Security in Internet of Drones: A Comprehensive Review

Snehal Samantha¹, Prema K V²* and Mamatha Balachandra³

Abstract: Unmanned Aerial Vehicles (UAVs), also called drones, are used for various applications with two basic classifications: civilian and military drones. Civilian drones are used for various applications like construction site monitoring, natural disaster area monitoring, agriculture, etc. Military drones are used for applications like monitoring a country’s border, the transmission of information about the intruders to Ground Control Station (GCS), or to any other server which has been designed for the purpose. Before the real-time deployment of the Internet of Drones (IoD), the feasibility and efficiency of a proposed UAV framework should be tested in an open-source UAV simulator or any network simulator. AirSim simulator is an open-source UAV simulator that has different features like ease of development, efficient motion capture, efficient obstacle detections and collision detections, use of different sensor models, and physics models. Hence, a review has been done on recent UAV frameworks which have been designed and tested using the AirSim simulator. Since a vast amount of data is being transmitted between IoD devices in this era, there is a need for designing secure IoD communication frameworks, with the least compromise in the performance of the designed frameworks. Hence, an extensive review has been done on different secure IoD communication frameworks which have used different cryptography concepts like key agreement.

ABOUT THE AUTHOR

Snehal Samantha is currently pursuing his PhD degree with the Department of Computer Science and Engineering, Manipal Institute of Technology, MAHE, Manipal, India.

Dr. Prema K V (Member, IEEE) is a Professor and Head in the Department of Computer Science Engineering at Manipal Institute of Technology, Bengaluru, MAHE. Her areas of research interest are Soft computing, Computer Networks, and Security. She has 30 years of teaching experience, 22 years of research experience and has published more than 120 papers in reputed Journals and Conferences.

Dr. Mamatha Balachandra is currently an Associate Professor - Senior scale in the Department of Computer Science and Engineering, Manipal Institute of Technology, MAHE, Manipal, India. She has around 22 years of teaching experience and has published around 25 research papers in national/international journals/conferences. She is also on the editorial board of some journals.

PUBLIC INTEREST STATEMENT

Drones are used for various applications that can be classified into civilian and military applications. Drones can be classified into different types based on weight, altitude, flight range, and flight time. Drones are also restricted by regulations that vary from region to region. The drone regulations are necessary to reduce the number of drone accidents, and loss of drone data. Internet of Drones (IoD) networks need to be analysed before real-time deployments, to prevent time-consuming experiments, drone accidents, and loss of drone data. Hence, a comprehensive review of how simulations can be done for drone tasks and applications has been provided. IoD networks are vulnerable to several physical and cyber threats, and also the devices are resource-constrained. Hence, a major review of the security and efficiency of the IoD networks has been provided.
authentication, encryption and decryption, integrity, blockchain, digital signatures, and have implemented their proposed frameworks in real-time, or by using network simulators. The common network simulators that have been used for simulating secure IoD frameworks/mechanisms are NS3 and OMNeT++.

Subjects: Computing & IT Security; Computer Science; General; Communication Technology

Keywords: AirSim; authentication; decryption; encryption; internet of drones; key agreement; security; UAV

1. Introduction

Unmanned Aerial Vehicles (UAVs) are also called drones. UAVs can be operated in two ways: autonomously, or manually by a pilot. In both the operating flight modes, there is a need for a communication link between Ground Control Station (GCS) and UAV. In autonomous flight operating mode, navigation is done usually through Global Positioning System (GPS) data. In manual flight operating mode, a pilot directly controls the drone through Line of Sight (LoS) or virtual cockpit control (Shoufan et al., 2018).

Drones fly in the sky with full network capabilities and they form a category of emerging new Internet of Things (IoT) devices. Cognitive drone platform is a flying IoT domain that quantifies the power characteristics and performance characteristics of cognitive applications based on these mobile flying IoT devices, i.e. drones (Genc et al., 2017). Internet of Drones (IoD) is an architecture that has been designed for providing controlled and coordinated access to drones. Layered architecture for IoD provides many benefits such as scalability, codebase maintainability, and layer modification flexibility with minimal changes to other layers (Gharibi et al., 2016).

Drones can be classified into two based on applications: civilian drones, and military drones (H. Wang et al., 2019). Civilian drones are used for applications like agriculture, search and rescue operations (Saif, Dimyati, Noordin, Alsamhi, et al., 2021)(Sahal et al., 2021), environmental monitoring (Almalki et al., 2021)(Alsamhi, Afghah, et al., 2021)(Alsamhi, Ma, Ansari, Almalki, et al., 2019), natural disaster monitoring (Saif, Dimyati, Noordin, Shah, Alsamhi, Abdullah, et al., 2021)(Alsamhi, Ma, Ansari, Gupta, et al., 2019)(Saif, Dimyati, Noordin, Shah, Alsamhi, Abdullah, et al., 2021), goods delivery, communication relays (Alsamhi, Almalki, et al., 2021), construction site monitoring, traffic monitoring, etc. Military drones are used for applications like border surveillance, intelligence reconnaissance, UAV combat missions, etc.

Before diving into any concept of IoD networks, it is necessary to get some idea about a brief evolution of drones which has been provided in subsection 1.1. Since the article is a review paper, a brief idea about how our review differs from some previous related works needs to be highlighted which has been done in subsection 1.2. Finally, subsection 1.3. shows the organization of the review paper.

1.1. Evolution of drones

The first appearance of drones was in the year 1849 when Austrians attacked Venice city of Italy by using explosives filled with unmanned balloons. Similar attacks were carried out even during the American civil war. Military drones were even used for the Cold war, World War I, World War II, American Civil War, Vietnam War, and Balkans war (Gynnild, 2014). The first aircraft drone was used for tactical reconnaissance during Vietnam War. Military drones’ effectiveness became more significant when they were used for conflicts of Iraq, Afghanistan, and Kosovo (Armour & Ross, 2017).
During the early 2000s, the civilian drone revolution started when drones were used for a broad range of civilian activities like photography, racing, construction site surveillance, agriculture, etc. (Tezza & Andujar, 2019). In the year 2006, a breakthrough had happened in the commercial drone field, when Federal Aviation Administration (FAA) issued a commercial drone permit for the first time. In the same year, SZ DJI Technology (A Chinese drone company) was founded (Maghazei & Netland, 2019). In the year 2010, a French company named Parrot had launched a drone called A.R. Drone, which is a quadrotor that was worth $300. This drone was developed for a mass market of video games. As time passed, it attracted features like stable hovering and onboard cameras. As time passed, A.R. Drone was used for various applications like feature map learning of a determined area, autonomous navigation, and position stabilization. For the A.R. Drone applications, the base station is the head of the network that extracts relevant information for generating a steering command based on a corresponding application (Lugo & Zell, 2014). Similar to other retailers, Amazon was facing delivery operations price challenges. Hence, to overcome these challenges, in the year 2013, Amazon announced its intention of drone-based delivery systems. As a result, Amazon overtook other third-party transportation companies. Amazon had assumed that delivery drones would have a speed of 80 km/h and a travel radius of 16 km (Shavarani et al., 2018). Following this, in the year 2014, Google made its drone delivery project debut. The project was called Project Wing. Following this, Dalsey Hillblom Lynn (DHL) integrated drones into the logistics network in early 2016. In the year 2016, FAA head Michael Huerta explained that they were working on a proposal that would help people fly drones beyond the visual LoS (Schneider, 2017). In January 2016, EHang Company unveiled its autonomous single passenger quadcopter 184 at the Consumer Electronics show, after which the drone was termed as “the world's first passenger drone”. Ehang Vice president said that the drone had an empty weight of 240 kg and a maximum gross takeoff weight of close to 360 kg. Figure 1 shows the image of the world's first passenger drone “manned drone” 184 (Whittle, 2017). As time passed, last-mile deliveries through drones started gaining popularity, since it was time-effective and cost-effective. After a disaster, due to probable damages to the traditional transportation infrastructures like truck drone systems or truck-only delivery, the integration of drones with air taxis can provide advantages at the onset of a disaster (Rajendran & Srinivas, 2020). After the Coronavirus Disease-19 (COVID-19) pandemic outbreak, drones have been used to combat the pandemic in many ways. Drones can be used for transportation tasks like food delivery, medicine delivery, etc. Drones can be used for spraying disinfection. Drones can be used for public space monitoring like maintaining social distance, infected cases identification, detection of the absence of masks, voice broadcast, etc. (Alsamhi, Lee, et al., 2021).
Table 1. Comparison of the current survey with previous related surveys/reviews/studies

| Reference                        | Analysis type | Publication year | Areas explored during the analysis                                                                                                                                 |
|----------------------------------|---------------|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| (Krishna & Murphy, 2017)         | Review        | 2017             | Cybersecurity Vulnerabilities for IoT networks                                                                                                                                 |
| (Ebeid et al., 2018)             | Survey        | 2018             | Open-Source Hardware flight controllers, open-source software flight controllers for IoT networks, and open-source simulation platforms for UAVs                      |
| (Syed et al., 2021)              | Survey        | 2021             | Security of UAV applications by using Machine Learning, Blockchain, and Watermarking Techniques                                                                        |
| (Boccadoro et al., 2021)         | Survey        | 2021             | Applications of IoT networks for each layer of Internet Protocol Stack, Security for UAV application-specific scenarios, Authentication and Security Frameworks for IoT networks, and security vulnerabilities in IoT networks from the perspective of Physical layer |
| (A. Sharma et al., 2020)         | Survey        | 2020             | Machine learning, Path Planning, Optimization, Encryption techniques for secure and efficient drone communications; Applications of IoT communications                  |
| (Yaacoub et al., 2020)           | Survey        | 2020             | Application domains of UAVs, Security vulnerabilities in UAV networks, and their corresponding countermeasures and detection mechanisms                                      |
| (Zhi et al., 2020)               | Survey        | 2020             | Analysis of IoT network safety and vulnerabilities in terms of 3 aspects: sensors, UAV communications, and Multi-UAV networks                                             |
| (Altawy & Youssef, 2016)         | Survey        | 2017             | Physical and Cyberthreats on civilian IoD networks, and the corresponding security measures against such threats                                                         |
| (Hentati et al., 2018)           | Study         | 2018             | Suitable UAV simulators, and GCS software frameworks                                                                                                                   |

(Continued)
1.2. Comparison of the current review and related previous surveys/reviews/studies

Table 1 shows the comparison of the current survey with previous related surveys/reviews/studies.

1.3. Organization of the review paper

Section 2 describes basic UAV architecture and UAV types. Section 3 describes some UAV regulations and UAV Communication protocol called MAVLink. Section 4 deals with some commonly used GCS software, UAV simulators, and UAV software frameworks. Section 5 provides a review of how
authors have used the AirSim simulator to simulate some proposed UAV application frameworks. Section 6 provides a review of how different cryptography frameworks/mechanisms have been designed and implemented for secure and efficient IoD communication. Section 7 deals with some UAV communication attack models or threat models, and some common attacks on IoD communication. Section 8 deals with security analysis tools, models, and logics that are used for security analysis of IoD communication. Section 9 provides details about the challenges and future work that have been identified for the two major reviews which have been conducted. Section 10 finally concludes our review paper. Figure 2 shows an overview of the review paper with logical relationships between different sections.

Table 2 shows the total number of papers referred for each section of the review paper. (Altawy & Youssef, 2016) is common to Sections 1 and 2.

2. UAV architecture and UAV types
The basic components of a drone system might differ in terms of names. There might be differences between the hardware and software parts of specific drone types. Hence, this provides a motivation to know the basic architecture of an IoD network, which has been done
in subsection 2.1. Since different UAV applications demand different types of UAVs in terms of size, weight, flying mechanism, flight height, and communication range, this provides scope for classifying UAVs into different types. Hence, classification of UAVs has been shown in subsection 2.2.

### 2.1. UAV architecture

A UAV system has six basic components: the UAV air-frame, the flight computer, the payload, the payload/mission controller, the base station, and the communication infrastructure. Figure 3 shows different UAV system components. The UAV air-frame is a small, lightweight, and pilot-less aircraft that is used to fly above the areas that need to be monitored. The flight computer is the heart of the UAV. It consists of a set of sensors like pressure sensors, magnetometer, gyro-meter, accelerometers, GPS, etc. to collect different aerodynamic information. The payload consists of a set of sensors like infrared sensors, thermal sensors, TV cameras, etc. that can collect information and process the information on board, or transmit the collected information to the base station for further analysis. The payload/mission controller is the on-board computer for the UAV. Based on the flight plan and actual mission assigned to the UAV, the mission controller is used to control different sensors of payload. The base station is a ground computer system, and it is the crucial component of the UAV system. The base station is used to operate UAV, UAV’s payload, and to monitor the mission development. The communication infrastructure consists of different communication mechanisms, among which the important ones are microwave links, radio modems, and satellite communications, to maintain a continuous and guaranteed link between the UAV and base station (Pastor et al., 2006).

---

**Table 3. Classification of UAVs based on flying range and single flight time**

| Category          | Flying range | Single flight time |
|-------------------|--------------|--------------------|
| Micro UAV         | <10 km       | <1 h               |
| Mini UAV          | <10 km       | 1–2 h              |
| Close Range UAV   | 10–30 km     | 2–3 h              |
| Short Range UAV   | 30–70 km     | 3–6 h              |
| HALE UAV          | >2000 km     | 24–48 h            |

---

**Figure 4. Taxonomy of UAV types.**
| Ref | RL based? | SE or SRE? | AirSim environment(s) | Features |
|-----|-----------|------------|-----------------------|----------|
| (Zafar et al., 2021) | No | SE | 3D AirSim with flood images on its floor | • Components: Monitoring, Communications, Network management, and Realignment.  
• The flight controller module is used in AirSim for programmatic drone movement and MAVLink protocol for communication with the simulated drones.  
• Different delivery tasks like food delivery, water delivery, clothes delivery, life saving, and other undefined class of tasks are done for evaluation.  
• Realignment component has a completion rate of 69% and a processing time of 12 min for 2600 available tasks, which shows a 14% increased completion rate and reduction of 20 min in processing time when compared to that of a centralized system for drones.  
• Convolutional Neural Network (CNN) model shows around 76% correctly predicted observations accuracy. |
| Ref | RL based? | SE or SRE? | AirSim environment(s) | Features |
|-----|-----------|------------|------------------------|----------|
| (Shamwell et al., 2019) | No | SRE | AirSim MAV | • The proposed method uses multi-scale projections and uses scaling factors of 2, 4, and 8.  
• Experiments are performed by capturing RGB-D imagery of resolutions 128*480 at 10 Hz.  
• The translational error percentage and rotational errors of the proposed method are respectively 4.94% and 10.24 which are lesser than the corresponding parameters of VIOLearner (RGB), VIO Learner (no IMU), and Structure From Motion (SFM) Learner approaches. |
| (Shin et al., 2020) | Yes | SRE | Simulated maze with 4-layered obstacles | • Action Critic network eliminates the need for manual labeling in contrast to the need for manual labeling in conventional supervised learning, by extracting depth map from a given environment, and it provides flexibility to a potential change in the environment.  
• AirSim simulations are done on UBUNTU 16.04 OS, with programming done using Python 3.6.  
• Action Critic using Kronecker-Factored Trust region (ACKTR) actor-network has the best performance in simulated training environment when compared to 3 other actor-critic algorithms.  
• Proposed network provides effective avoidance of obstacles, even with progressive changes in the real environment. |
| Ref                        | RL based? | SE or SRE? | AirSim environment(s) | Features                                                                 |
|----------------------------|-----------|------------|------------------------|--------------------------------------------------------------------------|
| (J. Li et al., 2019)       | No        | SRE        | Urban highway          | • The traffic dataset generation for vehicles detection is done by capturing imaging using UAV DJI-MATRICE 100 with image resolutions 1280*960.  
• For simulation setup, 2 devices are used: client computer for building a simulation environment and generating output scene images, server computer acts as a processor for implementation of the algorithm and obtaining speed estimation result of a vehicle.  
• Speed estimation of a vehicle is done using 6 different conditions of monitoring done by UAV (i.e 6 different case scenarios), by considering directions, uniform and variable motions, and observation heights of UAV.  
• While considering the 6 case scenarios of simulation, the average measurement error is around 1.275 m/s. |

(Continued)
### Table 4. (Continued)

| Ref                  | RL based? | SE or SRE? | AirSim environment(s)                                                                 | Features                                                                                                                                                                                                 |
|----------------------|-----------|------------|--------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| (Arce et al., 2020)  | No        | SRE        | Neighborhood, Refinery, and Landscape Mountains                                        | • The proposed method is used for terrains mapping without Digital Elevation Model (DEM)s or with incomplete DEMs.  
  • For the field study, a municipal water tank is chosen DJI Phantom 4 UAV and a computer with Windows 64-bit OS and 15.86GB RAM are used for field study.  
  • In the simulations, the obtained errors are directly proportional to the complexity of the chosen environment, hence the refinery environment produces more errors.  
  • Validation of iterative modeling for the AirSim simulation environment is done at 3.4 cm per pixel, and that for the field study case is done at less than 3 cm per pixel.  
  • A field study case can just use few iterations to successfully map an unknown area. |
| (Deng et al., 2020)  | No        | SRE        | Urban Environment                                                                    | • Real data is collected by using commercial DJI Matrice 100 quadcopter.  
  • Simulations use a monocular camera resolution of 320*240, and a field of view set to 53.  
  • Simulation shows that the proposed method gives an accurate and smooth velocity estimate.                                                                 |
| Ref                          | RL based? | SE or SRE? | AirSim environment(s)                                                                 | Features                                                                                                                                                                                                 |
|------------------------------|-----------|------------|--------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| (Shin et al., 2019)          | Yes       | SE         | Woodlands, Arena, and Blocks World                                                   • The experiments are performed using simple flight configuration in the settings.json configuration file for AirSim, and Python 3.6 on Ubuntu 16.04 OS computer.  
• Training for discrete action space shows that a depth map provides more information for learning than by RGB, and that for continuous action space shows that drones make successful paths by avoiding obstacles.  
• The racing experiment shows that the Arena environment is tougher than the other 2 for racing and that maneuvering through 3D obstacles can be done most probably by trained pilots. |
| (Koutras et al., 2020)       | No        | SE         | City Environment                                                                   • The paper uses a unit called time step which is the time interval at which a UAV can change its position and orientation.  
• Based on RGB images obtained by the UAVs, the YOLOv3 detector is used for the calculation of the detected objects.  
• Performance analysis shows that the proposed algorithm achieves a performance that is equivalent to that from 60 different UAVs’ configurations in a semi exhaustive algorithm to decide upon the next monitoring positions of UAVs. |

(Continued)
| Ref                  | RL based? | SE or SRE? | AirSim environment(s)                                                                 | Features                                                                                                                                                                                                 |
|---------------------|-----------|------------|--------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| (Goh et al., 2021)  | Yes (DRL) | SE         | Air Drone Rescue environment (+ 7 additional environments like City, Coastline, Forest, Africa, Football Field, Neighborhood, and Plains) | • In the proposed algorithm, the AirSim simulations are done by configuring 4 drones of which one is a target drone and the other 3 are follower drones.  
  • The proposed algorithm also uses a metric called reward function which ensures the level to which the follower drones keep up their distances and altitude with the target drone, and their formation maintenance while moving with the target drone.  
  • Experimental analysis shows that in the first iteration, Deep Recurrent Q-Network (DRQN) with a triple model achieves a higher reward than DRQN with a single model. During the third iteration, DRQN with a single model achieves effectiveness of 66%. |
| (Wei et al., 2019)  | Yes       | SE         | Room of size 20 m*20 m                                                              | • The environment resets if the UAV crashes or if the distance between the UAV and the target is less than 1 m.  
  • During the implementation, around 50,000 steps are trained.  
  • The results show that the proposed method has a success rate of 98.9% which is extremely high when compared to that of the other 2 detection and recognition methods. |

