International Journal of Research in Advent Technology, Vol.9, No.9, September 2021
E-ISSN: 2321-9637
Available online at www.ijrat.org

Distributed Cellular Framework for Secure Drone Delivery Services

Maansa Krovvidi, Ch Mvn Sai Teja Prashanth

Abstract— This paper describes in-depth the architecture of a Distributed Cellular framework for Secure Drone Delivery Services with an additional security layer. Delivery Drones are Unmanned aerial vehicles (UAV) that are responsible for the transportation of goods from one place to another place. In the modern world, with several e-commerce platforms, everything is traded, promoted, advertised online. This causes the need to deliver the packages rapidly and within a stipulated period of time. Unmanned aerial vehicles or drones come into the picture to retort the above-mentioned issue. Security nowadays has become a major concern where hackers are diverting the network traffic, hijacking, and crashing the drones. In order to prevent these attacks from taking place, this paper proposes a strong security framework to minimize these attacks from taking place. The proposed architecture has an additional layer of security which covers the two-factor and multi-factor authentication at the delivery spot. There exists an integration of different sensors like Obstacle detection, SOS detection, Facial Recognition, etc. Beyond the security framework, a distributed cellular network is applied to the delivery services to scatter the drones cell-wise and largen the scope to all remote areas.

Index Terms—UAV, Cellular, Security, SOS, Drone.

I. INTRODUCTION

Drones have become ubiquitous in the present day. The emergence of drones in various fields like military, agriculture, defense, safety surveillance, delivery services, aerial photography, calamity detection, hospitality, food delivery, weather forecasting, law enforcement agencies, disaster management, etc [1]. In recent times, (UNICEF) United Nations children's fund has proposed usage of drones to combat COVID-19 by monitoring public space for any unusual activity, aerial spraying of disinfectants in public spaces, transporting medical kits and necessary aid to remote areas during lockdown period [2]. Thus, it is evident that deployment and research in drone technology are prevailing across the globe. Drones come under Unmanned aerial vehicles (UAV), which are airborne systems that can be remotely operated by a person or autonomously maneuvered with an embedded system on board with the integration of multiple sensors. UAVs are small in size which helps to navigate in remote areas, these UAVs are different from ground vehicles due to the three-dimensional coordinates in space [3].

Manuscript revised on September 29, 2021 and published on October 10, 2021

UAVs carry multiple sensors based on the mission. Drones can be grouped into nine categories, such as fixed-wing, flapping wing, rotary-wing, tilt-rotor, ducted fan, helicopter, ornithopter, and unconventional types [4]. Classification of drones based on utility is discussed below:

- ***Defense and security:*** Drones are the most significant and lifesaving technology in anti-terror operations they are equipped with High Definition and infrared cameras which can provide 360-degree coverage for analyzing the targets.

- ***Infrastructure Monitoring and Inspection:*** Nowadays visual inspection is performed in almost every industry which is carried out by drones. And drones collect the visual data conditions on an asset instead of using manpower physically [5].

- ***Emergency:*** Emergency response teams are often working against the clock and in conditions that greatly reduce their mobility across the ground and can be deployed in an instant to respond to emergencies. During Covid-19, we see unmanned aerial vehicles (UAVs, or drones) being used for critical services. These include monitoring crowds, disinfecting contaminated areas, thermal screening of groups to detect fever, broadcasting information, and delivering medical supplies [6].

- ***Drones in Forestry, fisheries, and wildlife protection:*** It is known that flora and fauna are monitored continuously with the help of satellite imagery. But the major drawback with satellites is lesser resolution due to cloud coverage. This drawback is combated with drones as they can move swiftly to whatever height is required and calculate canopy height, fire detection, forest management, etc. Controlled fixed-wing UAVs with thermal and hyperspectral sensors integrated are used in this domain [7].

- ***Delivery services:*** Delivery drones are logistical devices that carry materials from a retail outlet to their consumer's location. Delivery drones are mainly used for delivering commodities or objects, this is because this device delivers faster due to its accurate locating program [8]. Delivery drones have become very popular lately as they can access remote areas too. These are cost-effective in nature and consume less power as they are battery operated. Amazon Prime Air, DHL delivery services, Apple, and many other companies are currently researching and performing test drives on drone delivery. By 2023 it is said that there will be wide-scale manufacture of drones to deliver various

doi: 10.32622/ijrat.99202103

commodities.

