International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

INTERNET OF DRONES

Miss. Sakshi. Ravsaheb Nikam, Miss. Rubeena Rasheed Makhamalla, Miss. Shivani Shivaji Pujari, Prof. Ms. Kalpana. N. Rode (SITCOE)

Email: knrodesit82@gmail.com, nikamsakshi05@gmail.com , rubeena24makhamalla@gmail.com , shivani10112001@gmail.com

ABSTRACT

The Internet of drones (IoD) can be described as an infrastructure designed to provide control and access over the Internet between drones and users. In reality, drones are rapidly becoming readily available commodity items, allowing any user to fly different missions in controlled airspace using multiple drones. Although technology helps mass-produce the onboard components of unmanned aerial vehicles (UAVs), including processors, sensors, storage and battery life, the performance limitations of these components impede and reduce expectations. IoD offers drones coupling vehicle as well as cloud mobility functions to allow remote drone access and control, as well as seamlessly scalable offloading and capabilities of remote cloud storage illustrates the IoD environment that includes base stations, signal link, and cloud environments.

***Keywords**: Internet of Drones (iod), Devastating, Hurricanes, Taxonomy, Unmanned Aerial Vehicles (uavs), GPS, ATC, FAA, ARTCC, MTSO*

1. INTRODUCTION

The uses of unmanned aerial vehicles or drones are a valuable technique in coping with issues related to life in the general public's daily routines. Given the growing number of drones in low-altitude airspace, linking drones to form the Internet of drones (IoD) is a highly desirable trend to improve the safety as well as the quality of flight. However, there remain security, privacy, and communication issues related to IoD. The key requirements of security, privacy, and communication and we present taxonomy of IoD based on the most relevant considerations. Furthermore, we present the most commonly used commercial case studies and address the latest advancements and solutions proposed for the IoD environments. Lastly, we discuss the challenges and future research directions of IoD.

The Internet of Drones is an architecture designed for providing coordinated access to controlled airspace for unmanned aerial vehicles (UAVs), often referred to as drones. With the on-going miniaturization of sensors and processors and ubiquitous wireless connectivity, drones are finding many new uses in enhancing our way of life. There are many applications for drone technology, ranging from the on-demand package delivery, to traffic and wild life surveillance, inspection of infrastructure, search and rescue, agriculture, and cinematography. All these applications share a common need for both navigation and airspace management. In this work, we lay the architecture for generic services that can provide such a foundation for all current and future applications.

2. HOW DO DRONES WORK?

Drones are a headline-making piece of technology, capable of capturing incredible video in the hands of skilled pilots and providing some serious internet entertainment when a dog mistakes one for a fris bee. We've watched drones perform record-breaking Super Bowl light shows, and looked on as they provided media coverage and relief assistance in the wake of devastating hurricanes.

With a joystick and a GPS system, the operations of most consumer drones seem no more complex than playing a video game. However, behind the easy user interface are an accelerometer, a gyroscope, and other complex technologies working to make the mechanics of drone flight as smooth as possible.

How do these mechanical features work? How does a drone actually fly? A little wireless technology and a whole lot of physics.

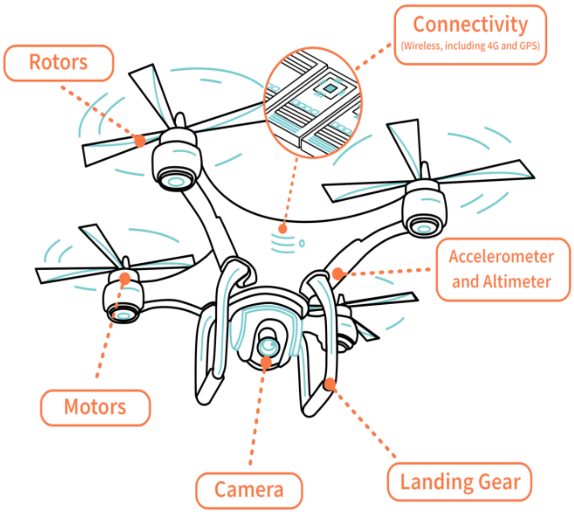

Fig.1.Drone Structure

Connectivity:

Drones can be controlled remotely, often from a smart phone or tablet. Wireless connectivity lets pilots view the drone and its surroundings from a birds-eye perspective. Users can also leverage apps to pre-program specific GPS coordinates and create an automated flight path for the drone. Another handy wirelessly-enabled feature is the ability to track battery charge in real time, an important consideration since drones use smaller batteries to keep their weight low.