(Continued)
| Ref | RL based? | SE or SRE? | AirSim environment(s) | Features |
|-----|-----------|------------|------------------------|----------|
| (Bondi et al., 2020) | No | SRE | Africa Savanna environment | - The proposed method uses 62,000 real frames and 1 lakh synthetic frames.  
- The dataset performs tasks like detection, single-object tracking, and multi-object tracking.  
- The real data and synthetic data have significant variations in terms of content and artifacts.  
- State of art detection models perform well for large animals, but performance declines when the animals are small.

| (S. Wang et al., 2017) | No | SRE | Landscape Mountains | - The Virtual Reality (VR) platform is used for displaying different objects like mountains, trees, and lakes, and all 4 seasonal changes.  
- UAV VR platform uses UE4 engine since UAV deep learning needs an accurate presentation of even minute things like lake reflections, shadows, and trees’ elastic deformations.  
- During a manual or automated AirSim simulation, images and data can be obtained for the process of UAV deep learning. |
| Ref                        | RL based? | SE or SRE? | AirSim environment(s)                                                                 | Features                                                                                                                                                                                                 |
|----------------------------|-----------|------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| (Hsieh et al., 2019)       | No        | SRE        | Not specified                                                                        | • Karlsruhe Institute of Technology and Toyota Technological Institute (KITTI) dataset is used in addition to AirSim generated dataset.                                                                 |
|                            |           |            |                                                                                        | • Performance analysis of the AirSim generated dataset for the proposed model shows that a fully trained model has a precision rate of 82.2% and recall rate of 85.25% which are more than that of corresponding performance metrics of other training settings. |
| (Zuluaga et al., 2018)     | Yes       | SE         | Neighborhood environment, blocks environment, and a customized environment             | • During training, 2 environmental functions are called: Step function, and Reward function.                                                                                                         |
|                            |           |            |                                                                                        | • Performance analysis shows that the success rate of the trained agent is 8% and that of the random agent is 5%.                                                                                       |
| (Lombard et al., 2020)     | No        | SE         | Blocks environment                                                                   | • The proposed method does not take into account the speed adaption of a UAV.                                                                                                                         |
|                            |           |            |                                                                                        | • During the simulations, drones are placed on the sphere and made to simultaneously cross the sphere with a maximum speed of 3.5 m/s each.                                                           |
|                            |           |            |                                                                                        | • The simulations also show that under extreme conditions, the proposed method cannot ensure safety.                                                                                                  |
Table 4. (Continued)

| Ref                         | RL based? | SE or SRE? | AirSim environment(s)                                                                 | Features                                                                                                                                 |
|-----------------------------|-----------|------------|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| (Boldini et al., 2020)      | No        | SE         | Downtown                                                                              | • A Deep Neural Network (DNN) architecture for Visual Inertial Odometry (VIO) has been developed for the determination of UAV's absolute pose and integrated into the closed-loop control system. |
|                             |           |            |                                                                                       | • The performance analysis of developed architecture for VIO shows that for 6 Degrees of Freedom (df) poses of UAV, the average RMSE is around 0.06 which is the least when compared to that of traditional VIO methods. |
|                             |           |            |                                                                                       | • The overall system outperforms traditional benchmark EuROC Micro Air Vehicle (MAV) dataset approaches, however sometimes the nth estimated pose is not consistent with (n + 1)th estimated pose. |
| (Singh & Alvarez, 2020)     | No        | SE         | Mars simulation environment, and Earth-like environment                                 | • The proposed method has got 3 main entities: Target Acquisition System, Navigation System, and Mars simulation environment. |
|                             |           |            |                                                                                       | • The major limitation of the proposed method is that the standard water index does not return the desired value (usually above 0.5 for water). The standard water index returns −1 and lower values for non-water objects. |
|                             |           |            |                                                                                       | • Another disadvantage of the proposed method is that it does not focus on reflectance values, and does not consider the sensor noise. |

(Continued)
Table 4. (Continued)

| Ref                      | RL based? | SE or SRE? | AirSim environment(s)                  | Features                                                                                                                                                                                                 |
|--------------------------|-----------|------------|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| (Pienroj et al., 2019)   | Yes (DRL) | SE         | Landscape Mountains with power line    | • Performances of different DRL algorithms are compared on simplified control task which aims for height above the power line.                                                                                   |
|                          |           |            |                                        | • The Deep Deterministic Policy Gradient (DDPG) algorithm is used for experiments in a more photorealistic environment that targets simultaneous height control and heading control, which uses independent controllers for height control and heading control. |
|                          |           |            |                                        | • Overall experiments in the paper consider 3 types of environment: simple, realistic, and lighting.                                                                                                        |
|                          |           |            |                                        | • When policies are adapted to new environments, experiments show that policies of harder environments with additional retraining increase the success rate for adherence to the ideal trajectory; but policies of an easier environment fail to complete the task even once. |
| Ref | RL based? | SE or SRE? | AirSim environment(s) | Features |
|-----|-----------|-----------|-----------------------|----------|
| (Lindgren et al., 2019) | No | SE | Virtual city environment | • The method is evaluated for the MAV dataset which is collected through the AirSim simulator, as well as against state of art methods based on the KITTI dataset.  
• During the AirSim simulations, flight speeds in the range 0 to 8 m/s are considered, with 14 trajectories each having a flight time of 108s.  
• The intensity of fog and snow are kept the same for both the KITTI dataset and the AirSim dataset, but rain intensity being higher for the AirSim dataset.  
• The proposed method successfully localizes through all environmental conditions and all difficulty levels.  
• BooM-VIO method outperforms VINS-Mono when different metrics are considered on harsh environments, and different difficulty levels, but does not strictly outperform traditional VIO methods. |

(Continued)
| Ref                        | RL based? | SE or SRE? | AirSim environment(s)                                                                 | Features                                                                                                                                                                                                 |
|---------------------------|-----------|------------|---------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| (Bondi et al., 2018)      | No        | SE         | Africa Savanna environment                                                            | • Since the flights and monitoring are done at night, the built environment is expanded to include thermal infrared imagery for dataset augmentation for the detection of animals and humans.  
• The emissivity of the objects in the environment varies between 0.8 and 0.99 on average for different objects in the environment.  
• The environment also considers a parameter called Point Spread Function (PSF) which measures the blurriness of the image, and also noise in the image.  
• Creation of environment and generation of simulation data took around 200hrs, and real data labeling took around 800hrs.  
• AirSim-W is a potential environment for a cost-effective solution for wildlife conservation. |
| (Mazdin & Rinner, 2019)   | No        | SE         | Environment measuring an area of 240 m²240 m, which has buildings blocks of different sizes of interest, and a GCS at the center of the area | • The default flight controller SimpleFlight is used for drones, and the recent ROS2 version is incorporated for a fully decentralized system.  
• Exploration time is independent of the number of drones but depends on environment uncertainty and exploration method.                                                                                   |
Table 4. (Continued)

| Ref | RL based? | SE or SRE? | AirSim environment(s) | Features |
|-----|-----------|------------|-----------------------|----------|
| (Vempra & Saripalli, 2018) | No | SE | Sparsely populated environment, and Urban environment | • The proposed algorithm handles the problem of pure rotation movement, by feature points matching between rotating MAV and another MAV which is used to observe common scene points.  
• When the proposed algorithm is applied to a sparsely populated environment, inter-MAV localization provides higher robustness when compared to intra-MAV localization.  
• Fusion of inter-MAV and intra-MAV localization with occasional fusions and relative measurements demonstrates the improvement in the overall localization accuracy. |
The adopted communication infrastructure depends on the operation range of the UAV. UAV missions are classified into two based on the distance between UAV and GCS: LoS missions, and Beyond LoS (BLoS) missions. In LoS missions, the transmission of signals happens through direct radio waves. In BLoS missions, the transmission of signals happens through satellite communications or relay drones (Altawy & Youssef, 2016).

2.2. UAV types

Figure 4 shows the taxonomy of UAV Types.

A new swarm of drones can either be permitted or not be permitted to accompany an existing swarm of drones. Based on this, a swarm of drones can be classified into three. They are static drones, dynamic drones, and hybrid drones. (i) Static drones consist of a static swarm of drones. Before the flight process starts, the ground station selects and registers this swarm of drones. Hence, once the flight process begins, the ground station does not allow a new drone to join the existing registered swarm of drones. Therefore, static drones provide high security since the ground station would regard a new unregistered drone as a potential enemy for the flight. (ii) Dynamic drones contain a dynamic swarm of drones. As a result, the unregistered drones need not be registered by the ground station, for the unregistered drones to accompany registered drones. A registered flying drone is capable of leaving the flight process at any time. Concerning requirements in security in communication, this is a beneficial feature. Among dynamic drones, there is an issue of mutual trust. (iii) Hybrid drones consist of a hybrid swarm of drones. A hybrid swarm of drones is a combination of static drones and dynamic drones. The swarm consists of two segments named flying with core and flying with the extended. The core consists of static drones and the extended consists of dynamic drones that allow new unregistered drones to join the flight process and permits the registered drones to leave the flight. As a result, hybrid drones combine the advantage of dynamic drones and security provided by static drones. As a result, hybrid drones are an effective solution to resist potential attacks (Akram et al., 2017). Figure 5, Figure 6 and Figure 7 represent the static, dynamic, and hybrid swarm of drones, respectively (Albalawi & Song, 2019).
Based on flying mechanisms, drones can be classified into 3: multi-rotor drones, fixed-wing drones, and hybrid fixed/rotary-wing drones. (i) Multi-rotor drones are also called rotary wing drones. They use the concept of vertical take-off and landing principle, and they provide continuous coverage for a particular area by hovering over it. They have to face gravity most of the time and hence have high power consumption. They also have limited mobility. (ii) Fixed-wing drones have more energy efficiency than multi-rotor drones. Fixed-wing drones can glide and travel at high speeds even with heavy payloads. But fixed-wing drones have three major drawbacks: the need for a runway for their take-off and landing, they cannot be used for hovering over a particular area, and are more expensive compared to multi-rotor drones. (iii) Hybrid fixed/rotary wing drones combine the advantages of both multi-rotor drones and fixed-wing drone types and can glide to reach a particular destination or hover over a fixed location (Fotouhi et al., 2019).

Multirotor drones are the cheapest and easier to build among the three classifications. They are used for applications like video surveillance and photography. However, since they have limitations of flight time, speed, and energy efficiency, they are not suitable for applications like long-distance monitoring and large-scale aerial mapping. Different examples of multi-rotor drones are tricopters, quadcopters, hexacopters, octocopters, etc. (Tahir et al., 2019).

Figure 8 shows the top view of a hexacopter (Verbeke et al., 2014).

Figure 9 shows a schematic view of a Titan-based fixed-wing drone (Pellerito et al., 2020).

Power consumption of a UAV type depends on different aspects like sensors and actuators, payloads, communication, data processing, internal and external loads, and system performance (Uragun, 2011).

Drones can also be classified based on take-off/landing mechanism into 2: horizontal take-off/landing (HTOL) style, and vertical take-off/landing (VTOL) style. HTOL style drones have
many advantages as they can fly for longer distances, they can capture better photos and videos in aerial photography and filming when compared to VTOL style drones. However, HTOL-style drones face difficulties during arrival and departure. Unlike HTOL-style drones, VTOL drones face the limitation of angle, stability, and coverage, because of which they cannot take good photos or videos (Estrada & Ndoma, 2019). Similar to conventional drones, VTOL drones have high cruise speeds, because of which they can perform take-off and landing operations even at hazardous places, and can reach the target place in a short period. VTOL drones can also switch between cruise flight mode and hover mode (Ozdemir et al., 2014). VTOL drones are efficient when compared to helicopters in terms of higher maximum cruise speed, a higher altitude at speeds greater than 185.2 km/h, lesser noise, and lesser container volume. Unlike helicopters, VTOL drones do not pose restrictions during forwarding flights (Ahn et al., 2010). Unlike conventional aircraft, VTOL drones do not require runways because of which VTOL drones have a greater number of options for take-off space, landing, and maneuverability (Keith & Hall, 2009).

Civil Aviation Safety Authority (CASA) has classified the UAVs into four categories based on a UAV’s gross weight: Micro UAVs (have a gross weight of lesser than or equal to 100 g), Small UAVs (have a gross weight of higher than 100 g, but lesser than or equal to 2 kg), Medium UAVs (have a gross weight of higher than 2 kg but lesser than or equal to 150 kg), and Large UAVs (have a gross weight of more than 150 kg) (Homajed & Rizos, 2015).

Weibel et al. have classified the drones into five based on their weights: Micro-drones (have weight less than 2 lbs), Mini drones (have a weight ranging from 2 lbs to 30 lbs), Tactical drones (have a weight ranging from 30 lbs to 1000 lbs), Medium and high altitude drones (have a weight ranging from 1000 lbs to 30000 lbs), and Heavy drones (have a weight greater than 30000 lbs) (Weibel & Hansman, 2004).
UAVs can also be classified based on their operating altitudes into 2: Low Altitude Platforms (LAPs), and High Altitude Platforms (HAPs). LAPs are small-sized UAVs that fly at low altitudes in the range of few tens of meters to few kilometers. HAPs are larger-sized and more capable UAVs that fly at altitudes of above 17 km. Generally, HAPs have more endurance than LAPs. HAPs are used for long-term missions and can operate continuously for few months or even more depending on the ability to overcome the energy constraints. LAPs are used for time-sensitive missions and can operate continuously for few hours depending on battery life and their ability to recharge. Typical examples of LAPs are Parrot AR Drone, DJI Phantom drone series, etc. Prominent examples of HAPs are Airbus’s Zephyr, Google’s Project Loon, etc. (Reynaud & Rasheed, 2012).

Figure 10 and Figure 11 represent Parrot AR drone power edition 2.0, and DJI Phantom 3 drone, respectively.

Airbus Zephyr is the first UAV capable of flying in the stratosphere, which can operate like a pseudo satellite that is used to harness solar energy. Airbus Zephyr is cheaper than a satellite. Airbus Zephyr provides new opportunities, new business models, and new services to the connectivity market. It is also applicable for adaptive mission planning at distances greater than 185.2 km (Bauk, 2020). In Google Loon Project, Google has used a HAP balloon integrated with a 4 G network, flying at an altitude of 18–50 km to provide long-term wireless connectivity to rural areas (Hayajneh et al., 2016).

Based on flying range and single flight time, UAVs can be classified into five categories: Micro UAV, Mini UAV, Close range UAV, Short Range UAV, and High Altitude Long Endurance (HALE) UAV. Table 3 shows the classification of UAVs based on flying range and single flight time (Robakowska et al., 2019).

2.3. Lessons learned
Subsection 2.1 has shown the basic architecture of an IoD network which has six components. This architecture is a foundation for deploying IoD networks with different types of UAVs. This architecture explains different sensors, different communication elements, and different sender and receiver components that require or do not require human intervention. Subsection 2.2 has shown a hierarchy for the classification of UAVs and has used seven main categories to further classify the UAVs. The classification enhances one’s knowledge on how a GCS has set entry restrictions to dynamic UAVs, different classifications for UAVs based on
weights, flying altitudes for UAVs, some popular examples like Google Loon Project, and single flight time and flight range of UAVs.

3. UAV regulations and UAV communication protocol
The UAV application domains are not just restricted to UAV types. But they also have constraints that different government agencies have imposed. The constraints are defined to reduce the number of drone accidents (which can cause loss to life and/or property) and for secure IoD data communications. These constraints usually vary from country to country, or from a region to region. Hence, this motivates us to know about the standard UAV regulations and some examples of how some regions impose these UAV regulations. So, subsection 3.1 provides a brief explanation on UAV regulations. Since IoD networks are quite dynamic in nature, it is important to explore some communication protocol that suits for dynamic nature of IoD networks. Hence, subsection 3.2 explains a communication protocol called MAVLink.

3.1. UAV regulations
The application domains may not be just limited to the UAV types. They also have constraints based on different UAV regulations which different governments may impose. The application domains of UAVs are vast, but there are different issues related to the use of UAVs like public safety, UAV-triggered accidents, and UAV data loss. To handle these types of issues, and based on UAV types and UAV capabilities, the UAV regulations can be classified based on six criteria: (a) Applicability, (b) Technical requirements, (c) Operational limitations, (d) Administrative procedures, (e) Human resource requirements, and (f) Ethical constraints (Stöcker et al., 2017).
UAV regulations vary based on types of regions (rural or urban) and countries. For instance, urban areas have got complex surfaces, several zones which are designated as no-fly zones, and also highly populated. Hence, to ensure that UAVs operate securely and efficiently at low altitudes, different countries and regions have been exploring different policies and techniques to establish stable UAV operations by considering different safety and efficiency
concerns related to UAVs. For example, FAA has stated a maximum flying height constraint that UAVs can fly to a maximum height of 122 m with respect to ground level, in uncontrolled locations (C. Xu et al., 2020).

3.2. MAVLink communication protocol
MAVLink is a header-only lightweight communication protocol that allows communication among a maximum of 256 UAVs on the same frequency band. The protocol was released under the license GNU Lesser General Public (LGPL) license in the year 2009 and is used for communication between GCS and UAV, or intercommunication between different elements of UAV. MAVLink messages can be categorized into 2: information requests and mission commands. Examples of information request messages are pitch angle, raw angle, yaw angle, GPS latitude, GPS longitude, etc. Examples of mission command messages are take-off, change home location, etc. (Fuller et al., 2014).

3.3. Lessons learned
The subsection 3.1 explains the need for UAV regulations to prevent UAV accidents which can cause loss to life and/or property, as well as for the protection of UAV data. Six criteria for UAV regulations have been listed. UAV regulations vary from country to country, or from a region to region. The subsection has also shown some examples of UAV regulations. The subsection 3.2 has explained a lightweight UAV communication protocol called MAVLink. MAVLink messages can have two types of data: information requests as well as mission command messages.

4. GCS software, UAV simulators and UAV software frameworks
Many innovations have been happening in UAV applications and the associated drone industry. This has led to an increase in the need for development and research in UAV technology. Some UAV experiments are extremely time-consuming, there are chances of loss to property and/or life due to UAV accidents, and there are chances of loss of UAV data. Hence, this motivates us to gain some basic knowledge about some IoT software and frameworks, choose some suitable simulator/software framework for performing IoD experiments, and then plan for real-time deployments. Figure 12 shows the taxonomy for Section 4.

QGroundControl is an open-source GCS software that provides different featured supports like full GCS support, flight control, multiple UAVs configurations through MAVLink protocol communications, and allows a user to control PX4 and Ardupilot-based UAVs. The GCS software provides straightforward usage for beginners and provides high-end features for experienced users. It also provides a display feature of a flight map which shows flight track, vehicle position, waypoint, video streaming, and vehicle instruments (Ramirez-Atencia & Camacho, 2018). The software has the feature of simultaneous management of multiple drones. It has two main functional components in an autonomous flight: mission planner, and mission tracker. Mission planner function is mainly performed by insertion of way-points. After mission planning gets completed and uploaded to the desired drone, one can switch to mission tracking mode. Mission tracker mode is used to monitor and command the drone. Different types of mission control commands are the start, resume, pause, and continue (Dobrea & Dobrea, 2020). QGroundControl can run on different platforms like Windows, IOS, Android OS, and macOS.