II. DRONE ATTACKS

The emergence of drones has led to many threats. In recent times, drones have been deployed to drop explosives, to trigger bomb blasts, used as spybots for surveillance purposes, etc. The most common threats that are prevailing apart from the ones mentioned above are drone hijacking, the man-in-the-middle attack, eavesdropping, de-authentication, etc. Mainly Drone attacks are classified into Physical and Logical.

A. Physical Attacks

- ***Privacy:*** Drone privacy is a primary concern for everyone nowadays, as they fly continuously everywhere on a timely basis with continuous real-time capturing of audio and videotapes. This may lead to data loss and proctoring of public activities.
- ***Smuggling:*** Smuggling is a very dangerous attack and the usage of drones for an illegal purpose is an offense. According to BBC News, wherein this attack they used to send drugs, phones, and even blades to highly secure prisons avoiding ground detection. Using drones in this way is prohibited according to law.
- ***Airstrike Disruption:*** In this attack octo-copter drones are used which are capable of lifting up to 20bls, attacks include crashing the drones into public or creating self-destruction drones to damage property. This is mainly used by the army to carry out heavy objects in battle combats and drones have the power to diffuse the bombs or pick them and drop the bomb at a safer place.
- ***UAV-Surveillance:*** This technique is mainly used by terrorists to capture raw video and audio content using high-end cameras. This is mainly used to plan an attack in a particular place at a particular time or for potential future attacks.

B. Logical Attacks

- ***Fake Access Points:*** This technique is used to create a fake mobile Wi-Fi network or points wherein the actual users are connected to the fake networks stating as "Free Wi-Fi" points, by doing so the sensitive information such as usernames, passwords can be captured.
- ***Hijacking:*** This is attack is used to Hijack the nearby drones by using programmed devices such as raspberry-pi. This is attached to the drone by programming it to intercept and hijack the drones, by regular drones have been hijacked and converted into a destructive drone.
- ***Phishing:*** Nowadays there are devices such as pineapple which are developed by security professionals used to perform automated Wi-Fi auditing. But these devices are used by hackers and the whole network traffic is been diverted via phishing emails and messages. [9] [10].
- ***Spoofing:*** The most dangerous attack nowadays is a spoofing attack. Most of the drones rely on the Global Positioning System for navigation. Attackers are using devices such as Hack-Rf and trying to spoof the GPS system which causes serious damage to Hospitality and Food delivery systems. [11].

III. SECURITY ISSUES IN DRONE

There exist many challenges in terms of security, privacy, and authenticity. In this section, the major challenges faced are discussed.

A. Physical challenges

In general, drones are power efficient in nature, as they utilize lithium-ion batteries which do not consume a lot of power, but the drawback is the motion control and speed control [7]. This can be combated with the deployment of a sensor network with will be discussed further in the proposed security framework. Due to the unpredictable weather conditions, there might be flight failure at any given time, thus a backup is required which is implemented by swarm flight of drones. The extreme weather conditions can lead to flight failure as discussed above which indeed increases the cost of maintenance. Majorly drones are operated by humans and not fully automatic in nature, this tends to reduce efficiency and restricts from taking smart decisions.

B. Data

Fully autonomous drones are smart devices with giving a 360-degree overview of the environment and the dynamics. Since there is continuous acquisition and transfer of data taking place, there is always a threat to the integrity of the data. The data collected can be user-specific, location-specific, environment-specific. User-specific might consist of personal details, name, address, contact details, email ID, financial information, apart from this there is data pertaining to the features and dynamics of the drone to be delivered. Thus, special hashing algorithms need to be used to ensure data integrity.

C. Position/Location

The most important concern when coming to delivery drones is knowing the exact point of delivery. An accurate GPS system must be mounted on the drones to receive continuous GPS signals. These signals are prone to noise and interference [7]. Deliberate miscommunication can take place regarding the location. There are chances of connection being lost, drone crashing into other objects, air traffic amongst other drones. As a result, proper crash avoidance methods and proper routing must take place to restore the authorization.