Rotors:

A drone relies on rotors for its vertical motion. Drones use their rotors—which consist of a propeller attached to a motor—to hover, meaning the downward thrust of the drone is equal to the gravitational pull working against it; climb, when pilots increase the speed until the rotors produce an upward force greater than gravity; and descend, when pilots perform the opposite and decrease speed.

To hover, two of a drone's four rotors move clockwise, while the other two move counterclockwise, ensuring that the sideways momentum of the drone remains balanced. To avoid throwing its vertical motion off-kilter, the other two rotors on the drone will increase their spin. The same principle applies to moving forward and backwards—the rotors of the drone must apply thrust while making sure the spin of the rotors keeps the drone balanced.

Accelerometer and Altimeter:

An accelerometer feeds the drone information about its speed and direction, while an altimeter tells the machine its altitude. These features also help a drone land slowly and safely, preventing it from sinking into an air vacuum called a wash that could pull the aircraft down in an unpredictable way.

Cameras:

Some drones have built-in cameras onboard that allow the pilot to see where the drone is flying without having a direct line of sight to the device. Drone-mounted cameras help users see difficult-to-reach locations and can be a game-changing tool for first responders, especially in search-and-rescue scenarios.

The intricate engineering that goes into building drones means that pilots don't need to worry about balance, thrust, and other complexities, and can just enjoy the act of flying them. The ultra-responsive nature of the machines, which will only be heightened with 5G, even allows experts to race drones through high-speed obstacle courses.

Drones are versatile pieces of equipment that harness the power of wireless technology to do everything from taking video to assisting in emergencies. And their utility is only going to grow as the technology evolves and the world becomes more connected. You can learn more about the transformative potential of drones.

3. RELEVANT NETWORKS

For designing the architecture of the IoD, we study three distinct large scale network structures; namely air traffic control (ATC), cellular network, and the Internet. Each of these networks achieves some of the goals or functionalities we desire for the IoD. In each case, however, their conceptual architecture falls short of providing a thorough solution to the unique challenges of IoD. Hence, the importance of studying these systems is twofold. First, they have valuable lessons about how a scalable and fault tolerant network can be engineered. Second, their differences guide us to IoD's specific challenges which have not been tackled before and are in need of innovative solutions. We describe these structures through a discussion of goals and functionality that are relevant to IoD and the differences with IoD that need to be addressed in our architecture.

A. AIR TRAFFIC CONTROL NETWORK

ATC has strong relevance to IoD as efficiently utilizing the airspace and maintaining collision free navigation is an integral part of any IoD architecture. The functioning of ATC follows similar procedures around the globe. We briefly summarize the components of ATC in the United States. The Federal Aviation

Administration (FAA) is in charge of regulations and air safety, and has partitioned the United States' airspace into 24 areas each managed by one of the 24 Air Route Traffic Control Centers (ARTCC). There are bilateral letters of agreement between any two adjacent ARTCCs on how aircraft must transition from one ARTCC to another. Similarly, within each ARTCC, the airspace is partitioned into between 20 to 80 sectors and each sector is exclusively managed by one controller and the aircraft

B. CELLULAR NETWORK

In the cellular network, the coverage area is partitioned into most commonly hexagonal cells forming a honeycomb pat tern. The communication signals in each cell are sent to and received from the mobile users by a dedicated base station. Each base station uses a certain frequency which is different from the near base stations frequencies to minimize the interference. The range of signal for each base station determines the size of each cell. Each base station can only carry a certain amount of calls over its frequency channel. As such, the main driver in determining the size of each cell is the expected number of mobile users in the region. Hence the densely populated downtown areas can have many smaller cells whereas in the rural areas, fewer cells with higher range are used. Each of the bases Office(MTSO). The MTSO is in charge of periodic localization of the mobile units and assigning a base station to them. Furthermore, it assigns channels to each call and performs the task of handoff or handover which is basically the transfer of responsibility for a moving mobile unit from one base station to the other base station as it enters a new partition. We will later use the same word in the context of IoD.