Mission Planner is a GCS software for autopilot of different vehicles like aircraft, helicopters, rovers, and UAVs. The software can be used for monitoring autopilot conditions and the situation on the ground, and to receive telemetry data for commands production for control of UAV flight parameters. Other tasks that the software can perform are performance optimization, saving and loading of autopilot autonomous missions with a simple point and click mechanism, download, and analysis of mission log files and flight simulator. The software is supported only for the Windows platform (Putera & Ramdani, 2018).
| Resistance against attacks | Denial of Service (DoS) | Physical | Location theft | Impersonation | Replay | Modification | Eavesdropping | Offline password guessing | Online password guessing | Password and biometric update | Denial capture | Identity guessing | MITM | Server spoofing | Stolen smart device/card | Node capture | Key escrow | Known session key | Known session-specific temporary information |
|-----------------------------|-------------------------|----------|---------------|---------------|--------|--------------|---------------|--------------------------|--------------------------|-----------------------------|-----------------|---------------------|------|-----------------|-----------------------------|-------------|----------|-------------------|----------------------------------|
| Putranto et al., 2019       | ✓                       |          |               |               |        |              |               |                          |                          |                             |                 |                     |      |                 |                             |             |          |                   | (Continued)                      |
| (Gope & Sikdar, 2020)       |                         |          |               |               |        |              |               |                          |                          |                             |                 |                     |      |                 |                             |             |          |                   | (Continued)                      |
| (Tanveer et al., 2020)      | ✓                       |          |               |               |        |              |               |                          |                          |                             |                 |                     |      |                 |                             |             |          |                   | (Continued)                      |
| (Yahuzo et al., 2021)       | ✓                       |          |               |               |        |              |               |                          |                          |                             |                 |                     |      |                 |                             |             |          |                   | (Continued)                      |
| (Khan et al., 2021)         | ✓                       |          |               |               |        |              |               |                          |                          |                             |                 |                     |      |                 |                             |             |          |                   | (Continued)                      |
| (Tanveer et al., 2021)      | ✓                       |          |               |               |        |              |               |                          |                          |                             |                 |                     |      |                 |                             |             |          |                   | (Continued)                      |
| (Putranto et al., 2019)     | ✓                       |          |               |               |        |              |               |                          |                          |                             |                 |                     |      |                 |                             |             |          |                   | (Continued)                      |
| (Gope & Sikdar, 2020)       | ✓                       |          |               |               |        |              |               |                          |                          |                             |                 |                     |      |                 |                             |             |          |                   | (Continued)                      |
| (Tanveer et al., 2020)      | ✓                       |          |               |               |        |              |               |                          |                          |                             |                 |                     |      |                 |                             |             |          |                   | (Continued)                      |
| (Yahuzo et al., 2021)       | ✓                       |          |               |               |        |              |               |                          |                          |                             |                 |                     |      |                 |                             |             |          |                   | (Continued)                      |
| (Khan et al., 2021)         | ✓                       |          |               |               |        |              |               |                          |                          |                             |                 |                     |      |                 |                             |             |          |                   | (Continued)                      |
| (Tanveer et al., 2021)      | ✓                       |          |               |               |        |              |               |                          |                          |                             |                 |                     |      |                 |                             |             |          |                   | (Continued)                      |
| (Putranto et al., 2019)     | ✓                       |          |               |               |        |              |               |                          |                          |                             |                 |                     |      |                 |                             |             |          |                   | (Continued)                      |
| (Gope & Sikdar, 2020)       | ✓                       |          |               |               |        |              |               |                          |                          |                             |                 |                     |      |                 |                             |             |          |                   | (Continued)                      |
| (Tanveer et al., 2020)      | ✓                       |          |               |               |        |              |               |                          |                          |                             |                 |                     |      |                 |                             |             |          |                   | (Continued)                      |
| (Yahuzo et al., 2021)       | ✓                       |          |               |               |        |              |               |                          |                          |                             |                 |                     |      |                 |                             |             |          |                   | (Continued)                      |
| (Khan et al., 2021)         | ✓                       |          |               |               |        |              |               |                          |                          |                             |                 |                     |      |                 |                             |             |          |                   | (Continued)                      |
| (Tanveer et al., 2021)      | ✓                       |          |               |               |        |              |               |                          |                          |                             |                 |                     |      |                 |                             |             |          |                   | (Continued)                      |

(Continued)
| Resistance against attacks | (Putranto et al., 2019) | (Gope & Sikdar, 2020) | (Tanveer et al., 2020) | (Y. Zhang et al., 2020) | (Sahingoz, 2013) | (Yahuza et al., 2021) | (Khan et al., 2021) | (Tanveer et al., 2021) |
|---------------------------|-------------------------|-----------------------|------------------------|-------------------------|--------------------|----------------------|----------------------|------------------------|
| Private key leakage       | ✓                       | ✓                     | —                      | ✓                       | ✓                  | ✓                    | —                    | —                      |
| Perfect forward secrecy   | —                       | —                     | —                      | —                       | —                  | ✓                    | —                    | —                      |
| Malicious device deployment | —                      | —                     | —                      | —                       | —                  | ✓                    | —                    | —                      |
| Cloning                   | —                       | —                     | —                      | —                       | —                  | ✓                    | —                    | —                      |
| Privileged insider        | ✓                       | ✓                     | —                      | ✓                       | —                  | ✓                    | ✓                    | ✓                      |
| Ephemeral Secret Leakage (ESL) | —                   | ✓                     | ✓                      | —                       | —                  | ✓                    | ✓                    | ✓                      |
| De-synchronization        | —                       | —                     | —                      | —                       | —                  | ✓                    | ✓                    | ✓                      |
| Hijacking                 | ✓                       | —                     | —                      | —                       | —                  | —                    | —                    | —                      |
| Forgery                   | —                       | —                     | —                      | —                       | —                  | —                    | —                    | —                      |
| Resistance against attacks | (Nikooogha et al., 2020) | (Everson et al., 2021) | (Goce et al., 2021) | (Y. Li et al., 2020) | (Alladi et al., 2020) | (Pu Li et al., 2020) | (Alladi et al., 2021) | (Abdelmalik et al., 2020) | (X. Xu et al., 2019) | (Hong et al., 2020) | (C.-L. Chen et al., 2020) | (G. Cho et al., 2020) | (Pirker et al., 2020) | (Srinivas et al., 2019) | (Wazid et al., 2020) | (Ali et al., 2020) | (Lei et al., 2021) | (Chaudhry et al., 2020) | (Hussain et al., 2020) | (Jan et al., 2021) |
|----------------------------|--------------------------|------------------------|---------------------|-----------------------|-----------------------|----------------------|------------------------|------------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|
| Impersonation              | ✓                        | ✓                      | ✓                   | ✓                     | ✓                     | ✓                    | ✓                      | ✓                      | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   |
| Verifier                   | ✓                        | ✓                      | ✓                   | ✓                     | ✓                     | ✓                    | ✓                      | ✓                      | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   |
| Drone capture              | ✓                        | ✓                      | ✓                   | ✓                     | ✓                     | ✓                    | ✓                      | ✓                      | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   |
| Insider                    | ✓                        | ✓                      | ✓                   | ✓                     | ✓                     | ✓                    | ✓                      | ✓                      | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   |
| MITM                       | ✓                        | ✓                      | ✓                   | ✓                     | ✓                     | ✓                    | ✓                      | ✓                      | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   |
| Replay                     | ✓                        | ✓                      | ✓                   | ✓                     | ✓                     | ✓                    | ✓                      | ✓                      | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   |
| Password guessing          | ✓                        | ✓                      | ✓                   | ✓                     | ✓                     | ✓                    | ✓                      | ✓                      | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   |
| Wi-Fi                      | ✓                        | ✓                      | ✓                   | ✓                     | ✓                     | ✓                    | ✓                      | ✓                      | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   |
| Traceability               | ✓                        | ✓                      | ✓                   | ✓                     | ✓                     | ✓                    | ✓                      | ✓                      | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   |
| DoS                        | ✓                        | ✓                      | ✓                   | ✓                     | ✓                     | ✓                    | ✓                      | ✓                      | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   |
| Physical                   | ✓                        | ✓                      | ✓                   | ✓                     | ✓                     | ✓                    | ✓                      | ✓                      | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   |
| Desynchronization          | ✓                        | ✓                      | ✓                   | ✓                     | ✓                     | ✓                    | ✓                      | ✓                      | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   |
| Message modification       | ✓                        | ✓                      | ✓                   | ✓                     | ✓                     | ✓                    | ✓                      | ✓                      | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   |
| Masquerade                 | ✓                        | ✓                      | ✓                   | ✓                     | ✓                     | ✓                    | ✓                      | ✓                      | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   |
| Tampering                  | ✓                        | ✓                      | ✓                   | ✓                     | ✓                     | ✓                    | ✓                      | ✓                      | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   |
| Cloning                    | ✓                        | ✓                      | ✓                   | ✓                     | ✓                     | ✓                    | ✓                      | ✓                      | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   |
| Coalition                  | ✓                        | ✓                      | ✓                   | ✓                     | ✓                     | ✓                    | ✓                      | ✓                      | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   | ✓                   |

(Continued)
| Resistance against attacks | (Nikoo et al., 2020) | (Ev et al., 2020) | (Gope et al., 2021) | (Y. Li et al., 2020) | (Alladi, Na ren, et al., 2020) | (Pu & Li, 2020) | (Alladi, Chamo la, et al., 2020) | (Ab del-Malek et al., 2020) | (X. Xu et al., 2019) | (Ho ng et al., 2020) | (C.-L. Che n et al., 2020) | (G. Ch et al., 2020) | (Pirker et al., 2019) | (Sriv as et al., 2018) | (Ali et al., 2020) | (Lei et al., 2021) | (Chaudpour et al., 2021) | (Jan et al., 2021) |
|---------------------------|----------------------|------------------|---------------------|----------------------|-----------------------------|------------------|-------------------------------|-----------------------------|----------------------|----------------------|-----------------------------|-------------------|---------------------|----------------------------|-----------------|------------------|-----------------|
| Spoofing                  | —                    | ✓                | —                   | —                    | —                           | ✓                | —                             | —                           | ✓                    | —                    | —                           | —                 | ✓                   | ✓                           | —               | —                |
| Known session key         | ✓                    | —                | —                   | —                    | —                           | —                | —                             | ✓                           | —                    | —                    | ✓                           | —                 | —                   | —                           | —               | —                |
| Remote                    | —                    | —                | —                   | —                    | —                           | ✓                | —                             | —                           | ✓                    | —                    | —                           | —                 | ✓                   | —                           | —               | —                |
| Bio-metric update         | —                    | —                | —                   | —                    | —                           | —                | ✓                             | —                           | —                    | —                    | —                           | —                 | —                   | —                           | —               | —                |
| ESL                       | —                    | —                | —                   | —                    | —                           | ✓                | —                             | ✓                           | ✓                    | —                    | —                           | —                 | ✓                   | —                           | —               | —                |
| Privileged insider        | —                    | —                | —                   | —                    | —                           | —                | ✓                             | ✓                           | ✓                    | —                    | —                           | —                 | ✓                   | —                           | —               | ✓                |
| Identity guessing         | —                    | —                | —                   | —                    | —                           | —                | ✓                             | —                           | —                    | —                    | —                           | —                 | ✓                   | —                           | —               | —                |
| Asynchronous              | —                    | —                | —                   | —                    | —                           | —                | ✓                             | —                           | —                    | —                    | ✓                           | —                 | —                   | —                           | —               | —                |
| Brute force               | —                    | —                | —                   | —                    | —                           | —                | ✓                             | —                           | —                    | —                    | ✓                           | —                 | —                   | —                           | —               | —                |
| Stolen verifier           | ✓                    | —                | —                   | —                    | —                           | —                | ✓                             | —                           | —                    | —                    | —                           | —                 | —                   | —                           | —               | ✓                |
| Session-specific temporary information | ✓    | —                  | ✓                  | ✓                    | —                           | —                | —                             | —                           | —                    | —                    | ✓                           | —                 | —                   | —                           | —               | —                |
| Node capture              | —                    | ✓                | ✓                   | ✓                    | —                           | —                | —                             | —                           | —                    | —                    | ✓                           | —                 | —                   | —                           | —               | —                |
| Resistance to attacks | MITM | Impersonation | Password guessing | Data modification | Data leakage | Eavesdropping | Tampering | Spying | Cloning | Privileged insider | Malicious device deployment attack | Drone/device physical capture attack | DoS | Double-spend | Illegal session key computation | Internal | Compromise | ESL |
|----------------------|------|---------------|------------------|------------------|-------------|---------------|------------|--------|---------|------------------|-------------------------------|----------------------------------|-----|-------------|-------------------------------|---------|-----------|-----|
| (Wazid, Bera, et al., 2020) | ✓    | ✓             | ✓                | ✓                | ✓           | ✓             | ✓          | ✓      | ✓       | ✓                | ✓                            | ✓                                | ✓   | ✓           | ✓                            | ✓       | ✓         | ✓   |
| (Bera, Das, et al., 2020) | ✓    | ✓             | ✓                | ✓                | ✓           | ✓             | ✓          | ✓      | ✓       | ✓                | ✓                            | ✓                                | ✓   | ✓           | ✓                            | ✓       | ✓         | ✓   |
| (Bera, Chattopadhyay, et al., 2020) | ✓    | ✓             | ✓                | ✓                | ✓           | ✓             | ✓          | ✓      | ✓       | ✓                | ✓                            | ✓                                | ✓   | ✓           | ✓                            | ✓       | ✓         | ✓   |
| (Y. Tan et al., 2020) | ✓    | ✓             | ✓                | ✓                | ✓           | ✓             | ✓          | ✓      | ✓       | ✓                | ✓                            | ✓                                | ✓   | ✓           | ✓                            | ✓       | ✓         | ✓   |
| (W. Xiao et al., 2021) | ✓    | ✓             | ✓                | ✓                | ✓           | ✓             | ✓          | ✓      | ✓       | ✓                | ✓                            | ✓                                | ✓   | ✓           | ✓                            | ✓       | ✓         | ✓   |

Table 7: Resistance of the IoD communication blockchain methods against some attacks

Samanth et al., Cogent Engineering (2022), 9: 2029080
https://doi.org/10.1080/23311916.2022.2029080
DroidPlanner is a GCS software for controlling UAVs and can control only 1 UAV. The first version of the software was launched in the year 2013 and released under GNU. The operations performed by the software are based on the communication of messages between mobile devices and UAVs through the MAVLink protocol. The messages sent from the software to a UAV represent the control commands for the UAV. The messages sent from the UAV represent the current state of the UAV. In addition, the software performs other operations like creating tasks, defining interest points on a map for the UAV flight (Zacarias et al., 2016). The software is meant for only Android platforms and provides an Android Graphical User Interface (GUI) between a UAV and an Android device.

Universal Ground Control Software (UGCS) is a GCS software and a commercial application for drone flight planning. It provides a provision for a user to define various mission parameters for a flight like flight height, flight profiles, and percentage of forwarding and side overlap (Šiljeg et al., 2021). It can be used on different platforms like Windows, Ubuntu, macOS, Android, and iOS.

MavProxy is a GCS software that supports python and helps in communication between UAVs through MAVLink protocol. MavProxy usage is limited to only those UAVs which have supporting hardware (Choi et al., 2016). MAVProxy is a lightweight software and is supported for Linux OS.

AirSim is a UAV simulator that is based on Unreal Engine and was released by Microsoft in the year 2017. AirSim is used to simulate UAV flight and collect data using Unreal Engine. It provides different types of visual data like RGB images, disparity maps, depth maps, and color segmentation maps which can be captured from all UAV directions. The simulation environment of AirSim looks more like a real environment (Yang et al., 2018). AirSim supports both Software In Loop (SITL) and Hardware In Loop (HITL), and popular UAV flight controllers like PX4 and Ardupilot. AirSim has a provision to simulate even cars in any unreal environment. It supports APIs in different programming languages like Python, C++, C, and Java. AirSim works on different platforms like Windows and Linux.

X-Plane is a UAV simulator that has FAA-certified vehicle and simulation models. X-Plane works on different platforms like Windows, Linux, and macOS. Some of the examples of X-Plane world models are clouds, rain, wind, fog, and thermals. X-Plane allows independent visual debugging and data collection for up to 10 vehicles simultaneously on a single display. X-Plane can be used for designing and testing control algorithms that can be used on actual hardware implementations (Garcia & Barnes, 2009).

FlightGear is an open-source UAV simulator that is programmed using C++, which is used for simulating and modeling a UAV. “.ac” extension is the commonly used 3D format by FlightGear. FlightGear can produce 3D animation graphics in real-time and is connected to Flight Dynamics Model (Vogeltanz & Jašek, 2015). FlightGear works on Windows, Linux, and macOS platforms.

Java Micro Air Vehicle Simulator (jMAVSim) is a simple and lightweight UAV simulator developed by the PX4 development team. The simulator provides flight simulation and sensor emulation implemented using the JAVA 3D library (S.-h Cheon et al., 2016).

Gazebo is a dynamic open-source simulator based on Bullet Physics or Open Dynamic Engine (ODE). Gazebo is also used for robotic simulations as well as UAV simulations. Through plugin interface, Gazebo can simulate various sensors like IMU, cameras, laser scanners. Gazebo is compatible with Robot Operating System (ROS) (Okoli et al., 2019). Gazebo also supports autopilots like PX4 and Ardupilot, in both SITL and HITL.
FlyNetSim is a scalable and flexible open-source software framework for a UAV network. Ardupilot and NS3 are the two open-source platforms that are interfaced by FlyNetSim. FlyNetSim captures the complicated inter-dependencies between the network environment, communication, and UAV operations, such as navigation and sensing, and inner-state dynamics. Some of the FlyNetSim objectives are accurate modeling of UAV dynamics and operations using a software approach that fully preserves control pipelines and data structures of UAV software, preserving individual’s paths of data between UAV sensors and controllers providing a GUI for the visualization of the system status and automatic generation of UAV scenarios (Baidya et al., 2018).

IoD provides good communication among UAVs, i.e., drones. It is applicable for many applications like traffic management, control signaling, and multimedia streaming. IoD network development is essential for drone-based applications like civilian and military-based services. Though IoD is an advanced technology with many advantages, several issues arise from the IoD communication point of view. As novel communication algorithms and protocols are used in IoD, there is a high need for IoD to support flexible tools to analyze the performance of the IoD network, before its actual deployment. Hence, to serve this purpose, an IoD software framework is used. IoD is developed on top of NS3. The framework implements the main Zone Service Provider, network access points, networking elements drones (Grieco et al., 2019).

Communication Control Distributed Simulator (CUSCUS) is a UAV software framework that is an integration of the UAV simulator FL-AIR, network simulator NS3, and a scenario module. The scenario module enables the loading of a real-world map and works between FL-AIR and NS3. The scenario module has a provision of modeling realistic 3D scenarios with building positions and street topologies which can be imported from the popular website named OpenStreetMap (Zema et al., 2018).

4.1. Lessons learned
Many innovations and advancements have been happening in UAV technologies and drone industries, which has eventually increased the need for development and research as time has passed. Without a proper analysis of the designed IoD networks, if real-time deployments are made, different issues can pop up such as time-consuming experiments and UAV accidents. Hence, in section 4 different UAV simulators, GCS software, and UAV software frameworks have been studied. The study has shown a majority of the software/simulators work well on Windows platforms. From the study, it was observed that the open-source UAV simulator, AirSim which was launched by Microsoft in the year 2017 has got impressive features like support of Computer Vision and Deep Learning algorithms, modeling of real-world objects (important examples are poles, trees, buildings, and clouds), support of ample of amount of Unreal Engine environments, and sufficient availability of Physics Engines for both drones and cars. Moreover, the configuration file of AirSim provides full freedom for customization by the user. Some important configurations that a user can make are if the user wants car(s)/drone(s), number of vehicles, Field of View of the cameras, starting points of the vehicles, and resolutions of images, during a simulation. Hence, by considering these facts from the study, the AirSim simulator has been chosen to review some recent works on simulations related to UAV tasks and UAV applications.