D. Sensor network

There are a multitude of sensors including, GPS, temperature sensor, motion sensor, thermal sensor, accelerometer, gyro sensors, etc. It is important to keep in mind the effect of temperature and other climatic conditions on the sensors. The reliability and liability of the sensors shouldn't be lost as accurate readings will help in the smooth navigation of the drone. Improper calibration of these sensors can result in serious damage to the drone as well as the product being delivered by the drone. Especially in covid.

doi: 10.32622/ijrat.99202103

IV. DRONE COMMUNICATION ARCHITECTURE

The usage of drones has become a useful technique to combat major issues during the pandemic by fulfilling the demand of the general public need and simultaneously providing access to basic amenities in remote areas. In general, Unmanned Aerial Vehicles and drones fly or function at altitudes within the troposphere [12], with the number of drones escalating year by year the communication and control of drones have become an issue of concern. As a result, the connectivity of drones is most desirable to ensure the safety and quality of drones [13].

Figure 1 represents the basic communication architecture in drones, which includes a Ground Control Station, Base station, WSN, Drone.

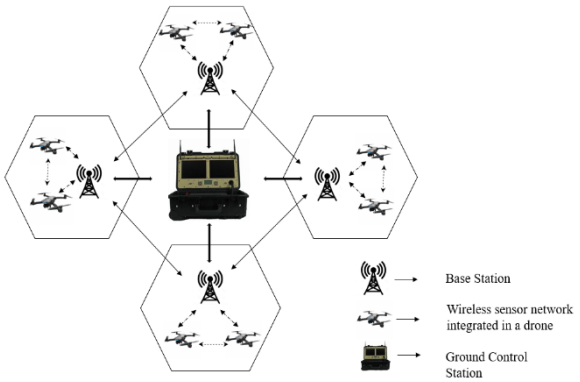

Fig. 1.Drone Communication Network.

A. Ground Control Station:

To ensure seamless communication among the drone network a ground control station (GCS) is required. Ground Control Station is a generic system designed for controlling the drone and monitoring its minute activities. Mainly these are the building blocks of Ground-based hardware and software components that trigger drones for communication. The main components in GCS are the Ground station, Base station, and integrated wireless sensor drones. The GCS is capable of controlling the UAV or drone directly or providing an allowance to autonomous operation where the drone can independently take actions without the GCS's intervention [14]. Ground control stations are specific to the type of drone in use. The heart of the GCS is a processing unit that is responsible for all the operations. There exist a wide variety of Ground control stations from lightweight handheld to portable double screened GCS [15]. Flight control, maneuvering, flight speed, toggling, flight locations, etc., are controlled and monitored by the GCS. There exist a radio unit that is responsible for the data link communication between UAVs, drones, Wireless sensor network (WSN).

B. Communication Network:

The communication between the drone and the ground station is established by MAVLink, a widely used communication protocol for drones [14]. The most widely used communication protocol used in drone communication is micro air vehicle link (MAVLink) helps in the bidirectional communication between UAV and ground stations. This protocol is deployed mostly with ArduPilot and PX4 and provides powerful features not only for monitoring and controlling. The MAVlink communication protocol consists of a set of messages which are shared between the GCS and the drone. This protocol uses a double checksum verification in the packet header to verify the integrity of the messages. At the same time, the communication protocol is responsible for the transmission of the packets into various layers of the TCP/IP model on the internet. The pipelining of the data packets, serializing the packets in order enables data transmission through various low data rate frequencies, Wi-Fi, Ethernet, etc. The frequency bands used for data transmission are 433 MHz, 868 MHz, 915 MHz, or 2.4GHz [16,17].