C. INTERNET

In the Internet, the goal is to connect networks of computers together, so all the computers on the world-wide network can communicate. The Internet has a layered architecture consisting of five layers .Layering makes it easier to solve the problem that the Internet addresses by separating concerns. Each of these layers is to be thought as a service and upper layers use the services of lower layers. For example, the link layer is concerned solely with the transfer of data on a single communication link or between two adjacent nodes and the physical layer is concerned with the physical means for transferring signals through various mediums, such as air (in case of WiFi) or Ethernet cables. The Internet layer, relying on the connectivity provided by the link layer is concerned mainly with routing or forwarding data packets between any two nodes potentially on two different local networks through the use of standard global addressing as a best effort service rather than a reliable one. This is achieved by routers which locally make a decision about forwarding the data packets they receive to one of the immediately connected networks. Utilizing the universal unreliable connectivity provided by Internet layer, the transport layer is concerned with tasks such as the reliability of transmission and congestion control. Finally, the application layer, uses this global and (if needs be) reliable connectivity for various applications like Web, Email, VoIP, Remote Login, etc. Such a decentralized and deliberately simple architecture has made the Internet a unique engineering feat in that it scaled by many orders of magnitude. Readers can refer to for a comprehensive treatment of the subject of the Internet and to and for discussions of the philosophical guidelines in its design.

4. REQUIREMENTS OF INTERNET OF DRONES (IOD)

The expected increase in the use of drones in a variety of applications could expose operators to a whole new array of risks, particularly damages to third parties and liability. Several of the requirements for potential drones are presented and classified in the following sub-sections. Figure shows the key requirements of IoD.

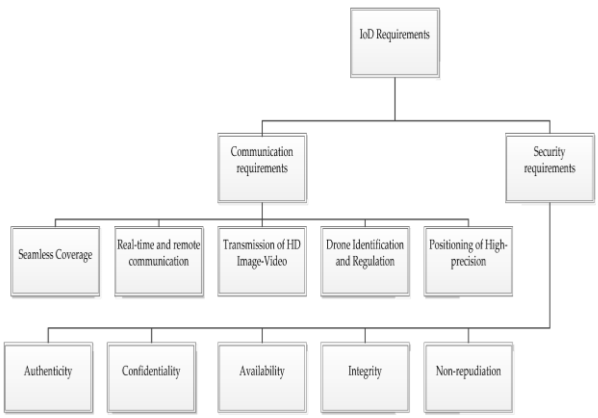

Fig.2.Key Requirement of IoD

4.1. Communication Requirements

The impact of IoD communication vulnerabilities is receiving increasing attention from researchers. Many remote locations would be hard to reach were it not for the usage of drones. As a result, drones are commonly employed for important tasks such as rescuing victims, providing surveillance, transportation, and helping with conserving and protection of the environment. Therefore, critical communication requirements to support the different drone applications are discussed as follows.

a. Seamless Coverage

Hot-spot coverage (stages, tourist areas, and industrial areas) is appropriate for aerial entertainment. Widespread coverage in suburban, urban, and rural areas is required for the inspection and logistics of power or base stations. In the future, seamless drone coverage will become more essential for network planning. Unlike conventional network coverage serving mostly land users, enhanced sky coverage is required to support drone users flying at different heights.