5. Review on UAV applications simulation using AirSim simulator
This section deals with a short review on how AirSim simulator can be used for different UAV applications. It is seen that different AirSim environments like Neighborhood, Refinery, Landscape Mountains, Blocks environment, etc. have been used for simulating different UAV-based applications. The experiments have also used standard machine learning areas like Reinforcement Learning (RL), and Deep Reinforcement Learning (DRL) algorithms. In the
review, there are some experiments done using both AirSim simulator and in real time, whereas some have just done AirSim simulations.

Ho et al. have proposed a Q-learning-based method to train UAV landing. In the proposed method, UAVs are trained to achieve certain tasks both in the real and virtual environment. The virtual environment which has been used is AirSim. In the virtual environment, Q learning RL algorithm is used. In AirSim, UAVs are given six types of movements (i.e. in x, y, and z directions in both positive and negative directions). The success rate of the mission for 100 epochs is around 100%. Command-operated UAVs are used for transferring virtual environment model training to the real environment. The real environment consists of a UAV named Parrot Bebop 2, and the UAV is connected to the server through Wi-Fi. In a real environment too, six types of movements as that used for the virtual environment are performed (Ho et al., 2018).

Liu et al. have proposed a collaborative perspective algorithm in which a group of UAVs (one target agent which has degraded observation, and others are normal agents) captures the images of their surroundings. The target agent receives information from other agents and integrates this information which can give a prediction about its local observation. The datasets which are used for serving the purpose are different landscapes like mountains, roads, buildings, etc. from any AirSim environment. The desired communication happens through a three-way handshake mechanism and has three main phases: Request phase, Match phase, and connect phase. The experiments are performed using four settings: Hidden Target View with Multi-agent Way-point following, Accurate Pose with Multi-agent Way-point following, Inaccurate Pose with Multi-agent way-point following, Accurate Pose with Multi-agent Random Exploration. Around 10,000 to 20,000 images are collected for each experimental setting. Experimental analysis of the proposed algorithm with different experimental settings shows an overall average accuracy of around 66%. The proposed method also shows overall positive values for bandwidth improvement scores which indicate that the proposed method provides a good accuracy with lesser bandwidth when compared to centralized methods (Y.-C. Liu et al., 2020).

Table 4 shows a short review on AirSim simulations for different UAV applications. The review has been tabulated by considering different aspects like whether RL algorithm(s) has/ have been used or not, whether only AirSim simulations have been done or both simulations and real-time experiments have been performed, AirSim environment, and features of the works. In the table, SE stands for only simulations, and SRE stands for simulations and real-time experiments.

5.1. Lessons learned
Section 5 has shown our review on how AirSim simulations have been done to simulate some UAV applications and/or tasks. From the review, it is evident that a couple of works have used RL and DRL algorithms during the simulations. Several works have performed only simulations, and several others have implemented their designs both through simulations as well as in real-time. The review shows that in addition to several pre-built Unreal environments available to AirSim, the authors in different works have also customized their environments (such as a room of size 20 m*20 m, Mars Environment, a customized environment with an area of 240 m*240 m, etc.) which would be convenient to their designed UAV networks for certain applications. When complex environments are built or chosen for AirSim simulations, there is a possibility of a minute increase in the error rates of the experiments. Hence, usually a desktop with at least 8GB RAM, or 16GB (recommended) is chosen for such experiments.
6. Review on secure and efficient communication in IoD networks

A vast amount of data is being transmitted and processed in this era by IoD devices. These data are vulnerable to malicious software and attackers. Hence, there is a need to keep this data storage, processing, and data transmission secure and efficient. Cryptography is a technique that can provide secure data transmissions in an IoD network. Before transmission of data between any two communicating entities, the two entities should be initially authenticated, and then secure keys have to be established in the two entities. Hence, this motivates us to classify the IoD network security based on different Cryptography concepts used by IoD networks like key-agreement mechanisms, Authentication mechanisms, Blockchain mechanisms, Encryption and Decryption algorithms, and a combination of any/all these concepts.

This section deals with a review of security mechanisms/frameworks that have been used for maintaining secure communication in IoD networks. This section has four subsections for secure IoD communications: key management mechanisms/frameworks, authentication mechanisms/frameworks, blockchain-based mechanisms/frameworks, and other security mechanisms/frameworks. Figure 13 shows the taxonomy for Section 6.

6.1. Key management mechanisms/frameworks

This subsection shows a review on key exchange mechanisms/frameworks related to IoD communication.

Putranto et al. have proposed a method that built a transmitter system that proves to be secure against hijacking, eavesdropping, and Distributed Denial-of-Service (DDoS) attacks. The methodology used for the proposed scheme is System Development Life Cycle (SDLC) with a prototyping approach. The proposed scheme is implemented by using three prototypes. The analysis of the proposed scheme has shown that delay caused by encryption at the transmitter is around 10–30 ms, but more delay is caused by a signal received by the receiver and remote. The proposed scheme uses an android application for a web platform and an Advanced Encryption Standard (AES) algorithm for secure transmission. The proposed scheme has shown the result of a functional and non-functional test and proves the suitability based on different functional requirements. The distance testing analysis of the proposed scheme has shown that the drone can receive signals up to a distance of 10 km from the transmitter. The proposed scheme passes 100% of security tests against all attacks. User Acceptance test of the proposed scheme has shown that the application used for secure transmission satisfies the user requirements (Putranto et al., 2019).

Gope et al. have proposed an efficient authenticated key agreement scheme that preserves privacy for Edge Assisted UAVs. The system model of the proposed scheme consists of a group of UAVs, Mobile Edge Computing (MEC) operators, and a UAV service provider (USP). The proposed scheme has considered different security threats like authentication threats, privacy threats, location threats, physical security threats, and session-key security threats. Formal security analysis of the proposed scheme is done using the real-or-random model. The performance evaluation has shown that the proposed scheme has lesser computation cost at UAV (4.76 ms), lesser computation cost at USP (0.2 ms), lesser communication cost at UAV (224-Bytes), and lesser storage cost at UAV (96-Bytes) when compared to those of an existing MEC key agreement scheme. The performance evaluation of the proposed scheme also shows that the proposed scheme has an extremely low Total Authentication time when compared to that of an existing MEC key agreement scheme (Gope & Sikdar, 2020).

Tanveer et al. proposed a Lightweight Authenticated Key Exchange Protocol for the IoD (LAKE-IoD) environment. LAKE-IoD uses two models: A Network model and a Threat model. The network model is used for remote authentication, and the threat model uses Dolev and
Yao (DY). The proposed method uses Fuzzy Extractor (FE) for bio-metric verification of the user, and AEGIS for authenticated encryption. Formal security analysis validates mutual authentication property by using the Burrows–Abadi–Needham (BAN) logic rules for LAKE-IoD. When security features of LAKE-IoD are compared with those of some existing authenticated key exchange (AKE) schemes, LAKE-IoD proves to be the best among all. LAKE-IoD has lesser storage overhead when compared to that of a majority of existing AKE schemes, but more than that of one existing AKE scheme, but with compensation of providing higher security. The communication overhead and computational overhead of LAKE-IoD are the least when compared to corresponding parameters of some existing AKE schemes (Tanveer et al., 2020).

Zhang et al. have proposed a lightweight Authentication and Key Agreement (AKA) protocol that uses a one-way secure hash function and bit-wise XOR operations for the IoD. The network model of the proposed protocol consists of three entities: Mobile user, Control Server, and drones. Security analysis of the proposed method is done using Random Oracle Model (ROM) and shows that it can provide anonymity, un-traceability, and session key agreement. Security analysis of the proposed scheme shows that it has better security features when compared to the two existing AKA schemes. Performance evaluation of the proposed scheme shows that it has got minimum computation cost, and communication cost when compared with those of the two existing AKA schemes (Y. Zhang et al., 2020).

Sahingoz et al. have proposed a dynamic multi-level key management scheme for Wireless Sensor Networks (WSN) with the help of UAV which acts as a key distribution and coordination center. The network model of the proposed scheme consists of four main entities: Sensor nodes, a sink node, cluster heads, and UAV. Two types of attacks are possible for the proposed scheme: passive attacks, and active attacks. The sensor nodes contain their corresponding private keys, and also public keys present in the UAV. The proposed scheme uses periodic updation of keys, as well as updation of keys based on traffic volume threshold. In the proposed scheme, the nodes only store the shared key with the neighboring nodes, and public keys of the neighboring nodes, hence the storage cost reduces (Sahingoz, 2013).

Semal et al. have proposed a group authenticated certificateless key agreement protocol to ensure security in untrusted UAV networks communication. The protocol has two main phases: the initialization phase and the group key agreement phase. The group key agreement phase has a setup phase, two rounds, followed by a key generation phase. The experiment is conducted using two Rasberry Pi (one acting as client, and another as server), and a wireless router. The implementation has been done using C language. Analysis of the proposed scheme shows that it exhibits different security features like mutual authentication, mutual key agreement, joint key control, non-repudiation, forward secrecy, known key security, key freshness, conditional privacy, entity revocation, and key escrow elimination; and also the proposed scheme provides the best security features when compared with some existing authenticated certificateless key agreement protocols. Formal analysis of the protocol is done using the Scyther tool. Scyther tool shows that the proposed protocol provides different security features like session key secrecy, non-injective synchronization, non-injective agreement, aliveness, and weak agreement. The total time elapsed for the group key agreement phase through WLAN is 598 ms, and that through loop-back interface is 471 ms. The extra total time in the WLAN interface is due to (n-1) bilinear pairing operations (Semal et al., 2018).

Zhang et al. have proposed a gateway-oriented two-server password authentication key exchange protocol for edge computing applications that are UAV enabled. The proposed protocol combines the advantages of gateway-oriented protocol and two server password protocol. The communication model of the proposed protocol consists of a mobile user, a gateway, and two servers (only the channel between two servers is considered to be secure). The proposed scheme’s security analysis shows that it supports both gateway-
oriented settings and two server settings. The proposed protocol's security analysis shows that it has key privacy and mutual authentication features, which the other related schemes considered for comparison lack. Another advantage of the proposed scheme regarding security is that it has been proven in CDH assumption. Performance analysis shows that its mobile user computation time, ground gateway computation time, and server computation time are, respectively, 8.42 ms, 2.81 ms, and 12.64 ms. It has almost the same server computational time as that of another related existing two-server scheme and is lesser than that of 2 existing related two-server protocols. The proposed protocol's communication cost is 3808 bits and is more than that of two existing two-server protocols, and more than that of the gateway-oriented protocol. The communication cost of the proposed protocol is lesser than that of one gateway-oriented protocol (H. Zhang et al., 2020).

Yahuza et al. have proposed a Secure Lightweight Proven Authenticated Key Agreement (SLPAKA) mechanism for IoT deployment which allows drones addition to the IoT network. The IoT network of the proposed mechanism consists of four entities: MEC devices, Trusted Authority (TA) Centre, GCS, and different flying zones with their corresponding drones. The proposed mechanism uses Canetti Krawczyk (CK) adversarial model. The proposed mechanism uses the concepts of Elliptic Curve Cryptography (ECC). The proposed mechanism is implemented using Python. The protocol's formal security analysis is done using the ProVerif tool. Security analysis shows that the proposed mechanism has better security features when compared to some existing bench-marking techniques. The proposed mechanism's total computation cost is 13.68 ms and least when compared to that of other existing algorithms. The total communication cost of the proposed mechanism is 2496-bits which is higher than that of the two existing mechanisms and less than that of the four other existing mechanisms. Performance evaluation compares the performance of the proposed mechanism with Chen et al. (2020) mechanism. The performance analysis shows that when the number of iterations is high, the total energy consumption of entity X of the proposed mechanism is extremely less when compared to that of Chen et al. mechanism. The performance analysis also shows that when the number of iterations is high, the computational time of entity X is extremely less when compared to that of Chet et al. mechanism. The performance analysis also shows a similar level of total computational energy and total computational time differences even for entity Y between the proposed and Chet et al. mechanisms (Yahuza et al., 2021).

Fan et al. have proposed a password and position-based authentication key exchange (PPAKE) protocol for two application scenarios: drone authentication, and authentication in a military base. Based on position and password, PPAKE performs identity authentication and key exchange between UAV and GCS. UAV holds a legal identity and a GCS granted password. UAV should send encrypted identity, password, and position to GCS when it wants to send authentication and information transmission requests to GCS. GCS generates a session key if the information matches with the pre-stored information, else the request from the drone will be aborted. A similar method of request and information transfer between two entities happens even on a military base. PPAKE has two phases: the initialization phase, and the execution phase. The proposed protocol has got resistance to an active adversary when the standard security model is used. An adversary will find it difficult to guess the password because the adversary who can listen, modify and transfer messages can do password guessing through online attack only at a specified position. Moreover, authentication does not happen when the adversary impersonates any position and password (Fan et al., 2021).

Khan et al. have proposed a secure and efficient certificate-based access control and key agreement scheme which uses concepts of Hyper ECC (HECC) for FANETs. The proposed scheme's network model consists of Sensor drones, gateway drones, and ground station. D3 threat model is used by the proposed scheme. The formal security analysis is done using the Real-or-Random (ROR) model, and formal security verification is done using the Automated Validation of Internet Security-sensitive Protocols and Sensitive Applications (AVISPA) tool. The proposed
scheme’s security analysis shows that it has different security features like mutual authentication, preservation of anonymity. The proposed scheme has the best security features when compared to some related existing schemes. Performance analysis of the proposed scheme shows that its total computational cost is 5.76 ms, communication cost is 1280 ms, and they are the least when compared to corresponding performance metrics of some related existing schemes. The performance analysis also shows that the proposed scheme’s storage cost is 320-bits which is equal to that of an existing related scheme, and lesser than that of three existing related schemes (Khan et al., 2021).

Sharma et al. have proposed UAV-assisted heterogeneous network model in dense urban areas to provide resistance against the intrusion attacks, by the implementation of functional encryption technique in the model. The system model consists of UAV-assisted HetNet where UAVs act as relay nodes for wireless communication between User Equipment (UE) and Macro Base Station (MBS), where UEs are in Non LoS (NLoS) communication with the MBS. The proposed model uses a random way-point mobility model. The overall security architecture is validated using the AVISPA tool. The simulations are performed in two steps: data transmission in the overall network through the Functional Encryption technique, and in the second step is without Functional Encryption Technique. During the simulation of data transmissions of both the considered implemented phases using the first step, results display that the ongoing data transmissions are unsafe and that an intruder has been detected and its details also will be shown. During the simulation of data transmissions of both the considered implemented phases using the second step, results display that the ongoing data transmissions are safe due to the implementation of functional encryption technique in the proposed model (D. Sharma et al., 2020).

Tanveer et al. have proposed a robust authenticated key management protocol for IoD, called RAMP-IoD. The network model of RAMP-IoD consists of the following components: Sets of drones with their corresponding flying zones, Ground Station, Servers, Registration Center, and Remote User. RAMP-IoD uses the DY threat model. RAMP-IoD uses concepts of ECC. Formal security analysis is done using ROM, and security analysis is done using the Scyther tool. Implementation of RAMP-IoD and related schemes are done using Rasberry-Pi 3B with 1GB RAM, and quad-core 1.2 GHz processor. RAMP-IoD has a total computational overhead of 21.055 ms which is lesser than that of 4 previous related security schemes. RAMP-IoD’s communication cost during the AKM phase is 1856-bits which is lesser than that of four previous related security schemes. RAMP-IoD’s storage overhead is 1384-bits which is lesser than that of four previous related security schemes (Tanveer et al., 2021).

Table 5 shows resistance of some key exchange mechanisms/frameworks for IoD communication, to some attacks. It can be seen from the table that attacks like impersonation, replay, and Man-In-The-Middle (MITM) have been addressed for majority of the security mechanisms.

6.2 Authentication mechanisms/frameworks
Tian et al. have proposed an authentication framework based on MEC which preserves privacy and security in small-scale and resource-constrained IoT. The proposed scheme has got three entities: TA, MEC devices, and UAVs. In the proposed scheme, UAV takes full control of its key generation using signature without facing the Key Escrow problem. The proposed scheme provides security for IoD against different threats like authentication threat, privacy threat, and repudiation threat. The proposed scheme is efficient in terms of communication cost, computation cost, and storage overhead. The simulation uses UAVs which are served by Raspberry Pi 3 with a frequency of 1.4 GHz quad-core processor and with a memory of 1GB. The simulation validates the scalability of the framework since MEC with 50 and 100 UAVs was used (Tian et al., 2019).
Nikooghadam et al. have proposed a secure authentication scheme based on ECC for secure smart city surveillance through the IoD network. The network model of the proposed scheme has three components: a mobile user, a drone, and a control server. To provide security for the proposed scheme, it has used two threat models: DY, and CK. The proposed scheme’s formal security analysis is done using the Scyther software tool. Formal security analysis shows that the proposed scheme has no reported vulnerability; the freshness of parameters that are newly generated such as random numbers or timestamps. The proposed scheme’s informal security analysis shows that it satisfies the security properties like Authentication, Anonymity, and Availability. Performance analysis of the proposed scheme has shown that its execution time and computational overhead are minimal when compared to some existing IoD authentication schemes (Nikooghadam et al., 2020).

Ever et al. have proposed a secure authentication framework based on ECC for UAVs which act as mobile sinks in an environment WSN—UAV. Informal security analysis of the proposed framework shows that it offers properties of security like data confidentiality, mutual authentication, and session key agreement. Performance evaluation shows that the proposed framework has lesser computation cost and communication cost when compared to those of some existing algorithms (Ever, 2020).

Gope et al. have proposed an anonymous authentication scheme based on Physically Unclonable Functions (PUFs) for UAV applications that are Radio Frequency Identification (RFID) enabled. The experiment consists of two entities: A UAV with a tag, and a server unit. The proposed scheme's security and privacy analysis is done using Ouafii and Phan's security model. The proposed scheme provides mutual authentication. Performance analysis of the proposed scheme shows that it is better than the two existing PUF-based authentication schemes since it executes all three features: mutual authentication, scalability, and untraceability. Performance analysis also shows that the computation cost of the proposed scheme at UAV with tag side is lesser than that of two existing PUF-based authentication schemes; whereas, its computation cost at server unit is lesser than that of one existing PUF-based authentication scheme, and more than that of another existing PUF-based authentication scheme (Gope et al., 2021).

Li et al. have proposed a lightweight identity authentication scheme based on ECC for communication between UAVs and road base stations. The experimental setup of the proposed scheme has four main entities: UAVs, Road Base Stations, Communication links, and Trusted Center. The proposed scheme’s security analysis shows that it has security features like unforgeability, and traceability. Since the proposed scheme uses ECC, the authentication time of the proposed scheme is just about 1/163 part of that with the Rivest–Shamir–Adleman (RSA) algorithm, hence providing higher security with a smaller key size (Y. Li et al., 2020).

Alladi et al. have proposed a lightweight mutual authentication scheme based on PUFs for UAV to Ground station authentication, and UAV to UAV authentication; the proposed method is called SecAuthUAV. The proposed scheme consists of two models: The system model, and the Attack model. The system model of the proposed scheme consists of a ground station, legitimate UAVs, and an adversary drone. The proposed scheme's formal security analysis is done using Mao Boyd logic. The proposed method provides security features like key agreement provision, mutual authentication, forward secrecy, and user anonymity. Security analysis also shows that it provides better security features when compared to some existing UAV to Ground station authentication. The experimental simulations have been done using Node MCU 3.0 and Raspberry Pi 3B for the system model, and different operations have been simulated using C and Python programming languages. The proposed scheme's performance analysis shows that it has lesser computation cost on both Node MCU 3.0 and Raspberry Pi 3B when compared to that of some existing UAV to ground station authentication.
authentication schemes. Computation cost using Python implementation is more than that with C implementation. The communication cost of the proposed scheme is lesser than that of three existing UAV to ground station authentication schemes, and more than that of one existing UAV to ground station authentication scheme. The storage cost of the proposed scheme is lesser than that of three existing UAV to ground station authentication schemes, and more than that of one existing UAV to ground station authentication scheme (Alladi, Naren, et al., 2020).

