic of security specifically in the domain of IoT based drones. There is a clear research gap to make drones secure and safe from major cybersecurity threats to make drones useful for commercial and industrial purposes.

| Sr. No | Attacks     | Security Technique | Machine Learning Solution             |
|--------|-------------|--------------------|---------------------------------------|
| 1      | Jamming     | Secure Offloading  | Q-learning [45], [46] Q/DQN [47]      |
| 2      | Denial of Service | Secure Offloading | Neural Networks [48] Multivariate correlation analysis [49] Q-learning [50] |
| 3      | Malware     | Access Control     | Q/Dyna-Q/PDS [51] K-nearest neighbors [52] Random Forest [52] |
| 4      | Intrusion   | Access Control     | Naive Bayes [53] Support vector machine [53] Neural network [54] K-NN [55] |
| 5      | Spoofing    | Authentication     | SVM [56] DNN [57] Dyna-Q [58] Q-learning [58] |
| 6      | Traffic blockage | Authentication | Q-learning [59]                        |

TABLE III. APPLICATION OF MACHINE LEARNING-BASED SOLUTION FOR CYBERSECURITY
There is a need for a smart and intelligent system for drone security that can analyze data of security breach attempts and attacks and adopt a proactive measure to ensure the security of the drones. Previously, machine learning-based cybersecurity solutions are proposed for mobile networks, wireless sensor networks but not proposed for drone security. Additionally, we propose to use a machine-learning-based security solution with Blockchain to improve authentication and access control mechanisms in drone security.

VII. DATA SOURCE FOR CURRENT LITERATURE REVIEW

Major data sources are explored for literature study of proposed system. Instead of searching through internets, direct databases are accessed to get relevant studies. However some other sources are also searched to get all possible relevant papers. These papers are filtered and only relevant papers are studied for this review. Manual selection is performed to exclude irrelevant papers. Table IV shows the data sources for current study.

A. Workflow of Current Literature Study

Literature study is carried out indifferent steps. Different actions are performed at each stage to get accurate and relevant proposed solutions. In the first step, literature review is performed with IoT, smart devices and security challenges for these devices. These security challenges are categorized and discussed accordingly. In next step, solutions for these threats are discussed and security issues are identified. Limitations for existing solutions are identified in these papers. A new solution is proposed to overcome these limitations. Fig. 5 shows the workflow of current literature study.

B. Year-Wise Publications

The following graph shows the year-wise publications list. In 2011 relevant studies were 9 which are considered in the proposed study shown in Fig. 6. This number increases each year. In 2020, relevant studies are increased which include IoT and drone security and solutions. Fig. 7 shows the graph in which drone security issues, solutions, threats, uses, frameworks, and algorithms are described for the current selection of papers.

| Data Foundation     | Web link                          |
|---------------------|-----------------------------------|
| IEEE Xplore         | http://ieeexplore.ieee.org/Xplore/|
| ACM Digital Library | http://dl.acm.org/                |
| Springer            | http://www.springerlink.com/      |
| Elsevier            | Elsevier http://www.elsevier.com/|
| Science Direct      | https://www.sciencedirect.com/    |
| Other Sources       | Conferences, books and webpages   |

Fig. 5. Workflow for Literature Review.

Fig. 6. IoT and Drone Security Publications for a Current Study Concerning the Year.

Fig. 7. Security, Privacy, and Risks Associated with IoT and Drone Objects.
VIII. CONCLUSION AND FUTURE WORK

Now-a-days, IoT is the most widely used network among all networks. It is a network of communicating devices, which are interacting with each other. It is widely used for home automation, health care, and remote devices. Among all these applications, IoT is wonderfully used in civilian departments. It is widely utilized to interconnect medical and industrial devices. These devices provide easy and effective facilities to people. The machine learning based solutions for drone security is also used to handle cybersecurity attacks for mobile networks, wireless sensor networks, cloud computing, IoT systems, etc. IoT devices provide far-off fitness, manufacturing, and emergency alert method. This research can be further enhance using machine learning based security solution with Blockchain to improve authentication and access control mechanisms in drone security.