Coverage of up to 10 m altitude is appropriate for plant protection (e.g., spraying of agricultural chemicals). Coverage of up to 50 to 100 m altitude is required for power line inspection. Coverage of up to 200 to 300 m altitude is sufficient for mapping of agricultural lands, while coverage of the upper air pipeline of up to 300 to 3000 m altitude may be needed. It is difficult for networks to serve this large spectrum of coverage scenarios at varying altitudes.

b. Real-Time and Remote Communication

Real-time and remote communication capabilities permit remote controllers to issue a time-based command and control instructions on the basis of the drone flight status report in real-time, such as space co-orders and equipment status. Real-time and remote controls are primarily used in the monitoring of flight conditions, drone task, and equipment and emergency control. The latency and rate of certain data requirements should be met to allow remote control for drones. The downlink (from the base station to drone) data rates in many application scenarios are about 300–600 kbps, and the existing 4G+ networks will fulfill this requirement. For potential implementations, such as remote real-time operations, the latency criterion is strict to guarantee the precision and experience of service.

c. Transmission of HD Image/Video

Networks should be able to provide a high uplink (from the drone to the base station) data rate for drones to permit the transmission of HD image/video. The data rate required is calculated mainly by picture/video size and quality.

In the future, the demand for higher resolution images/videos in vertical industries needing 4K/8K HD video support would need a higher Gbps-level data rate. The 5G networks are well equipped to support such services with a data rate requirement of multi-Gbps. Transmission of HD image/video will dramatically extend the drones' application scenarios including energy and power line inspection, agricultural exploration, control and rescue, entertainment and monitoring. With high transmission rates, drones linked to networks are able to transmit HD images/videos to enable the immersive experience of augmented reality and virtual reality.

d. Drone Identification and Regulation

Mobile networks may help identify and control drones by supporting drone registration, tracking, provision, and coordination.

- **Registration:** Identifying but standardizing the drone equipment number, serial number, and flight control serial number helps track the whole process orderly from initial drone production to in-use. Through standardizing registration of drone users, owners and mobile networks, drone users and owners can be legally monitored.
- **Monitoring:** Drone connections and data communications can be detected and monitored through mobile networks. Drone implementations can be completely tracked in real-time with additional regulatory protocols.
- **Forecast:** Flight situations can be dynamically evaluated and early warning of possible risks can be achieved by tracking drone positions and monitoring the flight traffic and path.
- **Coordination:** Knowledge exchange between industries and different companies can be carried out by approved oversight of all vertical industries involved.

e. Positioning of High-Precision

For numerous drone applications, positioning is critical. In several drone applications, vertical positioning also is important, in addition to traditional positioning on the horizontal plane. The requirement for positioning accuracy will increase from tens of meters to sub-meters with the drone applications' development. Fifty meters positioning precision is adequate for regular monitoring activities. Applications such as agricultural land mapping and automated loading involve high precision positioning at the sub-meter.

4.2. Security Requirements

Researchers have created several security and privacy approaches to secure the Internet of drones (IoD) network to protect the location of unmanned aerial vehicles (UAVs) and the privacy and security problems that come with using the IoD network. Due to these localization errors, drone positioning was previously unreliable, which had disastrous implications for the whole IoD network. Another critical aim of the IoD network is to increase the level of security and privacy to a point where it cannot be compromised. Therefore, the main requirements of security and privacy of the IoD network include authenticity, confidentiality, availability, integrity, and non-repudiation:

a. Authenticity:

Authentication is required for sensing devices, users, and portal nodes before access to a limited resource is enabled or essential information is disclosed. In addition, for communicating entities to have mutual authentication, two of the communicating entities have to be a monitoring drone and a ground-control station. To guarantee full forward secrecy, it is essential to employ a secure key exchange using a method that produces session keys that are impossible to recover.

b. Confidentiality:

Confidentiality or privacy of the wireless communication channel protects from the unauthorized disclosure of information. Another significant barrier to IoD implementation is making data available, and controlling access to that data (data confidentiality). For instance, when a group of drones collects road traffic data from several places, there is a continuing problem in sharing this data safely and effectively.

c. Availability:

Registered users should also be granted access to appropriate network services in conjunction with system denial-of-service attacks. Both the mechanism and the system are capable of recognizing if a drone is engaged in combat and keeping track of the battle limit, which governs whether the flight management system can pick up on a malfunctioning drone and determine if the availability criteria are compromised.

d. Integrity:

Integrity is essential to guarantee the trustworthiness of the information (for example, that it has not been altered in transit, and the source of the information is genuine).

e. Non-Repudiation:

The goal is to ensure that a criminal organization does not conceal its actions. In fact, when there are several parties conducting an action, one of the necessary security measures is to make sure that the action cannot be rejected without the others' knowledge.