Pu et al. have proposed a mutual lightweight authentication protocol called PCAP using PUFs and a chaotic system for securing the communications between UAVs and GCS. The network model of the proposed scheme consists of a ground station, legitimate UAVs, and a malicious UAV. A secret key is securely established based on PUFs’ challenge-response pair which forms Duffing map’s initial condition. Duffing map randomly shuffles the message bytes. The proposed method is resistant to MITM attack because the adversary lacks knowledge about the initial condition of Duffing map. The experiments have been conducted using the Objective Modular Network Testbed in C++ (OMNeT++) simulator. The proposed scheme does not require a server for secure session key establishment, hence the energy consumption is 0 at the server. The energy consumption in the ground station/user of the proposed scheme is lesser than that of an existing scheme, but the energy consumption in the UAV of the proposed scheme is more than that of an existing scheme (Pu & Li, 2020).

Alladi et al. have proposed a two stage lightweight mutual authentication scheme for software-defined network-backed UAV networks for surveillance purposes. The proposed algorithm is called PARTH (PUF-based Authentication for Remote Hovering Devices). The proposed scheme’s network model consists of four entities: GCS, Leader drone, mini drones, and malicious drone. Mini drones connect with a leader drone, and the leader drone communicates with the GCS. The proposed scheme’s main aim is to provide secure communication between leader drones and mini drones, and between GCS and leader drones. The proposed scheme’s security analysis is done using Mao and Boyd logic. The proposed scheme’s security analysis shows that it provides mutual authentication, message integrity, perfect backward secrecy, and perfect forward secrecy. Performance analysis shows that PARTH has the least mutual authentication time by the mini drones when compared to that of the two existing mutual authentication schemes (Alladi, Chamola, et al., 2020).

Abdel-Malek et al. have proposed a scheme of two fast and lightweight authentication mechanisms for UAVs in mmWave communication: drone to drone authentication, and drone to ground node authentication. Both the authentication mechanisms are based on proxy signatures. The system model of the proposed scheme consists of a control center, an observer drone, a group of other UAVs, and ground nodes. The control center is connected to the observer drone through LoRa link. mmWave Link is used for connecting the observer drone with the set of other UAVs, the set of other UAVs, for connecting UAVs with ground users, as well as for connecting a group of ground nodes. The proposed scheme’s implementation and testing are done using the NS-3 simulator by using the mmWave channel from the standard IEEE 802.11ad, and computations are based on Raspberry Pi. Security analysis shows that a legitimate UAV without its unique and valid proxy key cannot enter into the network. A replay attack by a malicious drone is not possible because of the stale timestamp value used in the captured message from a legitimate UAV. The proposed scheme’s results show that it is fast, scalable, and reliable for larger ad hoc networks (Abdel-Malek et al., 2020).

Xu et al. have proposed an effective UAV and dumb sensor authentication mechanism for RISTA missions. The system model uses three different types of devices: Dumb sensors, smart devices, and a UAV. The threat model considers two types of attacks: UAV impersonation, and Dumb sensor impersonation. Broadcast authentication of UAV uses µTESLA protocol, and authentication of dumb sensors uses smart device-assisted proximity-based authentication.
However, μTESLA protocol is enhanced by the addition of a physical covert channel which would provide security and low overhead one to many authentication. During UAV to sensor authentication, SHA-128 is used to generate a hash values chain. Covert channel authentication emulation is done using two Raspberry Pi 3 Model B boards. Authentication based on neighboring devices emulation uses six Raspberry Pi 3 Model B boards. The use of covert channels slightly increases the overhead. The correlation coefficient values of sensing signals of neighboring devices indicate that detection of sensors at different locations by neighbor devices-based authentication is accurate enough. Even when the distance between a smart device and a dumb device is as less as 10 cm, the correlation coefficient value is 0.8928 which is less than the threshold (0.95) (X. Xu et al., 2019).

Liu et al. have proposed a secure authentication mechanism based on large-scale UAV swarms' random labels. The proposed scheme performs label verification and generation for three entities: Among the UAVs; between swarms of UAVs, and ground stations, and relay stations; and for UAV swarm. Hash functions are used to generate labels, and SHA-256 is used for this purpose. The proposed scheme’s implementation is simulated using the OMNeT+ + simulator. By random guessing, an attacker tries to predict the uncertain labels, but the distribution of uncertain labels is almost a normal distribution and significantly reduces the likelihood of accurate prediction by the attacker. Moreover, detection of the wrong packet label would trigger an alarm to the system. Hence, the proposed mechanism is robust enough. The throughput of the proposed scheme reaches a maximum value of 19,000-bits/sec and a minimum of 1000-bits/sec, which shows that the proposed mechanism is feasible enough. Due to the use of multi labels for authentication, there is a huge reduction in overhead and space complexity when compared to that without multi-label authentication (L. Liu et al., 2019).

Hong et al. have proposed a data aggregate authentication scheme based on ID-based encryption. The proposed mechanism is called IBE-AggAuth. The system model consists of an airborne command and control platform (AC2P), clusters of reconnaissance UAVs each with a cluster head, and a cluster of attacking UAVs. A large amount of data is communicated between AC2P and reconnaissance UAV clusters and between AC2P and a cluster of attacking UAVs. IBE-AggAuth’s security analysis is done using a ROM. Aggregate signature validity can be guaranteed only after the validity of individual signatures. IBE-AggAuth’s unforgeable security is based on strength of the computational Diffie Hellman problem in ECC, and IBE-AggAuth is secure as long as the computational Diffie-Hellman problem of ECC is not solved. The communication cost of AC2P to reconnaissance UAVs and the communication cost of a reconnaissance UAV to its corresponding cluster head is the same for the IBE-AuggAuth scheme and unaggregation scheme. However, the communication cost of reconnaissance UAV cluster head to AC2P of IBE-AuggAuth is lesser than that of the unaggregation scheme (Hong et al., 2020).

Chen et al. have proposed a traceable and privacy-preserving authentication protocol that integrates different concepts like ECC, hash functions, and digital signatures for drone applications. The proposed scheme consists of four entities: A UAV manufacturing company, GCS, a mobile device (player), and TA center. Security analysis shows that mutual authentication happens between different entities in each phase, and BAN logic is used for the proof. Security analysis proves the integrity and confidentiality of the data transmission using ECC and Diffie Hellman algorithms. The use of digital signatures facilitates non-repudiation in the proposed scheme. The proposed scheme’s security analysis shows that it provides privacy and identity anonymity. Security analysis shows that it has the best security features among some existing schemes. However, the proposed scheme has higher overall computation and communication cost compared to that of an existing scheme (C.-L. Chen et al., 2020).
Cho et al. have proposed a framework called SENTINEL for mutual authentication between the GCS and drones, and for verifying the authenticity of drones in the IoD network. The experimental setup of the proposed framework consists of four main entities: Certificate authority, operator, drone, and ground station. SENTINEL uses different security protocols: Mutual authentication and key agreement protocol, drone authentication protocol. Drone authentication protocol can be divided into two subcategories: authentication between drone and ground station, authentication between drone and drone. Drone certificate format consists of six fields: version, issuer’s distinguished name, validity period, subject’s distinguished name, subject’s public key, and issuer’s signature. The digital signature of SENTINEL uses Elliptic Curve Digital Signature Algorithm (ECDSA) with SHA-256. SENTINEL’s certificate size is just about 0.272 times that of conventional X.509 v3 certificate and about 0.284 times that of compressed X.509 v3 certificate. The average execution time of SENTINEL’s mutual authentication and key agreement protocol is just about 0.55 times that of Transport Layer Security (TLS) for IoT, and the total message size of SENTINEL’s mutual authentication and key agreement protocol is just about 0.403 times that of TLS for IoT. The average execution time of SENTINEL’s drone authentication protocol is just about 0.325 times that of TLS for IoT, and the total message size of SENTINEL’s drone authentication protocol is just about 0.0437 times that of TLS for IoT. Formal security analysis of SENTINEL is done using ProVerif. Informal security analysis shows that SENTINEL has different security features like mutual authentication, anonymity, revocability, and that SENTINEL provides the best security features among some existing authentication schemes for IoD networks (G. Cho et al., 2020).

Pirker et al. have proposed a globally and secured operative UAV authentication system based on aspects of hardware security. The proposed scheme uses the combination of authentication by TLS, and the exchange of trusted location information and additional information about UAV through a secured communication channel. Hardware Security Module (HSM) is connected to UAV, which implements the TLS protocol of the proposed mechanism. The proposed mechanism also consists of I2C sensors. The authentication procedure of TLS uses X.509 certificates. The proposed mechanism has a protocol stack that extends the Open Systems Interconnection (OSI) model to interface HSM. The application running on UAV and the command library for HSM are written in C programming language. Integration of HSM which has protected storage for key materials in the proposed mechanism makes the mechanism resistant against physical attacks. I2C sensor values protect the proposed mechanism against remote attacks. Overhead evaluation of the proposed scheme is done using Raspberry Pi 3 with Wireshark. The drawbacks of the proposed mechanism are that necessary signaling of the sensor output introduces latency, and there is increased power consumption due to the requirement of HSM during operations (Pirker et al., 2020).

Chen et al. have proposed a mutual authentication scheme with enhanced Direct Anonymous attestation for UAV networks. The proposed scheme is called MA-DAA. The proposed scheme uses the concepts of ECC and pairings. The proposed scheme has three main entities: Issuer, Signer, and Verifier. The proposed scheme consists of three main protocols: Setup protocol, Join protocol, Sign/Verify protocol. The setup protocol is used for the establishment of system public parameters. Join protocol has four phases: The issuer request phase, trusted platform module (TPM) response phase, Issuer response phase, and Host verification phase. In sign/verify the protocol, TPM and host perform signing operation of a message and also generate DAA signature. The proposed scheme’s security analysis verifies the correctness of DAA certificate generation for the signature. TPM in the UAV network is secure and credible, hence the proposed scheme is secure. Performance analysis of the proposed scheme shows that its signature size is less compared to that of some existing DAA schemes. The proposed scheme’s total computation time in the Join protocol is about 0.711 times that of an existing DAA scheme. The proposed scheme’s total computation time
in the Sign/Verify protocol is about 0.5114 times that of an existing DAA scheme (L. Chen et al., 2018).

Srinivas et al. have proposed an anonymous and lightweight user authentication mechanism based on temporal credential for IoD networks. The proposed mechanism is called TCALAS. TCALAS uses the Authentication model and threat model (DY threat model). The network for TCALAS consists of a Ground Station Server (GSS), remote drones, mobile device, and a control room. ROR model and AVISPA tool are used for the proposed mechanism’s formal security analysis. Informal security analysis shows that TCALAS provides mutual authentication. Performance analysis of the proposed mechanism shows that its communication cost is least when compared to that of the other four existing schemes. TCALAS’s computation cost is more than that of the two existing schemes and lesser than that of the two other existing schemes (Srinivas et al., 2019).

Teng et al. have proposed an identity authentication mechanism based on ECC in UAV networks. The proposed scheme assumes that when a drone enters into a network, an attacker drone would initiate three types of attacks: message interception attack, fake ID attack, and replay attack. The proposed scheme uses an ECC digital certificate for credentials of UAV identification, ECDSA for UAV identification and signature verification, and Elliptic Curve Diffie Hellman (ECDH) algorithm for session key negotiation in the drone communication process. The performance evaluation of the proposed scheme shows that ECDH has a faster shared key generation process than that in the DH algorithm. Performance evaluation also shows that the average key generation time for ECC keys is lesser than that for RSA keys. It is observed that when key sizes are very large, the ECDSA signature process has better performance than that of the RSA signature process; ECDSA with a key size of 448-bits and RSA with a key size of 3072-bits have almost the same signing time. As the security and key length increases, ECDSA signature time becomes lesser than that of RSA. But the signature verification time for ECDSA is quite high when compared to that of the RSA signature algorithm. The key negotiation time for ECDH is quite less when compared to that of the DH key exchange algorithm (Teng et al., 2019).

Wazid et al. have proposed a novel user authentication scheme for the IoD network, in which an authorized user needs to access data directly from a drone. The proposed scheme’s network model consists of a control room, a server, an external user, and some fly zones each consisting of a drone and drone box. DY model is the threat model used for the proposed scheme. The simulations have been done using NS2.35 simulator on Ubuntu 14.04. Formal security analysis is done using the AVISPA tool. Performance evaluation of the proposed scheme shows that it has a communication cost of 1696-bits and is lesser than that of the two other existing schemes. Performance evaluation also shows that the proposed scheme has a throughput of 223.89bps, which is lesser than that of the 2 other existing schemes. The proposed scheme’s end-to-end delay is also the least when compared to two other existing schemes. But the proposed scheme requires more storage overhead for mobile user and server-side (Wazid et al., 2018).

Ali et al. have proposed a lightweight secure authentication scheme using lightweight symmetric encryption/decryption and hash operations for drones in smart city surveillance applications. The proposed scheme is called iTCALAS. The proposed scheme’s network model consists of a GSS, a control room, drones with their corresponding flying zones, and a drone user. Formal security analysis is done using ROM. The Proverif tool is used to verify the security properties of the proposed scheme. The proposed scheme provides security features like anonymity and untraceability of the user, mutual authentication, and robustness. The proposed scheme’s performance analysis shows that its communication cost is the same as that of an existing scheme, higher than that of another existing scheme, and lesser than that of three other related existing schemes. The proposed scheme’s computation cost is the
same as that of a related existing scheme, more than that of two other related existing schemes, and lesser than that of two other existing schemes (Ali et al., 2020).

Borisov et al. have proposed a secure authentication protocol based on ECDH, which can be used in robust command and control (C2) link security system of a UAV. The GCS and UAV both consist of a cryptography module and smart card. Initially, a connection is established between GCS and UAV. The connection establishment is used for generating and distributing session keys that can be used for encryption and calculating MAC. The cryptography module of communicating party sends a general authenticate command to its corresponding smart card, and the smart card generates the corresponding shared secret pre-master key. The corresponding cryptography module then reads the following data from the corresponding smart card: corresponding shared secret pre-master key, public key, and public key of the other communicating party. After this step, the communicating parties continue with transmission of messages, their corresponding public key, their corresponding random number, with the other communicating party (UAV to GCS, or GCS to UAV); generation of session encryption keys, a session key for MAC generation. After generation of session keys for MAC and encryption, encryption and decryption process, and MAC verification process happen in the two communicating parties. The process of generation of session keys will be repeated after every reboot. Identification of data packets and their structures during the transmission is hard due to dynamic encryption changes and MAC session keys. Retrieval of master keys is difficult due to the short-term use of keys for encryption and MAC calculation. Due to the use of external key storage, UAV battery consumption also reduces (Borisov et al., 2019).

Lei et al. have proposed an Optimized Identity Authentication protocol for IoD networks. The network model of the proposed protocol has four types of nodes: UAV, sensor, Access Point (AP), and Server. The proposed protocol has five processes: Broadcast, Response, Authentication, Verification, and Communication. The proposed protocol’s security analysis is done using the DY threat model. ProVerif is the security verification tool used for the proposed protocol. The proposed protocol provides different security features like Forward security, Backward security, and User anonymity. Security analysis also shows that the proposed protocol exhibits the best security features when compared to some related existing security protocols. The total communication cost of the proposed protocol is 1568-bits which is lesser than that of all the related security protocols, except one where the total communication cost of the proposed protocol is more than that of the compared related security protocol. The proposed protocol’s total time cost is 2.0622 ms which is more than 2 related existing protocols, but lesser than that of other related existing security protocols (Lei et al., 2021).

Chaudhry et al. have proposed a certificate-based generic access control scheme to provide inter drone and drone to GCS access control/authentication in the IoD network. The proposed scheme is called GCACS-IoD. The system model of GCACS-IoD consists of GCS, flying zones with their corresponding drones, and a Control Room. GCACS-IoD’s formal security analysis is done using the Real-or-Random oracle model. GCACS-IoD’s security analysis shows that it exhibits different security properties like mutual authentication, perfect forward secrecy, and known key secrecy. Security analysis shows that the proposed scheme is best when compared to some related existing schemes. The proposed scheme’s performance analysis shows that it has a running time of 17.9416 ms which is more than that of 2 related existing schemes, but lesser than that of 4 other related existing schemes. Performance analysis shows that the proposed scheme has a communication cost of 1664-bits with two message exchanges, which is the least when compared to other related six existing schemes (Chaudhry et al., 2021).

Hussain et al. have proposed a new authentication scheme based on ECC to provide secure communication between a drone flying in its corresponding flying zone and between a user.
The system model consists of four entities: flying zones each with a drone, GCS, Control Room, and Mobile Device (user). The proposed scheme's security analysis is done using ROM. Security analysis shows that the proposed scheme exhibits different security properties like User anonymity, Mutual authentication, and Untraceability. The proposed scheme's security analysis shows that it has the best security features when compared to some existing related schemes. The proposed scheme's performance analysis shows that it has a computation cost of 20.432 ms which is more than that of 3 other related existing schemes, but lesser than that of 3 other related existing schemes. The communication cost of the proposed scheme is 2208-bits with 3 messages exchanged, which is lesser than that of two other existing schemes, but more than that of four other existing schemes (Hussain et al., 2021).

Sun et al. have proposed a double authentication watermarking scheme for the UAV Adhoc network. The UAV Adhoc network in the proposed scheme has a distributed architecture and is based on clustering stratification. The complete network consists of a GCS, relay nodes, sink node, clusters with common sensor node, and cluster head node. The proposed watermarking scheme has three main steps: Collection node of each cluster uses collected data, hash function, and key for generation of authentication watermarking sequence and performs watermark embedding into the data packet. The cluster head node of each cluster received data from their corresponding collection nodes, authenticates the data packet, and performs cluster watermark generation and cluster watermark embedding operations. The sink node receives packets from cluster head nodes, performs verification of integrity and authenticity of collected data. Network simulations are performed in the OMNET++ simulator. LEACH routing protocol is used for clustering stratification. Security analysis shows that the attacks' selective forwarding, data replay, data tampering, and packet forging have a 100% correct identification rate, and the data transmission delay attack has a 90% correct identification rate. Results show that average delay decreases with an increase in alive node percentage. On average, the average delay of the proposed scheme is lesser than that of other related existing schemes. Its observed that for a simulation time of 15 min, the total energy consumption for the proposed watermarking scheme is around 100 kJ (Sun et al., 2020).

Jan et al. have proposed a secure, robust, improved, lightweight authentication protocol for providing security to IoD network, called Hash Message Authentication Code Secure Hash Algorithm 1 (HMACSHA1). The system model consists of GCS, a drone, and a certificate authority. The proposed protocol's formal security analysis is done using ROM, and ProVerif2.02 simulation. Security analysis shows that the proposed protocol is stronger when compared to some existing related protocols. The proposed protocol's performance analysis shows that it has a storage overhead of 1120-bits which is the least when compared to that of some existing related protocols. Performance analysis shows that the proposed protocol has a computation cost of 17.79 ms which is the least when compared to that of related existing protocols. The proposed protocol has a communication cost of 3720-bits which is lesser than that of just one related existing protocol and more than that of four other related existing protocols (Jan et al., 2021).