C. Base Station:

The Base station acts as a radio transmitter and receiver between various users in a wireless communication network. Similarly, in a drone communication network, the Base station acts as a mediator between the drone and Ground Control Station to exchange data. This results in a reduction in network traffic. Since there exists a single ground control station to monitor and control the drone network, a distributed cellular framework of base stations will ease not only the network traffic but also improve latency, data transmission, and availability. Various Base stations are connected to the core Ground control station and are not sole decision-makers in the communication framework. The Base station consists of an antenna unit, RF unit, Baseband unit, etc. Base stations are integral to any communication network specific to a drone network since it is not possible to have a Ground Control Station positioned in a remote area [18].

D. Wireless sensor network integrated into Drone:

The integration of Unmanned Aerial vehicles with wireless sensor networks has become the state-of-the-art solution for large-scale monitoring and controlling. This hybrid architecture results in real-time continuous data processing from ground to air. This collaborative approach leads to an improvement in reliability, latency, and accessibility. In order to maintain rapid, obstruction-free motion of the drone WSN plays a vital role by sending continuous packets of data to the controller or central operating system. The merge between WSN and UAV boosts energy-saving leading to a more efficient network. The synchronization between the radio network present in WSN and UAV is vital for seamless communication and continuous streaming of data to the ground station. The WSN architecture consists of several sensor nodes centered with a cluster head responsible for collecting data and sending it to the user [19].

V. DRONE DELIVERY ARCHITECTURE

The advent of technology in the past decade has opened a wide range of opportunities and scope for drones. Apart from

doi: 10.32622/ijrat.99202103

military surveillance, drones are also used for delivery purposes. A delivery drone is a UAV used for shipping packages of food, medical supplies, and other products. In recent times many companies have begun drone delivery services including Apple, Amazon, FedEx, etc. The main responsibility of delivery services is to transport packages from sellers to customers safely. Here lies the concept of trustworthiness, but at times this factor remains at risk and several security frameworks have been proposed to ensure the safety of the package and personal details. Cryptographic techniques have been proposed to avoid white-box attacks and to safeguard the delivery drone from any physical attack [20]. But, apart from providing protection to the package and drone another concern is the product details, personal details which are also at risk. Amidst the pandemic time, there are various other concerns as well which are discussed further in the proposed framework.

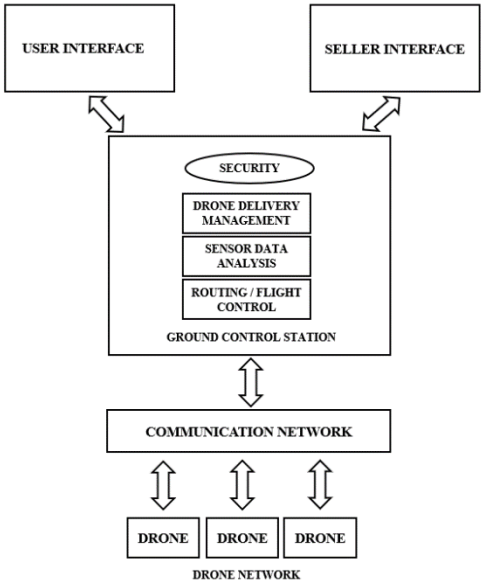

Fig. 2.Stagewise Delivery Block Diagram.

Figures 2 and 3 describe the overall flow of package delivery in the pipeline from the first stage to the final destination.

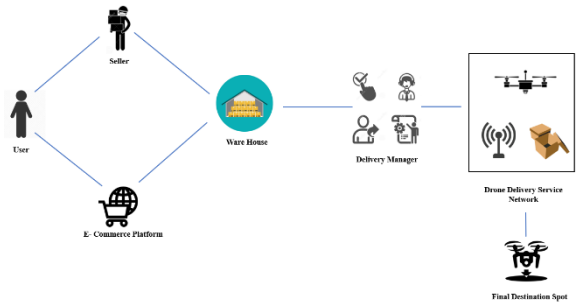

Fig. 3.End-to-End Drone Delivery Service.

As shown in Figure 3 architecture includes five basic components as User interface, seller interface, Ground Control Station, Communication Network, and Final Destination spot.

User Interface*:* This is the first phase in the architecture where the user had to purchase commodities virtually via electronic devices and needs to confirm the products to be delivered to the provided address. The confirmed product will be passed to the next phase and the user receives the receipt of payment on the delivery spot.