REFERENCES

[1] E. Biddlecombe, “UN predicts ‘internet of things’,” June 7, 2009.
[2] D. Butler, “2020 computing: Everything, everywhere,” Nature, vol. 440, no. 7083, pp. 402–409, 2006.
[3] S. Dodson, “The net shapes up to get physical,” Guardian, 2008.
[4] N. Gershenfeld, R. Krikorian, and D. Cohen, “The Internet of things,” Scientific American, October, 2004.
[5] R. Lombreglia, “The Internet of things,” Boston Globe, pp. 76–83, 2005.
[6] A. Reinhardt, “A machine-to-machine Internet of things,” 2004.
[7] E. A. Kosmatos, N. D. Tslikas, and A. C. Boucouvalas, “Integrating RFID and smart objects into a unified Internet of things architecture,” Advances in Internet of Things, vol. 1, pp. 5-12, 2011.
[8] M. A. Shahid, U. Akram, M. M. A. Shahid, A. Samad, M. F. Mushtaq and R. Majeed, “A Systematic Approach Towards Compromising Remote Site HTTPS Traffic Using Open Source Tools” IEEE 23rd International Multitopic Conference (INMIC), 2020.
[9] H. Choi, W.-C. Lee, Y. Aafer, F. Fei, Z. Tu, X. Zhang, D. Xu, and X. Xinyan, “Detecting attacks against robotic vehicles: A control invariant approach,” in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, ACM, pp. 801–816, 2018.
[10] G. Biamino, “Semantic model for socially aware objects, Advances in Internet of things,” vol. 2, pp. 47-55, 2012.
[11] I. Ungurean, N. C. Gaitan, and V. G. Gaitan, “An IoT architecture for things from industrial environment,” in Proc. 10th Int. Conf., 2014, pp. 1–4.
[12] F. Li, M. Voegler, M. Claessens, and S. Dustdar, “Efficient and scalable IoT service delivery on cloud,” Proc. in IEEE 6th Int. Conf. Cloud, pp. 740–747, 2013.
[13] K.D. Atherton, “The FAA says there will be 7 million drones flying over America by 2020”, Popular Sci., 2016.
[14] E. Vattapparamban, I. Güvenç, A. I. Yurekli, K. Akkaya and S. Uluagac, “Drones for smart cities: issues in cybersecurity, privacy, and public safety”, IEEE International Wireless Communications and Mobile computing Conference (IWCMC), pp. 216–221, 2016.
[15] K. Dalamagkidis, K.P. Valavanis and L.A. Piegl, “Aviation history and objective UAV routing”, IEEE International Conference on Unmanned Aircraft Systems (ICUAS), pp. 534–542, 2014.
[16] E. Yanmaz, R. Kuschnig, M. Quaritsch, C. Bettstetter and B. Rinner, “Automatic collision avoidance for manually tele-operated unmanned aerial vehicles”, IEEE International Conference on Robotics and Automation (ICRA), pp. 6638–6643, 2014.
[17] J. Israelsen, M. Beall, D. Bareiss, D. Stuart, E. Keeney and J. Berg, “On path planning strategies for networked unmanned aerial vehicles”, IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 212–216, 2011.
[18] L. H. Hernandez, A. Tsourdos, H. S. Shin and A. Waldock, “Multi-objective UAV routing”, IEEE International Conference on Unmanned Aircraft Systems (ICUAS), pp. 534–542, 2014.
[19] E. Vattapparamban, I. Güvenç, A. I. Yurekli, K. Akkaya and S. Uluagac, “Drones for smart cities: issues in cybersecurity, privacy, and public safety”, IEEE International Wireless Communications and Mobile computing Conference (IWCMC), pp. 216–221, 2016.
[20] J. Dinger, H. Hartenstein, "Defending the Sybil attack in P2P networks: taxonomy, challenges, and a proposal for self-registration," First Int. Conf. on Availability, Reliability and Security (ARES’06), 2006.
[21] M. F. Mushtaq, S. Jamel, and M. M. Deris, "Triangular Coordinate Extraction (TCE) for Hybrid Cubes," J. Eng. Appl. Sci., vol. 12, no. 8, pp. 2164–2169, 2017.
[22] H. Rowhani, W. Enck, P. McDaniel and T. La Porta, “Limiting sybil attacks in structured P2P networks, 26th IEEE International Conference on Computer Communications, pp. 2596–2600. 2007.
[23] N. Naoumov and K. Ross, “Exploiting P2P systems for DDoS attacks”, Proc. of the 1st international conference on Scalable information systems, ACM, 2006.