Table 6 shows the resistance of some authentication frameworks/mechanisms for IoD communication, to some attacks. It can be seen from the table that replay attack has been addressed for majority of the frameworks, followed by MITM attack and so on.

6.3. Review on IoD communication using blockchain
In this subsection, a short review has been done on how blockchain can be used to provide security in IoD communication. The review throws more light on cryptography-related concepts like authentication, confidentiality, integrity, and encryption and decryption, of the proposed methods, rather than on blockchain-related concepts of the proposed methods.
Aggarwal et al. have proposed a system model which consists of a public blockchain-based distributed network to provide secure drone communication. The main aim of the proposed scheme is to provide data authentication, data integrity, validation and verification (using Proof-of-Stake algorithm), authorization, accountability, and to protect identity anonymity. The proposed scheme’s analysis has shown that the total computation cost of the block creation process and block validation process is 768-bits. The proposed scheme has the same computation time of block creation and blocks validation each, i.e. 0.0023 ms. The proposed scheme satisfies its main aim and proves to be efficient compared to some existing schemes, hence increasing its reliability and scalability for real-time drone applications (Aggarwal et al., 2019).

Wazid et al. have proposed a secured communication framework for the blockchain of Internet Battlefield Things (SCF-BIoIBT) which uses drones for battlefield-related communication. The secure communication framework has been proposed because the IBT network is vulnerable to several cyber attacks. The system models used by the blockchain of the IBT network are the network model and threat model. Generation and Verification of signature provide data integrity and data authentication in the proposed scheme. The proposed scheme has set an aim to reduce computation cost, communication cost, and storage cost (Wazid, Das, et al., 2020).

Tan et al. have proposed a distributed key management scheme based on the blockchain for Heterogeneous Flying Ad-Hoc Network. The setup consists of multiple UAV clusters. Each cluster of UAVs consists of two types of UAVs: a head UAV that has strong transmission power, sufficient storage space, high computation ability; and multiple-member UAVs which can only support lightweight tasks. The implementation of the proposed scheme uses python programming to simulate the heterogeneous FANET with the 3D Guass Markov mobility model. AES 128, ECC-secp256k1, Schnorr signature based on secp256k1, and SHA 256; are used for symmetric encryption, asymmetric encryption, signature, and verification for easy implementation of aggregated signatures, and hash functions, respectively. The proposed scheme has also been analyzed by considering energy consumption for three parameters: number of requests, number of clusters, and size of clusters; each time keeping two parameters as constants, and the other one variable. In the proposed scheme drones update their keys anonymously, hence preventing the key escrow issue. The drawbacks of the proposed scheme are that it never anticipates the head UAVs to be attackers; due to the high mobility of drones with dynamic topology changes, it is difficult to realize accurate and high-quality communication in FANET (Y. Tan et al., 2020).

Bera et al. have proposed and analyzed a new blockchain-based secure framework for the management of data in IoD networks. The proposed scheme is called BSD2C-IoD. The system model consists of five main entities: Drone, Control room, Registration Authority, GSS, and Blockchain center. BSD2C-IoD’s formal security analysis is done using ROR oracle model, and formal security verification by using AVISPA tool. Informal security analysis shows that BSD2C-IoD exhibits different security properties like mutual authentication, and key agreement. Security analysis shows that BSD2C-IoD exhibits the best security features when compared to other related existing schemes. Performance analysis shows that BSD2C-IoD has a communication cost of 2240-bits which is the least when compared to that of other related schemes. Performance analysis shows that BSD2C-IoD has a drone computation cost of 11.022 ms which is lesser than that of 2 other related schemes and more than that of one other related scheme. Performance analysis also shows that BSD2C-IoD has a GSS computation cost of 4.378 ms which is the least when compared to that of other related existing schemes (Bera, Saha, et al., 2020).

Bera et al. have proposed a novel access control scheme for unauthorized UAV detection and mitigation in an IoD environment. The proposed scheme is called ACSUD-IoD. ACSUD-IoD
uses concepts of ECC. The network model consists of four main entities: Control Room, GSS, P2P Cloud Server Network, and flying zones which consist of legitimate drones and unauthorized drones. The threat model uses DY and CK adversary threat model. Formal security analysis is done using the ROR oracle model, and formal security verification is done using the AVISPA tool. Security analysis proves the correctness of the scheme. The proposed scheme's informal security analysis shows that it exhibits different security properties like mutual authentication, key agreement, anonymity and untraceability. Security analysis shows that the proposed scheme exhibits the best security features when compared to some related existing schemes. Performance analysis shows that the drone to GSS communication cost and drone to drone communication cost are 2368-bits and 1952-bits, respectively, with three communicated messages each. The average total communication cost of the proposed scheme is lesser than that of other related existing schemes. Blockchain implementation results show that the total computation time increases with an increase in the number of blocks that are mined. Blockchain implementation results also show that the total computation time increases with an increase in the number of block transactions (Bera, Das, Sutrala, et al., 2021).

Bera et al. have proposed an access control scheme based on blockchain in IoT enabled IoD environment. The scheme provides secure communication among drones, and also between drones and GSS. The proposed scheme is called BACS-IoD. The proposed scheme uses concepts of ECC, ECDSA, One-way hash function, and blockchain consensus algorithm. The network model consists of four main entities: Control Room, P2P Cloud Server Network, flying zones with their corresponding drones, and GSS. The attack model uses two threat models: the DY threat model, and CK adversary model. Security analysis proves the correctness of the proposed scheme. Formal security analysis is done using the ROR model, and formal security verification is done using the AVISPA tool. BACS-IoD exhibits different security properties like mutual authentication, and key agreement. Performance analysis of the proposed scheme shows that it has a drone to drone total communication cost of 1888-bits and a drone to GSS communication cost of 1728-bits, with three communicated messages each. The average communication cost of BACS-IoD is lesser than that of existing related schemes (Bera, Chattaraj, et al., 2020).

Wazid et al. have proposed an effective access control, authentication, and key management combined with a blockchain mechanism that forms a secure framework for Artificial Intelligence (AI)-enabled IoT-based drone-aided health-care services. The framework also uses concepts of ECC and ECDSA. The proposed framework’s network model consists of four main entities: GSS, drones, Control Room, and Peer to Peer Cloud Server networks. Based on the data received by Peer Peer cloud server networks, it can perform big data analytics by using Machine Learning (ML)/AI techniques. The threat model uses two threat models: the DY threat model and the CK adversary model. The simulations are performed on a platform with 4 GB RAM, Intel(R) Celeron(R) CPU, Ubuntu 20.04 64-bit OS. Blockchain implementations show that the total computation time increases with the number of mined blocks, and also with the number of each block transaction (Wazid, Bera, et al., 2020).

Islam et al. have proposed a blockchain-based surveillance architecture for marine vehicles in which drones perform surveillance and a 2-phase authentication process for verification of marine vehicles. The proposed architecture is named BUMAR. The network model of the proposed architecture consists of eight entities: satellite, UAVs, Control Center (surveillance boat or a remote center), civilian boats, edge server, base station, cloud server, and mobile core network. Each server plays the role of a validator and stores data in the blockchain. The experimental setup uses parrot bebop 2 UAV, raspberry pi 3 models are used for civilian boats and python for middleware. Performance evaluation of the proposed architecture is done by considering two metrics: authentication time, and energy consumption. The results show that the authentication time and energy consumption remain almost constant even when the
number of marine vehicles is increased from less than 25 to as high as 200. The authentication time and energy consumption of BUMAR are extremely less when compared to that of sequential search method, and slightly lesser when compared to that of hash map method. Even when the number of marine vehicles is 200, the authentication time is less than 1 ms, and the energy consumption is less than 0.01 J (Islam et al., 2020).

Ghribi et al. have proposed a secure communication mechanism for UAV networks, based on the integration of blockchain with ECDH key agreement protocol and one-time pad encryption method. The proposed mechanism uses a consensus algorithm called Proof of Communication. The proposed mechanism consists of a blockchain-based UAV FANET which has three entities: GCS, a leader UAV which is designated by GCS, and other UAV nodes. Since the network is a private blockchain network, UAVs’ public keys are known by GCS. In the network, the sender UAV can encrypt a message with the generated secret key, and the verifier UAV can decrypt the message. Blockchain authorizes a UAV before sending the message without the need for decryption. A sender needs to have 51% of endorsement UAVs for its verification, hence making an attacker compulsorily attack those 51% UAVs for causing harm to the complete network. One-Time Pad (OTP) encryption method ensures the safety of the blockchain system. Since blockchain uses ECC, the implementation complexity does not increase significantly. However, the key exchange process is vulnerable to a MITM attack (Ghribi et al., 2020).

Lv et al. have proposed a privacy protection scheme for UAV big data, by using blockchain technology. The proposed scheme uses concepts of blockchain and N-th degree Truncated polynomial Ring Units (NTRU) cryptography algorithm. The system model of the proposed scheme consists of four layers: blockchain layer, cloud layer, data layer, and user layer. The proposed scheme is executed in four stages: user data encryption stage, files upload and download stage, data recording in blockchain and user data reading from blockchain stage, and data exchange stage. Protection of data privacy and user private key privacy is preserved, due to encryption of exchanged data between users and blockchain center, and because of the NTRU password protection mechanism in the blockchain system. Considering the different NTRU parameters compatible with the X9.98 protocol, a key is selected to provide good performance without compromise in security. Results show that NTRU key generation takes the highest time, NTRU encryption consumes lower time, and NTRU decryption consumes the lowest time. Decryption time increases by hardly a ms when the key size is increased from 557-Bytes to 821-Bytes. NTRU cryptosystem shows the high efficiency of encryption and decryption. It has been observed that when the key size of NTRU is increased from 557-Bytes to 821-Bytes, the homomorphic encryption time of NTRU increases by around 6–8 ms. Multiplicative homomorphic encryption time is less than that of additive homomorphic encryption time, hence the proposed privacy protection scheme provides high security (Lv et al., 2021).

Xiao et al. have proposed a secure crowd monitoring UAV swarm system based on blockchain. The proposed architecture considers three aspects during the establishment of a UAV-based crowd monitoring system: identity authentication with high efficiency, secure drone swarm communication, and distributed data management. The proposed architecture consists of three layers: data layer, blockchain layer, and decision-making layer. The proposed architecture consists of three types of nodes: UAV node, management node, and monitoring node. The proposed architecture performs five main tasks: IoT and UAV devices registration, crowd monitoring tasks assignment, monitoring data upload and storage, monitoring data access control, and monitoring node management. The simulation platform is deployed on a local server that uses Intel Core2, 2.66 GHz. The information data, user’s private key signature, and signature verification are encrypted and decrypted by using the RSA encryption algorithm. Crowd monitoring tasks assignment task is performed using K-nearest neighbor algorithm. Performance analysis during IoT and UAV devices registration phase shows
that time overhead of key pair creation linearly increases with an increase in the number of accesses of UAV devices. Encryption, decryption, signature operation, and signature verification time overheads are relatively lower compared to that of key pair creation. During the UAV sub swarm task allocation phase, signature verification time overhead increases almost linearly with an increase in the number of UAVs. Moreover, the signature verification time overhead is more than that of task assignment, encryption, decryption, and signature operation. During the data upload and storage phase, decryption operation has the highest time overhead (W. Xiao et al., 2021).

Ferrag et al. have proposed an intrusion detection system and a blockchain-based delivery framework called DeliveryCoin for drone-delivered services. The threat model of the proposed framework consists of two networks: attack network, and victim network. A global external attacker is considered against the blockchain-based delivery platform. The global external attacker is located in the attack network, and the blockchain-based delivery framework is located in the victim network. The global external attacker can perform six types of attacks: DoS attacks, DDoS attacks, Brute Force attacks, Web attacks, Infiltration attacks, and Botnet attacks. The network model of the proposed framework consists of five entities: Package delivery service, Autonomous vehicle, Macro enB (5 G), Package buyer, and Package Vendor. Autonomous vehicles assume two types of vehicles: UAVs and self-driving cars. IDS performance is studied using Google Colaboratory and the blockchain platform is studied using a custom simulator built in Java. The accuracy of the proposed framework is analyzed using four classification techniques: support vector machine, recurrent neural network, CNN, and decision tree. Results show that CNN and RNN classifiers provide better effectiveness and accuracy results when compared to SVM and DT classifiers. CNN classifier has lesser training time when compared to that of RNN classifier. The proposed deliveryCoin framework has a lesser average communication overhead when compared to that of Paillier Cryptosystem-based DeliveryCoin (Ferrag & Maglaras, 2019).

Table 7 shows the resistance of some proposed blockchain frameworks/mechanisms for IoD communication, to some attacks. It can be seen from the table that attacks like impersonation and replay have been addressed for majority of the frameworks, followed by MITM attack and so on.

6.4. Other security mechanisms/frameworks

Steinmann et al. have proposed a data security model for Unmanned Aircraft System (UAS). The proposed security model aims to provide data security for communication link UAS to GCS, data security for board/memory chips of UAS, and authentication of data transmitted between GCS and UAS. UAS generates a key based on GCS’s seed, it uses this key and encrypts the data it captures using the AES-128 algorithm, hence providing resistance against Brute force attack, until a new key is generated. UAS sends the encrypted data as well as encryption of its encrypted data and its signature (second level encrypted data) to GCS. GCS uses its private key to decrypt the second-level encrypted data from UAS. GCS authenticates UAS based on UAS’s signature, uses its random key to generate a symmetric key, and decrypts the encrypted data of UAS. The proposed method has used Java for its implementation. The drawback of the proposed method is that it does not take care of security at GCS, hence if GCS is compromised, all the encrypted data until then will be compromised (Steinmann et al., 2016).

Li et al. have proposed a secure UAV communication scheme that is lightweight, that is based on the SM4 algorithm in improved CTR mode for the confidentiality of the transmitted message, and the HMAC algorithm SHA-1 for the integrity of the transmitted message. The proposed algorithm compares its performance in terms of encryption time cost and decryption time cost with those of the traditional algorithms SM4_CTR and ChaCha20. The analysis of three algorithms is done for data with different sizes in the range of 1KB to 2MB. Results of
the analysis show that when the data size is small, the encryption time cost and decryption time cost of the three algorithms are almost the same. But when the data size increases, the encryption and decryption time cost of the proposed communication scheme are lesser than those of the traditional SM4_CTR algorithm, but more than those of ChaCha20 algorithm (T. Li et al., 2019).

Sattar et al. have proposed a mechanism of Homomorphic encryption for secured aerial photography that is based on Nth Degree Truncated Polynomial Ring Units (NTRU) encryption algorithm which provides efficient encryption and decryption in software and hardware domain, faster key generation, and low memory consumption especially suitable for memory-constrained devices. The experimental setup uses each drone as a client and for a server, it uses an Amazon E2 cloud server. The proposed method considers three approaches for implementation, with improvement in every approach with respect to the previous one. Approach 1 requires a huge execution time for images with high resolution. Approach 2 resolves the issue of approach 1 by re-sizing the images before encryption, but with a compromise in the quality of images. Approach 3 resolves the issues of the two previous approaches by using images with less height, but with a probable cost increase because of the requirement of more clients. The analysis has shown that execution time is more for higher resolution images than that for images with bigger sizes. The analysis has also shown that execution time is linearly and directly proportional to NTRU Polynomial size (Sattar et al., 2017).

Ronaldo et al. have proposed a hybrid cryptography algorithm for secure drone communication in a cellular network (4G/Long Term Evolution (LTE)). Different information captured by drone sensors such as IMU sensor data, GPS sensor data, and battery usage status data are stored in a JSON file. A secure and lightweight communication model which is a combination of AES-256 (symmetric cryptography algorithm) and ECC (asymmetric cryptography algorithm) is used to transmit the JSON file from the drone to GCS. The proposed method is implemented on Raspberry Pi which is equipped with a drone. Random Key used by the sender is encrypted using receiver’s public key and ECC algorithm, and sensor data of drone is encrypted using AES-256 algorithm. The encrypted data and keys are sent to GCS over a 4G network, and to ensure the integrity of the sent data, hashing technique (SHA-256) is used. If the calculated hash value by GCS is the same as the hash value obtained from the drone, then it is assured that data has not been changed and the random key is generated by decrypting the keys obtained from the drone, and server’s private key using ECC algorithm. The encrypted data received from the drone is decrypted using GCS’s random key and by using the AES-256 algorithm. The analysis of the proposed scheme shows that the preparation time of transmitter node is more than that of receiver node, preparation time of transmitter node also depends on the type of Raspberry Pi used (Raspberry Pi 3 or 4), and authentication process time is longer at the receiver. The proposed algorithm has provided security against fake transmission of data from attacker nodes, by using SHA-256 (Ronaldo et al., 2020).

Allouch et al. have proposed a method to secure communication between GCS and UAV, which uses MAVLink protocol for communication. To validate the security of the proposed method, the implementation is done in ArduPilot by evaluating the performance through the development and integration of different encryption algorithms like AES-CTR, AES-CBC, RC4, ChaCha20 into UAV autopilot and GCS. The source code of the Mavlink protocol is modified to include the cryptography security aspect for the MAVLink protocol. The proposed method was implemented by simulating in ArduPilot SITL simulator and QGroundControl software. The experimental analysis of the proposed method has shown that MAVLink based on AES-CTR and ChaCha20 send more packets when compared to that of MAVLink based on AES-CBC and RC4. The analysis has shown that MAVLink based on ChaCha20 is suitable for low-powered real-time UAV communication. The analysis has also shown that memory consumption and CPU usage for Mavlink-ChaCha20 are the least when compared to those of MAVLink based on other implemented cryptography algorithms, but differences between memory consumption
and CPU usage of MAVLink and those of MAVLink-ChaCha20 are almost negligible, respectively (Allouch et al., 2019).

Nagbandi et al. have proposed a protocol for secret key generation between two UAVs, based on ground-stationed relay. The protocol is called Relay-Assisted Selective Inversion (RASI) Protocol. In the protocol, one UAV transmits a probing signal to other, and the received signal at the other UAV will be based on the probing signal and Additive White Gaussian Noise (AWGN). Similarly, the relay sends a probing signal to two UAVs, respectively, and the received signals at the two UAVs, respectively, will be based on the probing signal sent by the relay and AWGN. The variance associated with the UAV to relay channel is more than that of the UAV to UAV channel. Based on the corresponding received signals, the two UAVs generate their corresponding secret keys. The relay contributes to differential entropy. Analysis of the proposed protocol has shown that UAVs generate keys at a faster rate than those without using a relay. The UAVs will have lower computational complexity for the proposed protocol, with a drawback of negligible communication overhead because of the requirement of an additional phase of 1-bit transmissions by the relay (Nagubandi & Harshan, 2018).

Cheon et al. have proposed a Linearly Homomorphic Authenticated Encryption (LinHAE) scheme for the ground controller of a multi-rotor drone. The proposed scheme proves its confidentiality by proving a probability equation consisting of message and ciphertext, and its authenticity by proving that a negligible value is required for making the message unforgeable. The proposed scheme has considered an adversarial model by eavesdropping of the control signals, by injection of some signal in the network, by injection of some signal to control parameters, and by injection of some random signal to make the drone go wrong or fall. The proposed scheme has shown that securing the controller defends itself against forgery and eavesdropping attacks (J. H. Cheon et al., 2018).

Khanh et al. have proposed an efficient and safe scheme for the dynamic environment of drones. The proposed scheme uses the Anylogic software modeling tool, running on Windows 10, with executions done using Java for UAV swarms. Experiments have been conducted to calculate the authentication percentage of the proposed scheme and strong hash-based authentication scheme with 10%, 20%, 30%, and 40% malicious agents in the swarm of drones. Results of the experiments show that authentication is higher in the case of the proposed scheme when compared to that of a strong hash-based authentication scheme. The security analysis of the proposed scheme shows that it provides confidentiality, integrity, and mutual authentication. The security analysis also shows that the proposed scheme is resistant to attacks like MITM, DoS attack, Forgery attack, Replay attack, Insider attack, and Disclosure attack. The proposed scheme also has a good performance in terms of communication cost, computation cost, and storage cost. The proposed scheme has planned its future work to be time to time agreement of secret keys (Khanh et al., 2020).