Seller Interface**:** In this interface, the request is been initiated as per the customer-selected product and the exact product is been processed to the customer delivery address with E-Receipt printed and the information is also is been transferred to Ware House.

Ware House/Store*:* In this warehouse, the final dispatch product is been verified and checked whether the product is present or not and then sent to the Delivery Manager for further process.

Delivery Manager**:** The Delivery Manager is the drone manager. Here the verification is done thoroughly whether the correct products are processed or not. The delivery manager is responsible for the drone delivery to the respected addresses requested by the customer, depending upon the size and weight of the product the particular drone is selected for their delivery. The drone delivery management system is integral to the Ground control station and makes decisions on the selection and monitoring of drones with respect to the order received.

Drone Delivery Service Network**:** The drone delivery service network is responsible for transporting the package to the concerned customer upon receiving instructions from the Drone delivery management system. The allotted drone in the service network approaches the warehouse, collects the package, and heads towards the addressed location of the customer with the help of the Global Positioning System.

Final Destination Spot*:* This is the final phase of delivering the commodities to the customers. The products after delivery are returned to the final destination and ready to take the next delivery flight.

VI. PROPOSED DRONE DELIVERY SECURITY ARCHITECTURE

Various drone attacks like hijacking, smuggling, phishing, white-box attack, and surveillance attacks have been discussed earlier in the paper. Thus, the need to safeguard privacy, ensure seamless delivery and simultaneously preserve the integrity of the system arises. Initially, drones have played a key role in military surveillance and other civilian activities, but at present as the demand for drone technology is proliferating steadily the need for drone delivery services comes into action. Drone delivery services can tackle issues such as pollution, access to remote areas, rapid transportation, and most importantly in the midst of the COVID-19 pandemic the need for contactless delivery from the seller to the customer has emerged.

The three main concerns for communication are capacity, the number of users, and limited bandwidth. These issues have

doi: 10.32622/ijrat.99202103

been taken care of by the concept of cellular networks, frequency reuse, etc. The distribution of area into cells has led to proper management of frequency spectrum and improved the system capacity. In this paper, a distributed cellular framework for drone delivery services is proposed. The below Figure 4 describes the architecture and process of delivery.

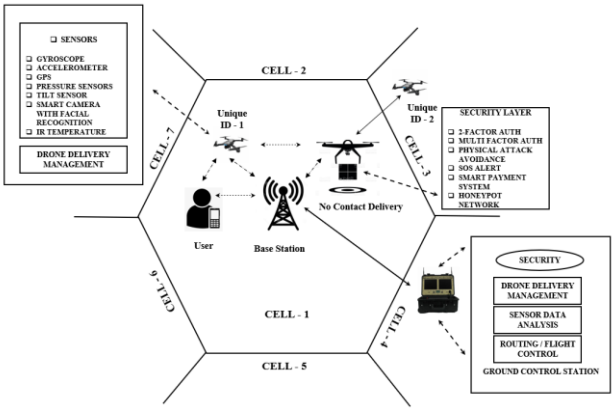

Fig. 4.Proposed Drone Delivery Security Architecture.

A. Proposed Delivery Framework:

According to the above Figure, 4 cell-1 consists of a Ground station, Base station, user interface, inter and intra drone communication, and a no-contact delivery drone. The overall area is distributed into cells as the figure describes. All the drone-to-drone communication taking place within a particular cell is regarded as inter drone communication, where all the traffic lies within the cell structure. This distributed network ensures rapid transportation and efficiency in delivery management. The first stage in the delivery service involves placing the order by the User/Customer with the help of an electronic device (Laptop, Smartphone, etc) virtually which the intern sends the request to the ground control station. In a specific cell, the number of drones allotted for delivering packages (food, medicinal equipment, etc) remains fixed. As soon as the order is placed, it is alerted to the Drone delivery management system as well as the seller.