[24] J. Irizarry, M. Gheisari and B.N. Walker, “Usability assessment of drone technology as safety inspection tools”, J. Inf. Technol. Construct. (ITcon), vol. 17, no. 12, pp. 194–212, 2012.
[25] R. Altawy and A.M. Youssf, “Security, privacy, and safety aspects of civilian drones: a survey”, ACM Trans. Cyber-Phys. Syst. Vol. 1, no. 2, 2017.
[26] F. Barfield, “Autonomous collision avoidance: the technical requirements”, Proceedings of the IEEE National Aerospace and Electronics Conference, pp. 808–813, 2002.
[27] R. Sharma and D. Ghose, “Collision avoidance between UAV clusters using swarm intelligence techniques”, Int. J. Syst. Sci., vol. 40, no. 5, pp. 521–538, 2009.
[28] A. Hamza, U. Akram, A. Samad, S. N. Khosa, R. Fatima and M. F. Mushtaq, “Unmanned Aerial Vehicles Threats and Defence Solutions”, IEEE 23rd International Multitopic Conference (INMIC), 2020.
[29] S. Ueno and T. Higuchi, “Collision avoidance law using information amount”, Numerical Analysis-Theory and Application, IntTech, 2011.
[30] J. Israelens, M. Beall, D. Bareiss, D. Stuart, E. Keeney and J. Berg, “Automatic collision avoidance for manually tele-operated unmanned aerial vehicles”, IEEE International Conference on Robotics and Automation (ICRA), pp. 6638–6643, 2014.
[31] E. Yannaz, R. Kuschnig, M. Quaritsch, C. Bettstetter and B. Rinner, “On path planning strategies for networked unmanned aerial vehicles”, IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 212–216, 2011.
[32] L. H. Hernandez, A. Tsourdos, H. S. Shin and A. Waldock, “Multi-objective UAV routing”, IEEE International Conference on Unmanned Aircraft Systems (ICUAS), pp. 534–542, 2014.
[33] E. Vattapparamban, I. Güvenç, A. I. Yurekli, K. Akkaya and S. Uluagac, “Drones for smart cities: issues in cybersecurity, privacy, and public safety”, IEEE International Wireless Communications and Mobile computing Conference (IWCMC), pp. 216–221, 2016.
[34] A. Rango, A. Laliberte, C. Steele, J.E. Herrick, B. Bestelmeyer, T. Schmugge, A. Roanhorse and V. Jenkins, “Using unmanned aerial vehicles for rangelands: current applications and future potentials”, Environ. Pract. 8, 3, pp. 159–168, 2006.
[35] N. Jumaat, B. Ahmad and H.S. Dusenwai, “Land cover change mapping using high resolution satellites and unmanned aerial vehicle”, IOP Conference Series: Earth and Environmental Science, 2018.
[36] J.-P.A. Yaacoub, M. Noura, H.N. Noura, O. Salman, E. Yaacoub, R. Coudurier and A. Chehab, “Securing internet of medical things systems: limitations, issues and recommendations”, Future Generat. Comput. Syst., 2019.
[37] C.A. Thiels, J.M. Aho, S.P. Zietlow and D.H. Jenkins, “Use of unmanned aerial vehicles for medical product transport”, Air Med. J. 34 (2) (2015) 104–108.
[38] M. Lipsitch, D.L. Sberdlow and L. Finelli, “Defining the epidemiology of covid-19-studies needed”, N. Engl. J. Med., 2020.
[39] F. Jiang, L. Deng, L. Zhang, Y. Cai, C.W. Cheung and Z. Xia, “Review of the clinical characteristics of coronavirus disease 2019 ( covid-19)”, J. Gen. Intern. Med., pp. 1–5; 2020.
[40] M.N.K. Boulos and E.M. Geraghty, “Geographical tracking and limitations, issues and recommendations”, Future Generat. Comput. Syst., 2019.
[41] Syst., 2019.
[42] S. Ueno and T. Higuchi, “Collision avoidance law using information amount”, Numerical Analysis-Theory and Application, IntTech, 2011.
[43] J. Israelsen, M. Beall, D. Bareiss, D. Stuart, E. Keeney and J. Berg, “Automatic collision avoidance for manually tele-operated unmanned aerial vehicles”, IEEE International Conference on Robotics and Automation (ICRA), pp. 6638–6643, 2014.
[44] A. Rango, A. Laliberte, C. Steele, J.E. Herrick, B. Bestelmeyer, T. Schmugge, A. Roanhorse and V. Jenkins, “Using unmanned aerial vehicles for rangelands: current applications and future potentials”, Environ. Pract. 8, 3, pp. 159–168, 2006.
the Global Fight against Outbreaks and Epidemics", Int J Health Geogr., 2020.