Shoufan et al. have proposed a technique to authenticate the drone flight data continuously based on the behavior of UAV operator who manually operates the drone. The proposed technique uses a Hummingbird quad-rotor drone and a standard transmitter from Futaba. The proposed technique shows that the drone operator is a unique signature that can be used for operator authorization and detect malicious commands to provide resistance against hijacking attacks on the drone. The results have shown that drone operator identification accuracy for Random Forest Classifier is highest and that the accuracy increases with an increase in the number of trees. The results have also shown that the identification accuracy is different for different feature signals. The proposed technique does not show its performance for unseen flight data from attackers, and it does not address autonomous drone flights (Shoufan, 2017).
Xion et al. have proposed a resource-efficient encryption scheme for video-sensing system based on UAVs. The hardware platform has three modules: a control module, a module for processing data, and a video sensing module. The Security and Freedom Through Encryption (SAFE) encryption scheme is used for the encryption of continuous data and is best applicable for multimedia encryption. However, for wireless transmission modules, the SAFE encryption scheme cannot be used since there will be issues like packet loss and bit error. For the Wireless transmission module, Packet Oriented SAFE (POSAFE) scheme is used. The SAFE scheme consists of a speed control parameter called “l” which should be saved in a separate file or as an encryption flag EF. The experimental simulation is designed in C++. The experimental analysis shows that when “l” is small, SAFE throughput values grow almost linearly, but when “l” is large, SAFE throughput values start converging at some constant values in the order of a few GBps. Performance analysis has shown that the proposed scheme is efficient enough to support real-time data encryption in embedded video sensing systems especially based on UAVs (C. Xiao et al., 2016).

Fernando et al. have proposed a mechanism for reconciliation of independently derived secret keys based on Reed Solomon (RS) code, for secure communication at wireless PHY layer or upper layers, between a UAV and a controller in an environment that is semi-mobile. The proposed mechanism uses adaptive secret key “L” and a scaling factor ‘α’. The communicating parties generate shared keys based on the probing packets transmitted between the two communicating parties, and the corresponding noise components in the channel. The adversarial model has got an eavesdropper Eve who is assumed to be passive and stationary. The analysis of the proposed mechanism shows that there has been an improvement in bit mismatch rate when compared to some existing algorithms. The analysis has shown that due to the use of the loss-less quantization method, the secret bit extraction improves between the two UAVs (Fernando et al., 2017).

Deebak et al. have proposed a smart IoD (S-IoD) framework by using a lightweight privacy-preserving scheme (L-PPS) for a UAV environment that collects sensible information independently. L-PPS uses Chebyshev Chaotic Maps. Formal security analysis uses a software tool called Scyther, and a ROM. The proposed scheme’s informal security analysis shows that it provides data confidentiality, and is resistant to attacks like forgery, replay, password guessing, session key-disclosure, privileged insider, stolen smart card, server spoofing, DoS, drone capture, and Wi-Fi. The proposed scheme’s performance analysis shows that it has lesser computation and communication cost when compared to those of some existing authentication schemes. The experiments are performed using NS3 simulator to support protocols such as Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and LTE. The experimental analysis shows that the proposed scheme has a higher throughput rate, higher packet delivery rate when compared to those of some existing authentication schemes. Also, the proposed scheme has better performance metrics like the end-to-end delay and time for each drone to connect when compared to those of some existing authentication schemes (Deebak & Al-Turjman, 2020).

Verma et al. have proposed a Certificate-based Proxy Signature (CB-PS) for the UAV network for attacks mitigation. The proposed scheme’s security analysis shows that it has security features like the authentication of source, message integrity, signer identifiability; and is resistant to attacks like modification, impersonation, replay, and MITM. The proposed scheme’s efficiency analysis shows that its signature has the least bit size among some of the existing Designated Verifier Proxy Signature (DVPS) schemes. Efficiency analysis also shows that the proposed scheme has the least total signature computational time among some existing DVSP schemes (Verma et al., 2019).

Bera et al. have proposed an access control protocol scheme for IoT environment assisted by drones, to provide secure battlefield surveillance. The scheme is called ACPBS-IoT. ACPBS-
IoT uses DDoS threat model. Formal security analysis is done using ROR model, and formal security simulations are done using the AVISPA tool. Informal security attack shows that the proposed scheme is resistant against attacks like replay, MITM, impersonation, device physical capture, privileged insider, ESL, and Insider. The proposed scheme is implemented using High-Level protocol specification language. The minimum, maximum, and average execution times of different cryptography primitives of the proposed scheme are estimated using the MIRACL library on Raspberry Pi 3 setting as well as MIRACL on the server setting. Computation cost at drones for the proposed scheme is least among the existing schemes; computation cost at the server/GSSs is more than that of one existing scheme and lesser than that of another existing scheme. The communication cost of the proposed scheme is more than that of one existing scheme and lesser than that of three other existing schemes (Bera, Das, Garg, et al., 2021).

Haque et al. have proposed a novel, secure, and lightweight framework based on identity-based encryption for UAV network. The proposed work is slightly inspired by research on lightweight security enforcement for Cyber-Physical Systems. Three main aims of the proposed framework are computation overheads distribution, system lightweightness, and obscuring transmitted data, and digital data right management. Architecture for overhead distribution consists of a base station, and clusters of UAVs each with a cluster head. Cluster heads are elected routinely and dynamically. System lightweightness is achieved through Identity-based encryption and selective data encryption. Identity-based encryption uses ECC, hence provides high security, lower bandwidth, lower power consumption, and lower computational requirements. Selective data encryption can be used for different formats of data like text, images, audio, and videos; and it reduces the overhead for the encryption/decryption process without compromise in the security of the devices. The third aim of the proposed framework is achieved through the steganography technique. The proposed scheme also provides other security features like forward and backward secrecy, and resistance against node capture attack (Haque & Chowdhury, 2017).

Kim et al. have proposed a drone security module for secure data transmission and security of stored information. The drone security module consists of a Micro Controller Unit and a secure element which are responsible for actual security functions. The connection between a mission computer/flight controller and the drone security module is established through a USB interface. The secure element can perform various tasks like generation and verification of a digital signature, key agreement, symmetric and asymmetric encryption, and decryption. The secure element has three layers: Application layer, Kernel layer, and Hardware layer. The software driver of the drone security module is implemented using C/C#/Java and can be used on different OS like Linux, Windows, macOS, and Android. Nvidia Jetson TX2 is the mission computer that is used. The proposed scheme exhibits different security features like key management, certificate management, authentication, and key agreement. The limitation of the proposed scheme is that the data fed as input to encryption are not actual telemetry data (Kim & Kang, 2020).

Atoev et al. have implemented OTP technique for secure communication link in the UAV network. The experimental setup consists of a UAV, a GCS, and an attacker, and the communication happens through the MAVLink protocol. The experiment uses two 3-DR 915 MHz telemetry radios for communication over the data link. The implementation of encryption and decryption of data communicated between GCS and UAV is done by using C++. Result analysis shows that the OTP encryption technique provides an accuracy of 95% which is better than that of AES-128, Twofish, and Triple Data Encryption Standard (DES) algorithms. Result analysis also shows that the execution time of OTP for a 10MB file is around 2 seconds, and in general the execution time of OTP is lesser than that of AES-128, Twofish, and Triple DES algorithms (Atoev et al., 2019).
Khan et al. have proposed a secure and efficient key encapsulated certificateless sign-cryption scheme based on Hyper ECC for UAV network. The experimental setup consists of three main components: UAVs, a GCS, and KGC. The proposed scheme uses the DY threat model. The proposed scheme’s formal security analysis is done using the AVISPA tool. Formal security analysis proves the confidentiality of the proposed scheme. The proposed scheme’s informal security analysis shows that it provides different security features like resistance against replay attack; integrity, and forward secrecy. Performance evaluation shows that the proposed scheme has a total computation cost of 2.4 ms, which is the least among the other related existing schemes. The proposed scheme’s communication cost is 1264-bits which is the least among the other related existing schemes. The proposed scheme has been used for crop health monitoring applications (Khan, Ullah, Nisar, Noor, Qureshi, Khanzada, Amin, et al., 2020).

Won et al. have proposed a secure communication model between drones and smart objects. The protocol is called efficient Certificateless Signcryption Tag Key Encapsulation Mechanism (eCLSC-TKEM). The proposed scheme has explained its application for smart parking management. The use of drones and sensors makes parking management cheaper and efficient. The proposed protocol has experimented on A.R. Drone 2.0 and TelosB sensors. The computation time of the proposed scheme with secp192r1 is 13.03 s and is the least among the existing related schemes. With a wake-up interval of 9 s, the proposed protocol has a mission completion time of 46.8 s, and it significantly saves energy when compared to other related existing schemes. With an altitude of 20 m, the proposed scheme has a mission completion time of 47 s. When dual channels are used in the proposed protocol, the completion time reduces significantly when compared to a single channel. Security analysis of the proposed protocol depends on one-sided gap Diffie Hellman problem (OGDH), one-sided decision Diffie Hellman oracle (ODDH), and Elliptic Curve Discrete Log problem (ECDLP). The proposed protocol exhibits 4 security features: user authentication, key agreement, user revocation, and non-repudiation (Won et al., 2015).

Sparrow et al. have proposed an encryption algorithm called LEOPARD which is based on Permutation Substitution design, for tactical UAVs. LEOPARD algorithm is similar to AES algorithm, except that the order of operations in LEOPARD encryption from first to last but one round are Mix column, add round keys, and shift rows. The operations in the last round of LEOPARD are Substitute Bytes, Shift Rows, and Add round key. Preliminary statistical analysis is done for both AES and LEOPARD with a payload size of 256-Bytes and 10 rounds of operations. Arithmetic mean and serial correlation tests are the two statistical tests performed on the two algorithms. Preliminary statistical analysis shows that LEOPARD has an entropy of 7.19, arithmetic mean of 134.7, and serial correlation of 0.07. Preliminary statistical analysis shows that random output generation can be done by using LEOPARD as it can be suitably done by AES. The actual experimental setup consists of a human operator, a base station, and a fixed-wing tactical UAV. The human operator and the tactical UAV use microchip PIC18F45K22. Testing of the algorithm is done using an emulated platform to check the impact of LEOPARD on some aspects of UAV performance metrics. Analysis shows that LEOPARD has got increased throughputs when compared to AES for the corresponding set of payload sizes, reduced latency for a corresponding set of payload sizes, and reduced power consumptions for a corresponding set of crystal frequencies (Sparrow et al., 2016).

Ozmen et al. have proposed an efficient cryptography framework for small aerial drones. The proposed framework has used low-cost public-key cryptography (PKC) primitives and low-cost symmetric key primitives. The low-cost PKC primitives are an integration of Boyko-Peinao-Venkatesan (BPV) FourQ on ECDH protocol, integration of BPV FourQ on Schnorr digital signature, and integration of BPV FourQ on Elliptic Curve Integrated Encryption Scheme (ECIES) protocol. The low-cost symmetric key primitives are CHACHA20 stream cipher, CHACHA-POLY as authenticated encryption scheme, and POLY1305 as MAC protocol. The
| Ref | Model or logic | Authors | Features |
|-----|----------------|---------|----------|
| (Ouafi & Phan, 2008) | Ouafi and Phan model | Khaled Ouafi and Raphael C W Phan | • Used for formal security analysis of RFID-based authentication protocols.  
• Used to verify tag anonymity and tag untraceability properties.  
• An adversary is capable of issuing the following queries in the communication network: Execute, Send, Corrupt, and Test. |
| (Bellare & Rogaway, 1993) | Random Oracle Model | Mihir Bellare and Phillip Rogaway | • Provides a bridge between cryptography practice and cryptography theory.  
• Replaces the random oracle with an object like a hash function.  
• Candidate instantiations use hash functions in different ways: truncated hash output, restricted input length of hash functions, and hash functions used in a non-standardized manner. |
| (Burrows et al., 1989) (Boyd & Mao, 1993) | BAN logic | Michael Burrows, Martin Abadi, and Roger Needham | • Differentiates different types of objects or statements like principals, encryption keys, and formulas.  
• Uses statements for the identification of messages.  
• Considers different properties for each protocol: protocol goal, whether secret keys are used or not, type of cryptosystem used, redundancy, bugs, whether or not the protocol proves the presence of each participating entity to the other, and whether timeliness of the messages are guaranteed with nonces or synchronized clocks.  
• BAN logic also has some limitations: incapability to express some events, lack of precision in movement from a protocol description to logical expression, misjudgment of some insecure protocols to be secure. |
| Ref                  | Model or logic | Authors                              | Features                                                                 |
|---------------------|----------------|--------------------------------------|--------------------------------------------------------------------------|
| (Mao & Boyd, 1993)  | Mao Boyd logic | Wembo Mao and Colin Boyd             | • Adopts BAN logic’s basic notation framework, and a more formalized approach.  
• Has few rules for formalizing authentication and confidentiality scenarios: authentication rules, confidentiality rules, nonce verification rule, the super principal rule, the fresh rule, the good key rules, and intuitive rules. |
| (Gong et al., 1990) | GYN logic      | Li Gong, Roger Needham, and Raphael Yahalom | • Provides a systematic way of understanding the cryptography protocols.  
• does not need several universal assumptions as that of BAN logic.  
• differentiates between the content of a message and the information implication of the message.  
• Regards each protocol as a distributed algorithm. |
security of the proposed framework depends on the FourQ curve and BPV precomputation technique. The experiment for the proposed framework was conducted on Crazyflie 2.0. FourQ curve provides the same security as that of secp256k1 curve. The security of the proposed framework is almost the same as that of the standard framework. The key exchange of the proposed framework has an energy consumption of just 3.61% of the key exchange energy consumption of the standard framework. The digital signature energy consumption of the proposed framework has an energy consumption of just 2.83% of the digital signature energy consumption of the standard framework. The proposed framework's authenticated encryption has an energy consumption of 14.42% of the standard framework. The proposed framework's integrated public-key encryption energy consumption is just 3.61% of the integrated public-key encryption energy consumption of the standard framework (Ozmen & Yavuz, 2018).

He et al. have proposed a certificateless designated verifier proxy signature (CLDVS) scheme to solve problems of key escrow and digital certificate management, for UAV networks. The network model of the proposed scheme consists of a Command center, GCS, and a UAV. The command center acts as the original signer, GCS acts as the proxy signer, and UAV acts as the designated verifier. The proposed scheme has successfully verified its correctness. The proposed scheme's security analysis uses ROM, and it proves its unforgeability under an adaptive chosen message attack. Efficiency analysis is done by comparing the proposed scheme with other related existing signature schemes. The proposed scheme's delegation generation time is higher than that of an existing Certificateless Proxy Signature (CLPS) scheme and lesser than that of other related existing CLPS schemes. The delegation verification time of the proposed scheme is the least when compared to other related existing CLPS schemes. The signing-time of the proposed scheme is higher than that of an existing CLPS scheme and lesser than that of other existing CLPS schemes. The proposed scheme's verification time is higher than that of an existing CLPS scheme and lesser than that of other existing CLPS schemes. The signature time of the proposed scheme is the least when compared to other related existing CLDVS schemes. The verification time of the proposed scheme is higher than that of an existing CLDVS scheme and lesser than that of other existing CLDVS schemes (He et al., 2021).

Rabieh et al. have proposed a proxy re-encryption scheme for efficient and secure sharing of drone videos in scenarios of public safety. The proposed scheme's network model consists of a control center, cloud storage, drones, and first responders (police, ambulance personal, and firefighters). The control center generates keys for first responders and interacts with other entities through LTE networks. The proposed scheme exhibits different security features like the privacy of passengers' location, availability of surveillance videos, mitigation of collusion attacks, and mitigation of MITM attack. The assessment of communication performance is done using NS3.27. Performance analysis shows that the exponentiation computation time is 0.15 ms, DSA signature computation time is 0.85 ms, and DSA verification computation time is 0.62 ms. Performance analysis shows that communication overhead is high for video frames of higher resolution and higher quality. Performance analysis shows that for a single frame of resolution 160*120 at 50% it takes 0.1512 s for complete re-encryption and decryption process. Performance analysis shows that transmission time increases with an increase in the quality of frames (Rabieh et al., 2020).

Hussein et al. have proposed Authenticated Encryption New One Time Pad (AENOTP) algorithm to provide confidentiality, authentication, and integrity of data transmission between UAV and Base station. The proposed scheme consists of two double AES-256 algorithms, RC4 algorithm is used as Pseudo-Random Number Generator (PRNG), some XOR operations, and tag partitioning. Tag partitioning reduces the delay time of re-transmitting wrong blocks. Security analysis shows that the proposed scheme is resistant to different attacks like linear cryptanalysis, differential cryptanalysis, divide and conquer, sliding, algebraic, correlation,
related key, and Binary Decision Diagram. The proposed scheme’s performance analysis shows that it has got a throughput of 256-bits which is double that of the ASC-1 algorithm, the proposed algorithm has no error propagation, and the proposed algorithm is faster than the ASC-1 algorithm by 60% (Hussein et al., 2017).

Dong et al. have proposed an improved image scrambling algorithm based on Fibonacci-p coding for wireless image transmission systems of UAVs. The system model for the proposed algorithm consists of different entities like UAV, early warning machine, reconnaissance aircraft, satellite, field commander, field command vehicle, satellite ground station, rear command center, emergency control system, and individual portable wireless image transmission system. Input to the proposed algorithm is an unscrambled color or grayscale image, and the output of the algorithm is the corresponding scrambled color or grayscale image. Correlation coefficient analysis of horizontal pixels shows that for the proposed algorithm the correlation distribution is more dispersed when compared to that of the original image scrambling algorithm, hence the improved image scrambling algorithm provides a better encryption effect and more security when compared to that of the original image scrambling algorithm. Histogram analysis has been done for the original image, image encrypted using original image scrambling algorithm, and image encrypted using improved image scrambling algorithm. Histogram of the encrypted image for improved image scrambling algorithm is almost in concentrated form and has more uniform distribution when compared to that of an encrypted image from the original image scrambling algorithm. Entropy analysis shows that the original image has an entropy of 3.36, the entropy of encrypted image using the original image scrambling algorithm is 6.86, and entropy of encrypted image using the improved scrambling algorithm is 7.04; hence, the encrypted pixels from the proposed algorithm have higher randomness. The encryption and decryption time of the image scrambling algorithms are almost the same. The encryption time of a “Baboo” image through an improved image scrambling algorithm is just 29.35% of that through the original image scrambling algorithm (Dong et al., 2018).

Won et al. have proposed a look-up table-based shuffling mechanism that uses white-box cryptography for UAV applications. The white box block cipher used for the proposed mechanism is based on a dynamic SPACE encryption scheme. SPACE algorithm provides the same security as that of AES, hence an interceptor cannot obtain any data about plaintext from the ciphertext. The proposed mechanism uses ECDH key agreement protocol, and ECDSA. ECDSA algorithm prevents the impersonation of the control station. Impersonation of UAV is prevented by using a shuffling mechanism based on a White box block cipher. The experimental setup uses a GPU-enabled SoC. An attacker cannot extract the secret key that is used to generate the lookup table. Even if an attacker gets to know the shuffling shared seed of a particular period between UAV and control station, the attacker will find it hard to extract the data because of the large table size and short residence of the shared shuffling seed. The control station measures the response time, and since a large number of shuffling rounds are used, it can easily detect malicious behaviors, since malicious behaviors would require additional memory access. Performance analysis shows that the encryption performance (kB/sec) is highest when a GPU is used with shared memory when compared to that when GPU with global memory, and when CPU is used for a particular SPACE block cipher. The energy consumption is measured using DJI Phantom 3 drone. The energy consumption is less with the use of GPU, hence increasing the operation time of UAV (Won et al., 2019).