The Ground control station is a core integral part of monitoring and controlling drones. The GCS is not present in each and every cell, but only sends commands, instructions to the Base station and the drones. The GCS is solely responsible for supervising and smooth management of the delivery service. When an order is placed, the GCS acknowledges the order received and allots a drone closest to the delivery location. This is done with the help of a base station present in the cell nearing the delivery address. Each drone is differentiated from another with its unique ids, such as IP address or MAC address. Upon receiving the order, the Delivery management system orders for a particular drone in that cell to collect the package from the Ware House or store, this communication takes place with the help of the radio unit present in the Base station. BS is responsible for transferring instructions and command signals from GCS to the Delivery drone.

In this way all areas can have access to drone delivery services including remote areas and faster delivery is assured. By doing so, the system capacity and channel capacity are efficiently utilized. It is previously mentioned that the frequency bands used for data transmission are 433 MHz, 868 MHz, 915 MHz. These bands will not interfere with the frequency bands of Wi-Fi communications which range from 900Mhz, 2.4GHz, and up to 60GHz. Thus, the frequency spectrum is utilized to the maximum extent and reduces the possibility of interference.

In a particular cell when there is an insufficient drone requirement, this message is transferred to the neighboring cell's base station and a service drone is borrowed based on the requirement. Thus, avoiding delays in delivering the product. Drone to drone communication is also important in this distributed framework to avoid obstructions or interference between the drones. The drone communication within a cell is termed as inter drone communication and in order to communicate information pertaining to the nearby cell, intra drone communication is used.

In delivery services, the drones employed have a wide variety of sensor networks integrated into them. The most common sensors used in drones are the tilt, accelerometer, gyroscope, and air pressure sensors. The tilt sensor is used to avoid obstacle collision and detour to the landing spot without any deviation. The gyroscope sensor is a device that is used to measure and maintain the orientation and angular velocity of the drone to ensure steady movement. In order to measure the acceleration, whether the drone is in a static or dynamic position the accelerometer is used. In order to know the coordinates of any drone, the most important is the Global Positioning System. It is the main component in the drone architecture where it provides the exact location of the source and destination address of the customer. Apart from the basic sensors, in the proposed framework a facial recognition sensor is also embedded to ensure the integrity and security of the product being delivered to the concerned customer. The facial recognition camera scans the particular product before the flight and verifies with the customer at first. Later, during delivery, the same product is re-scanned and cross-checked for re-assurance. Amidst the COVID-19 pandemic, social distancing is a key role to avoid the spreading of the virus. In red zone areas, with the help of a facial recognition sensor, it can be verified whether the customer is wearing a mask or not. IR temperature sensors are fundamental to know the temperature of any object with the help of reflecting Infrared waves.

B. Additional Security System:

In the Drone delivery architecture, additional security is added via two-factor and multi-factor authentication. In two-factor authentication the barcode is scanned before delivery to verify the user authenticity, additionally, in multifactor authentication, the customer image is taken along with the food or delivered goods and sent the image to the delivery manager for approval. During any physical attack scenario to the delivery drone, the SOS alert is initiated and sent to both the delivery manager and the nearest Law enforcement authority, and a delay request alert is sent to the

doi: 10.32622/ijrat.99202103

end-user. If there is any error or failure of the drone the delivery manager sends a substitute drone to the place and notifies the same to the customer. During the delivery, the smart payment system is launched where the difference amount is been saved via Bar code and a request is sent to the delivery manager. This difference is been used in the next delivery order.

Additionally, to overcome GPS spoofing, intercepting communication traffic, and Information disclosure a Honey pot network is installed. The Honey pot network acts as a duplicate security system by masking the actual network from unauthorized users thereby diverting the attacker.

VII. FUTURE SCOPE

Drones have been taking a part in many disciplines including farming, rescue drones for emergencies, health care, fire extinguishers, delivery, surveillance, video streaming, and many more. With the advancing 6G technology, drone communication will become faster and more reliable. The main aspect of drone delivery services is to reach the last mile which will solve many world issues and improve globalization to a greater extent. This pollution free technology will open doors to more sustainable development in the field of technology.

VIII. CONCLUSION

In this paper, integration of security and distributed cellular framework is proposed for drone delivery services to maximize the system capacity, increase availability and ensure seamless communication. This reliable, sustainable, and efficient framework ensures vulnerable free drone delivery services.