[41] L. K. Johnson, A. W. Dorn, S. Webb, S. Kreps, W. Krieger, E. Schwarz, S. Shprio, P. F. Walsh and J. J. Wirtz, "An ins special forum: intelligence and drones/eyes in the sky for peacekeeping: the emergence of UAVs in un operations/the democratic deficit on drones/the german approach to drone warfare/pursuing peace: the strategic limits of drone warfare/seeing but unseen: intelligence drones in israel/drone paramilitary operations against suspected global terrorists: us and australian perspectives/the ‘terminator conundrum’ and the future of drone warfare", Int. Natl. Secur., vol. 32, no. 4, pp. 411–440, 2017.

[42] A. Cavoukian, "Privacy and drones: Unmanned aerial vehicles, Information and Privacy Commissioner of Ontario", Canada Ontario, 2012.

[43] R. L. Finn and D. Wright, "Unmanned aircraft systems: surveillance, ethics and privacy in civil applications", Comput. Law Secur., vol. 28, no. 2, pp. 184–194, 2012.

[44] H. Du and M.A. Heldeweg, "Responsible design of drones and drone services: Legal perspective synthetic report", 2017.

[45] K. Wackwitz and H. Boedecker, "Safety risk assessment for UAV operation, Drone Industry Insights", Safe Airspace Integration Project, Part One, Hamburg, Germany, 2015.

[46] E. B. Carr, "Unmanned aerial vehicles: examining the safety, security, privacy and regulatory issues of integration into us airspace", Natl. Centre Policy Anal. (NCPA), 2014.

[47] R. L. Finn, D. Wright and M. Friedewald, "Seven types of privacy", European data protection: coming of age, Springer, 2013.

[48] R. Clarke, "The regulation of civilian drones’ impacts on behavioural privacy", Comput. Law Secur. Rev., vol. 30, no. 3, pp. 286–305, 2014.

[49] R. Majeed, N. A. Abdullah, I. Ashraf, Y. B. Zikria, M. F. Mushtaq and M. Umer, "An Intelligent, Secure, and Smart Home Automation System", Scientific Programming, 2020.

[50] Y. Zeng, R. Zhang and T. J. Lim, "Wireless communications with unmanned aerial vehicles: opportunities and challenges", arXiv preprint arXiv:1602.03602, 2016.

[51] D. Rudinskas, Z. Goraj and J. Stankunas, "Security analysis of UAV radio communication system", Aviation, vol. 13, no. 4, pp. 116–121, 2009.

[52] A. J. Kerns, D. P. Shepard, J. A. Bhatti and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing", J. Field Rob., vol. 31, no. 4, 617–636, 2014.

[53] S. H. Seo, B. H. Lee, S. H. Im and G. J. Lee, "Effect of spoofing on unmanned aerial vehicle using counterfeited GPS signal", J. Positioni. Navigat. Timing, vol. 4, no. 2, pp. 57–65, 2015.

[54] X. Lin, R. Wiren, S. Euler, A. Sadam, H. L. Maatannen, S. D. Muruganathan, S. Gao, Y. T. E. Wang, J. Kauppi and Z. Zou, "Mobile networks connected drones: field trials, simulations, and design insights", arXiv Preprint arXiv:1801.10508, 2018.

[55] A. Abdallah, M. Z. Ali, J. Misic and V. B. Misi, "Efficient security scheme for disaster surveillance UAV communication networks", Information, vol. 10, no. 2, 2019.