5. CHALLENGES AND FUTURE RESEARCH TRENDS

This section highlights the most crucial challenges and future research trends on the Internet of drones.

- **Privacy and Security-Related Challenges:**

Since government agencies grant licenses for drone usage in civilian and commercial applications, the modern IoD is equipped with numerous connected sensor devices. These devices are vulnerable to various threats including hijack, human error, and loss. These issues should be given higher priority in the design of drone applications.

- **Global Resource Management-Related Challenges:**

Resource distribution is critical in serving productivity and reducing cost and can be divided into two groups, the global allocation of resources and local allocation. Global concerns concentrate on the expenditure spent on the global resources of time, energy, and equipment. In addition, the maximum global productivity can be deployed by various equipment in the Internet of everything (IoD), such as edge computers, cloud servers, and UAVs. Under digital media transmission in IoD, global efficiency can be increased by networking algorithms and video coding. Energy and power are allocated for every role based on committed performance. For instance, in a smart building scenario (such as in a local network), an efficient data collection algorithm is good for increasing the user's data rate. In addition, for the flying terminals, the energy management system is essential for making use of limited energy. This is the concept of allocating resources at various nodes.

- **Sensor Communication-Related Challenges:**

The IoD sensor's communication protocols are designed with lightweight and highly sensible objects which have a substantial chance for data loss or receive the wrong data from other nodes. Furthermore, sensors face routing issues when communicating with multiple drones with a network center. Some of the drone manufacturers use cheap hardware components which increase the chance of other network communication issues namely, high throughput, latency, and delay between the device and center. To address these issues, next-generation network technologies such as 5G, intelligent routing, narrowband-Internet of things, LoRa-based IoT systems, Sigfox, NB-IoT, and LTE-M need to support connection choices in the future. Lastly, the standardized policy should be developed to use the authorized component for drones' communication protocol.

- **Drones Distribution and Deployment-Related Challenges:**

Apart from data confidentiality, data sharing and access control are challenges that face IoD deployment. For instance, in the application where a set of drones can collaborate to collect road traffic data of different regions, how to securely and efficiently share these collected data (e.g., in the sense that only authorized entities have access to the data) remain an ongoing challenge

REFERENCES

[1] file:///C:/Users/SERVER/Downloads/IEEE_Template.pdf

[2] https://www.ctia.org/news/up-up-and-away-how-do-drones-work

[3] https://docs.google.com/document/d/1Pn2Z6fznv29UI_op5yrzYYnaU57JFqAahcVMsuYbkQw/edit

[4] https://www.mdpi.com/1424-8220/21/17/5718/htm

[5] https://www.google.com/search?q=dark+colourful++drone+icon+png&tbm=isch&ved=2ahUKEwj9soeSr_f2AhVogmMGHa7fB8AQ2-cCegQIABAA&oq=dark+colourful++drone+icon+png&gs_lcp=CgNpbWcQAzoHCCMQ7wMQJ1C5CViXN2DGOWgAcAB4AIABaIgBpAmSAQM1LjeYAQCgAQGqAQtnd3Mtd2l6LWltZ8ABAQ&sclient=img&ei=akxJYv3VFeiEjuMPrr-fgAw&bih=789&biw=1583&rlz=1C1YTUH_enIN974IN974&hl=en

[6] https://mail.google.com/mail/u/0/?tab=wm#sent?projector=1

[7] https://scholar.google.co.in/scholar?q=research+paper+on+drone+technology+pdf&hl=en&as_sdt=0&as_vis=1&oi=scholart