IX. REFERENCES

[1] https://www.ijeat.org/wp-content/uploads/papers/v9i4s/A10020594S20.pdf
[2] https://www.unicef.org/supply/media/5286/file/%20Rapid-guidance-how-can-drones-help-in-COVID-19-response.pdf.pdf
[3] Magdi S. Mahmoud, Mojeed O. Oyedeji, Yuanqing Xia, Chapter 9 - Path planning in autonomous ground vehicles,
[4] Shahmoradi, J.; Talebi, E.; Roghanchi, P.; Hassanalian, M. A Comprehensive Review of Applications of Drone Technology in the Mining Industry. Drones 2020, 4, 34.
[5] Mitka, Eleftheria & Mouroutsos, Spyros. (2017). Classification of Drones. American Journal of Engineering research. 6. 36-41.
[6] https://training.nidm.gov.in/Home/Download?q=UYA1RBFPVSU=
[7] Singhal, Gaurav & Bansod, Babankumar & Mathew, Lini. (2018). Unmanned Aerial Vehicle Classification, Applications, and Challenges: A Review. 10.20944/preprints201811.0601.v1.
[8] https://grinddrone.com/info/pros-cons-delivery-drones
[9] https://droneztogo.com/dronelife-exclusive-can-hackers-use-drones-to-steal-your-personal-data/
[10] https://www.techradar.com/news/what-is-phishing-and-how-dangerous-is-it
[11] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8114815/
[12] https://dronecenter.bard.edu/high-altitude-drones/
[13] Abdelmaboud, "The Internet of Drones: Requirements, Taxonomy, Recent Advances, and Challenges of Research Trends," Sensors, vol. 21, no. 17, p. 5718, Aug. 2021.
[14] Haque Nabil, Syed & Kormokar, Robi & Ashik, Akhlak Uz. (2017). Drone ground control station with enhanced safety features. 1207-1210. 10.1109/I2CT.2017.8226318.
[15] https://www.unmannedsystemstechnology.com/category/supplier-directory/ground-control-systems/ground-control-stations-gcs/
[16] https://beaglebluevoyager.com/understanding-mavlink-between-drone-and-ground-station-gcs-4g-lte-based/
[17] A. Koubâa, A. Allouch, M. Alajlan, Y. Javed, A. Belghith and M. Khalgui, "Micro Air Vehicle Link (MAVlink) in a Nutshell: A Survey," in IEEE Access, vol. 7, pp. 87658-87680, 2019, DOI: 10.1109/ACCESS.2019.2924410.
[18] Popescu, Stoican, Stamatescu, Chenaru, and Ichim, "A Survey of Collaborative UAV–WSN Systems for Efficient Monitoring," Sensors, vol. 19, no. 21, p. 4690, Oct. 2019.
[19] Gura, Dmitry, Rukhlinskiy, Victor, Sharov, Valeriy and Bogoyavlenskiy, Anatoliy. "Automated system for dispatching the movement of unmanned aerial vehicles with a distributed survey of flight tasks: " Journal of Intelligent Systems, vol. 30, no. 1, 2021, pp. 728-738. https://doi.org/10.1515/jisys-2021-0026.
[20] Seo, Seung-Hyun & Won, Jongho & Bertino, Elisa & Kang, Yousung & Choi, Dooho. (2016). A Security Framework for a Drone Delivery Service. 29-34. 10.1145/2935620.2935629.

AUTHORS PROFILE

Ms. Maansa Krovvidi is a young researcher yearning to upskill herself in the latest cutting-edge technologies. She has been trained in Data analytics, designing secure high bandwidth networks, Machine Learning and python. Her research areas of interest are Wireless communications and IoT.

Mr. Ch Mvn Sai Teja Prashanth is an Ardent Security Researcher and Bug Bounty Hunter. He has good experience in Web-app security, Android-app security, and Vulnerability Assessment and Penetration testing. He has been featured in MNC's like United Nations, Netflix, Indeed, Swiggy, Big basket, and many more.

doi: 10.32622/ijrat.99202103