[56] P. Ramon Soria, R. Bevec, B. Arrue, A. Ude and A. Ollero, "Extracting objects for aerial manipulation on UAVs using low cost stereo sensors", Sensors, vol. 16, no. 5, 2016.

[57] S. I. Kim, G. J. Lim and J. Cho, "Drone flight scheduling under uncertainty on battery duration and air temperature", Comput. Ind. Eng., 291–302, 2018.

[58] C. M. Tseng, C. K. Chau, K. Elbassioni and M. Khonji, "Autonomous recharging and flight mission planning for battery-operated autonomous drones", arXiv preprint arXiv:1703.10049, 2017.

[59] H. Du and M. A. Heldeweg, "Responsible design of drones and drone services: Legal perspective synthetic report", 2017.

[60] M. F. Mushtaq, S. Jamek, K. M. Mohand, S. A. Khalid and M. M. Deris, "Key Generation Technique based on Triangular Coordinate Extraction for Hybrid Cubes", J. Telecommun. Electron. Comput. Eng., vol. 9, no. 3–4, pp. 195–200, 2017.

[61] M. Erdelj and E. Natalizio, "Drones, smartphones and sensors to face natural disasters", DroNet18: Proceedings of the 4th ACM Workshop on Micro Aerial Vehicle Networks, Systems, and Applications, pp. 75–86, 2018.

[62] P. Velagapudi, S. Owens, P. Scerri, M. Lewis and K. Scyara, "Environmental factors affecting situation awareness in unmanned aerial vehicles”; AIAA Infotech. Aerospace Conference and AIAA Unmanned. Unlimited Conference, 2009.

[63] O. Westerlund and R. Asif, "Drone hacking with raspberry-pi 3 and wifi pineapple: Security and privacy threats for the internet-of-things", 2019 IEEE 1st International Conference on Unmanned Vehicle Systems-Oman (UVS), pp. 1–10, 2019.

[64] D. He, S. Chan and M. Guizani, "Drone-assisted public safety networks: the security aspect", IEEE Commun. Mag., vol. 55, no. 8, 218–223, 2017.

[65] A. Nayyar, B. L. Nguyen, and N. G. Nguyen. “The Internet of Drone Things (IoDT): Future Envision of Smart Drones”, First International Conference on Sustainable Technologies for Computational Intelligence, Springer, pp. 563-580, 2020.

[66] Z. Yin, Q. Song, G. Han, and M. Zhu, "Unmanned optical warning system for drones", Global Intelligence Industry Conference (GIIC 2018), 2018.

[67] R. Koslowski and M. Schulzke, "Drones along borders: border security UAVs in the United States and the European Union", International Studies Perspectives, vol. 19, pp. 305-324, 2018.

[68] M. O. Ozmen and A. A. Yavuz, "Dronecrypt-an efficient cryptographic framework for small aerial drones", in MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM), pp. 1-6, 2018.

[69] M. O. Ozmen, R. Behnia, and A. A. Yavuz, "IoD-Crypt: A Lightweight Cryptographic Framework for Internet of Drones", arXiv preprint arXiv:1904.06829, 2019.

[70] E. Bertino, "Data Security and Privacy in the IoT," in EDBT, pp. 1-3, 2016.

[71] M. F. Mushtaq, S. Jamek, A. H. Disina, Z. A. Pindar, N. S. A. Shaker, and M. M. Deris, “A Comprehensive Survey on the Cryptographic Encryption Algorithms,” Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 11, pp. 333–344, 2017.

[72] M. O. Ozmen, R. Behnia, and A. A. Yavuz, "IoD-Crypt: A Lightweight Cryptographic Framework for Internet of Drones", arXiv preprint arXiv:1904.06829, 2019.

[73] D. Hussain, M. A. Khan, S. Abbas, R. A. Naqvi, M. F. Mushtaq, A. Rehman and A. Nadeem, Enabling Smart Cities with Cognition Based Intelligent Route Decision in Vehicles Empowered with Deep Extreme Learning Machine, Computers, Materials & Continua, 2020.

[74] Z. Lv, "The security of Internet of drones", Computer Communications, vol. 148, pp. 208-214, 2019.