Prapulla et al. have realized secure communication mechanisms for the transmission of data between MAV and GCS. The algorithms used for the realization of secure communication mechanisms are AES-128 in CTR (Counter) mode for encryption and decryption, SHA-256 for key hashing, and Diffie Hellman for key exchange. MAVLink is the communication protocol used between MAV and GCS. MAVLink algorithm and the security algorithms are implemented both on GCS and the MAV autopilot side. Mission Planner is the open-source GCS that is used.
Before implementation of the algorithms on an actual MAV-GCS platform, a feasibility study of the algorithms was done using MATLAB which proved to be feasible (Prapulla et al., 2016).

Abdallah et al. have proposed an efficient networking and security architecture for disaster surveillance through a UAV system. Communication in the UAV system happens through the IEEE 802.11ah standard. The proposed architecture uses lightweight Ring Learning With Errors (Ring-LWE) cryptosystem to ensure the confidentiality of exchanged messages with low computation overhead. The system model of the proposed architecture consists of a TA, a central substation, relay nodes (not used for monitoring), and groups of UAVs for disaster surveillance of different sub-areas of the complete disaster area. The proposed architecture ensures the integrity of readings transmitted during monitoring operation, integrity of exchanged messages during join/leave process, and the integrity of message readings even in presence of compromised monitoring drones/cluster head drones. The proposed architecture provides information availability even when a whole group of drones is compromised. The proposed architecture makes sure that only the control station receives the desired plaintext readings messages, CS receives accurate readings even in presence of some compromised drones, and that the adversaries cannot even read the plaintext nor falsify them. Ring-LWE is resistant to post-quantum attacks. Performance analysis shows that for a particular number of drones in a group, the computation overhead per group using Ring-LWE is extremely low when compared to that with RSA cryptosystem. Performance analysis also shows that the cluster head of a group consumes more energy than that by any other ordinary drone just used for scanning an area and collecting data, but the difference is low because of the low communication and computation complexity of the proposed architecture (Abdallah et al., 2019).

Ko et al. have proposed a secure drone communication protocol for secure communication between UAVs, and secure communication between GCS and UAV, in military scenarios. The system model of the proposed protocol consists of ordinary UAVs, monitoring UAVs, a GCS, and a certificate authority. The proposed scheme uses DV threat model. It is assumed that the GCS and the UAVs are pre-configured with digital signature (ECDSA), encryption and decryption, cryptography hash algorithms (HMAC), and pseudo-random number generator. The security algorithms for the protocol are coded using Python 3.8. The actual experimental setup consists of UAVs which are equipped with Raspberry Pi, and Pixhawk flight controller; and an 11GB RAM laptop with Ubuntu which acts as the GCS. The formal security analysis is done using BAN logic and Scyther automated tool. Security analysis shows that the proposed protocol has different security features like confidentiality, integrity, mutual authentication, non-repudiation, perfect forward secrecy, perfect backward secrecy, response to MITM attack and DoS attack, and drone to drone security support. The security analysis shows that the proposed protocol is best when compared to security aspects of four existing related protocols. Performance analysis of the proposed protocol shows that the total latency of UAV to GCS secure sub-protocol is 213.2196 ms, and that of UAV to monitoring UAV secure sub-protocol is 29.2 ms. Performance analysis shows that similar to the 2 existing related protocols, the proposed protocols cannot avoid the large computational overheads when they provide both perfect forwards and backward secrecy. Due to the strong session key generated during sub-protocol drone to GCS, and during drone to monitoring drone, the proposed protocol has relatively lightweight computation with high security when compared to other existing protocols (Ko et al., 2021).

Tan et al. have proposed a UAV authenticated group association design in which UAVs are used as auxiliary facilities which improve the transmission availability and transmission quality of Road Side Units (RSU) aided Vehicular Ad hoc Network (VANET). The UAVs act as message forwarding and transmitting nodes in the vehicular communication process. Security analysis of the proposed scheme shows that it has different security features like Unforgeability, Conditional Anonymity, Session Key Establishment, Key Escrow Resilience, Scalability, Efficient key updation, Collusion attack resilience, vehicle to vehicle connectivity,
and ununlinkability. The proposed protocol has got best security features when compared to three other existing schemes. Performance analysis shows that the computation cost on the RSU side increases from around 25 ms to 35 ms when the number of vehicles is increased from 5 to 50. But for other existing protocols, the computation cost on the RSU side increases from around as little as (9–15 ms) to as high as (50–60 ms) when the number of vehicles is increased from 5 to 50. When there are 10 vehicles, the RSU overhead for the proposed protocol is more than that of 1 existing protocol and lesser than that of 2 other existing protocols. Hence, the proposed protocol has reasonably better performance when compared to three existing related protocols (Tan & Chung, 2021).

Khan et al. have proposed a lightweight security scheme called identity-based signcryption which is based on Multi-access Edge Computing (MEC) and uses concepts of HECC. The network model of the proposed scheme consists of a MBS, Small cell Base Station (SBS), MEC-UAV, Monitoring UAV (M-UAV), and core network. DY threat model is used by the proposed scheme. MEC-UAVs are equipped with Raspberry Pi which is powered by a 1.5 GHz quad-core 64-bits ARM cortex-A72 processor. Informal security analysis shows that the proposed scheme has different security properties like confidentiality, integrity, unforgeability, and resistance to replay attack. The proposed scheme has the best security features when compared to some existing related security schemes. The proposed scheme’s performance analysis shows that its computational cost is 5.28 ms, total communication cost is 1264-bits, and they are least when compared to corresponding performance metrics of some related existing schemes (Khan, Ullah, Nisar, Noor, Qureshi, Khanzada, Khattak, et al., 2020).

Tan et al. have proposed an efficient Digital Signature algorithm based on ECC for on-demand routing protocol ad-hoc on demand vector (AODV), hence the overall algorithm is called Improved Security AODV (ISAODV). Simulations of the UAV communication network are performed in the NS2 simulator. Two types of performance comparisons are done while comparing ISAODV with SAODV and AODV: under normal conditions, and in the presence of malicious nodes. Under normal conditions, the Packet Delivery Ratio (PDR) and the Throughput of the three algorithms decrease when the speeds of the UAVs are increased. Under normal conditions, ISADOV and SAODV inherit characteristics of AODV. When malicious nodes are added (five are added) to the network, a common malicious node attack model is implemented in the simulation experiment. With the addition of malicious nodes, there is no significant change in PDR and throughput of the three algorithms. But ISADOV has got highest average PDR and throughput when compared to those of ISADOV and SAODV, even when the malicious nodes are added. Both under normal and malicious nodes addition conditions, the delay and routing overhead of three algorithms increase with an increase in the speeds of UAVs. Under normal and malicious nodes addition, the average delay of ISADOV is lesser than that of SADOV and more than that of AODV (X. Tan et al., 2020).

Liu et al. have proposed a public audit scheme for the support of dynamic data and privacy protection based on distributed string equality check protocol and Merkle Hash tree multi-level index structure for UAVs. The system model of the proposed scheme consists of three entities: UAVs (users), Cloud Service Provider (CSP), and Third-Party Server (TPS). The security model assumes CSP and TPS to be untrusted entities of the system model. During the setup phase, the users generate public-private key pairs and authorize themselves and TPS. Based on data granularity size and operation types, users can perform five operations during the dynamic data operation phase: data partition insertion, data partition deletion, data block insertion, modification of data block, and data block deletion. The proposed scheme’s security is analyzed in terms of data privacy, the inability of authorization forgeability, and audit reliability. The proposed scheme’s performance is analyzed in terms of computation cost, communication cost, and storage cost. In the proposed scheme, implementation of data integrity auditing is done using distributed string equality checking protocol, which improves
the security of the proposed scheme with low computational cost and communication cost, when compared to that of some related schemes (J. Liu et al., 2020).

Ge et al. have proposed a provenance aware distributed trust scheme resilient UAV networks, in which safe data transmission happens by the use of digital signature technology, and reduced resource consumption in presence of malicious nodes. The proposed scheme's network model consists of three entities: GCS, scouting UAVs, and ferrying UAVs. The thread model considers the following threats: fake identity, fake recommendation, modification attack, black hole attack, gray hole attack, and packet injection attack. Simulations are performed by considering an experimental area = 800 m*800 m, number of UAVs = 13, and simulation time = 450 s. Performance analysis shows that malicious nodes' detection rate increases as malicious nodes' attack intensity increases, and for the highest attack intensity the detection rate is 96%. The detection rate decreases as the malicious nodes' density increases. The detection rate is 80% when the density of the malicious nodes is 30%. In the majority of the cases, the proposed method outperforms the existing schemes in terms of detection rate, delivery rate, and system energy consumption (Ge et al., 2020).

Bae et al. have proposed a save-less key management and delegation system for operating a multi-drone control system, to make it highly resistant to physical capture attack. The system model consists of drones and GCSs which are connected by Wi-Fi. Security analysis shows that the proposed system exhibits different security features like forward and backward secrecy, resistance to physical capture attack, and key independence. Security analysis shows that the proposed system has got best security features when compared to other related schemes. The proposed system’s usability analysis shows that it has got properties like mobility support, delegation support, message broadcasting support, and multi-hop communication support. Usability analysis shows that the proposed system has the best usability properties when compared to three other related schemes. The proposed system's performance analysis shows that it has got least data sending traffic, least computational overhead, and least storage overhead when compared to other related schemes (Bae & Kim, 2019).

He et al. have proposed a Designated Verifier Proxy Blind Signature (DVPBS) for a UAV network architecture which is based on MEC. The proposed DVPBS is based on ECC. The UAV network architecture based on MEC consists of three layers: the Cloud Computing layer, Edge Computing layer, and the Device layer. The Cloud Computing layer is the original signer of the proposed DVPBS scheme. The edge computing layer consists of command stations that act as proxy signers of DVPBS. UAV is present in the device layer. The proposed scheme's analysis proves its correctness based on the requirements of a private key and public key for proxy signature. Security analysis shows that the proposed scheme’s signature verification cannot be done by a third party other than the signer and the verifier. Security analysis also shows that DVPBS can distinguish between the proxy signature generated by a proxy signer and that by the original signer. DVPBS also exhibits the property of signature blindness. Efficiency analysis of the proposed DVPBS scheme is done by comparing it with other related schemes by implementing the proposed and related schemes on a PC with Intel i5-4590 CPU and 4GB RAM. Efficiency analysis shows that the total time of execution of DVPBS is 150 ms which is more than that of just one related existing scheme, but lesser than that of 4 other related existing schemes. Efficiency analysis shows that DVPBS has got more signature length when compared to that of other related schemes, but still, that is less than the UAV transmission capacity (He et al., 2019).

Khan et al. have proposed a secure and efficient certificateless blind signature scheme based on the concepts of HECC, for FANET constituted by UAVs based on MEC. The proposed architecture has three layers: Layer 1, layer 2, and Layer 3. Informal security analysis shows that the proposed scheme has different security properties like Unforgeability, Integrity,
Unlinkability, resistance against replay attack. AVISPA tool is used for formal security verification of the proposed scheme, and also demonstrates the resistance of the proposed scheme to replay attack and MITM attack. The proposed scheme’s security analysis shows that it exhibits the best security properties when compared to other related schemes. The proposed scheme’s performance analysis shows that it has a total computation cost of 0.48 ms which is negligible compared to that of other related existing schemes. Performance analysis shows that the proposed scheme’s communication cost is 1616 ms which is the least when compared to that of other related existing schemes (Khan, Qureshi, et al., 2020).

Minu et al. have proposed a secure image transmission algorithm based on multiple share creation with optimal ECC, for UAV networks. The proposed algorithm is called SC-SSOECC. The following are the processes that are executed for SC-SSOECC: Input secret image development by the sender, division of the image into 12 shares (4 shares each for R, G, and B components), the arbitrary public key generated by the sender, private key generation based on Social Spider Optimization (SSO) by the desired receiver, encryption of 12 shares through public key at the sender and sending the 12 encrypted shares to the receiver, decryption of 12 encrypted shares through private key, reconstruction of 12 shares to form the actual input secret image at the receiver. Simulations are performed on a UAV benchmark dataset. Five images are considered for the experiment, and three performance metrics are considered: Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and Correlation Coefficient (CC). The average MSE, PSNR, and CC for SC-SSOECC are 0.13, 57.176, and 0.995, respectively. MSE is close to 0, CC being close to 1, and PSNR being so high represent a good performance for the proposed algorithm. The performance of the proposed algorithm is compared with three other related existing algorithms in terms of CC. The average CC of none of the three other related existing algorithms reaches as high as 0.995 (Minu & Aroul Canessone, 2021).

Lee et al. have proposed a security framework based on ROS for security improvement of UAS. The implementations of the proposed security framework are performed using the MAVROS environment. The security measures are implemented in master, publisher, and subscriber nodes which address two security issues related to UAVs and GCS: Unauthorized users’ nodes registration without permission, and false data injection by unauthorized nodes. Performance analysis shows that the proposed framework has got very low computational overhead when compared to existing related frameworks based on RSA, and ECDSA algorithms. Since the connection establishment, MAC provides data integrity and authentication of each transmission. HMAC digital signatures used in the proposed framework verifies the message abnormalities’ presence. Experiments of the proposed framework are performed using native ROS and non-native ROS environments. A UAV uses a Rasberry-pi companion computer and Pixhawk flight autopilot. The desired drone altitude of 2 m is considered for flight during the experiments. In a native ROS environment, without a security framework, the drone altitude fluctuates a lot with time, and after around 40 s, the altitude is less than 0.25 m. In the native ROS environment, with a security framework, the drone altitude fluctuates very less and the flight altitude is almost 2 m. Non-native ROS environment also shows similar results with security framework and without security framework as that for native ROS environment. The authors have planned to develop customized security modules for the proposed framework in the future (Lee et al., 2021).

Rashid et al. have proposed a secure communication model for UAV-assisted HetNet applications. The proposed model is based on an identity-based encryption scheme. The network of the proposed model consists of three main entities: user, base station, and UAV. The integration of the IBE scheme in the UAV-assisted HetNet provides two types of secure communication within the network: authentication between user and base station, and authentication between user and UAV. If there is an undesirable shutdown that occurs in
the network, then the users have to re-authenticate with the base station. In the second type of authentication, the UAV authenticates the users on its own, or with the help of a base station. The second type of authentication has lesser communication overhead. The proposed model's formal validation is done using the AVISPA tool. AVISPA tool proves the data confidentiality and authentication in the network. The proposed model also preserves valid information integrity in the network (Rashid et al., 2019).

Tao et al. have done two investigations for trustworthy data collection for UAVs that act as mobile sinks in federated WSN enabled IoT applications: introduction of the concept of great full coverage sub-graph, and a lightweight authority authentication model. The first step for the overall architecture is the determination of the candidate area for UAV deployment. The first investigation considers two main parameters: coverage radius for UAV service, and UAVs traffic balance. After the first investigation which focuses on UAV deployment, the second investigation is needed to provide security for open wireless mediums and unattended sensors in the networks. The deployed UAVs and sensors act as delegation decision-makers and delegation requestors. The session request for implementation of authority delegation for new data collection session request initiated by the sensor is signed using Forward Secure Revocable Group Signature (FSR-GS). The signature validation and session request evaluation by the target UAV is done based on policies provided by the control center. The second investigation considers three authentication scenarios for authentication of arrival data collection session requests. Simulations of the overall architecture are performed using MATLAB 2012a on 64-bit Windows 7 with 4GB RAM. The lightweight authority authentication method permits only legitimate sensors for the generation of valid group signatures. The second investigation makes the overall architecture resistant to attacks like MITM, repudiation attack, and impersonation attacks. The second investigation provides anonymity and untraceability of sensors. The second investigation also provides anonymity for the control center. The computation cost and communication cost of the architecture based on lightweight authority authentication are lesser than that of corresponding parameters of two other related existing schemes (Tao et al., 2020).

Agron et al. have proposed a secure routing protocol for secure communication between a GCS and UAV in a FANET. The network model of the proposed protocol consists of several UAVs which act as relays, and a GCS. A back-end C2 network operates the GCS. Key Distribution Center (KDC) present in the C2 network performs the management of credential network, and all the network nodes recognize the KDC’s public key. The nonce hash algorithm maintains the integrity of the connection and security of routing messages. Digital signatures with symmetric encryption algorithm provide security of exchanged packets fields like flight schedule, flight route of UAVs, geographical information provided by UAV, and link status message to be received by GCS. An asymmetric scheme provides a secure connection between GCS and other nodes in the network. TWINE lightweight encryption algorithm provides security of critical fields of routing messages. Packet leashes mechanism makes the network resistant to worm-hole attack. The simulations are performed in NS3. Performance analysis shows that even in presence of one hijacking attacker, the Packet Data Rate of the proposed protocol is maintained and is more than that of the AODV routing protocol. Performance analysis also shows that the proposed protocol has lesser network overhead when compared to that of the AODV routing protocol (Agron et al., 2019).

Cho et al. have proposed a random number generator specific to drones, called droneRNG. DroneRNG considers the sensor characteristics of drones in flight and stationary mode, like barometer signals, accelerometer signals, and gyroscope signals captured by drones. The experiments are performed using Raspberry pi drone and Pixhawk drone. DroneRNG initially collects data from drone sensors and performs four operations: dividing operation, shuffling operation, byte binding operation, mixing and swapping operation. Pixhawk drones do not have Linux Pseudo Random Number Generator (LPRNG). When the internal buffer falls
below 50% of capacity, generation of random numbers and filling of buffers takes place. When DroneRNG is implemented in Raspberry Pi drones, the entropy pool size is set to 4096-bits, and when the entropy falls below 2048-bits, random bits are collected from sensor data and random numbers are generated which fill the entropy pool. The randomness of DroneRNG is evaluated using the NIST test suite. The p-value of frequency tests of both Pixhawk drones and Raspberry Pi drones in both stationary and flight states for DroneRNG is equal to 1 (unlike that for existing random number generators where the corresponding values are less than 1), indicating higher randomness of DroneRNG. When 8-bits are passed as parameters for the three random number generators, it has been observed that DroneRNG requires a time of 0.171 ms, RAM of 1484KB. During this analysis, DroneRNG has more time and RAM requirements when compared to corresponding parameters of standard C Random function. But during the same analysis, DroneRNG has a lesser time requirement and more RAM requirement than that of corresponding parameters of LPRNG. Power consumption analysis shows that the Raspberry pi drone running both motors and DroneRNG has a power consumption of 1.27 W, and the same for Pixhawk drone is 157.19 W (S.-M. Cho et al., 2020).

Fournier et al. have proposed a secure routing protocol for a swarm of UAVs, which provides routing messages integrity and sender authentication with low energy consumption. The proposed protocol is called SEER4US. It is based on a proactive ad hoc routing protocol Optimized Link State Routing (OLSR) and authentication protocol Timed Efficient Stream Loss-tolerant Authentication (TESLA). The UAVs of a swarm share a piece of common knowledge.

Each node of the network exchanges Hello and Topology Control messages. “Hello” message contains neighbor nodes’ addresses, and Topology Control messages contain addresses of the nodes for Multi-Point Relay. A sender does not send a series of messages. Instead of a corresponding message, it sends three parts: the current data packet payload, the previous key that is used in the chain, and HMAC of the first two parts. On receiving each message, the desired receiver checks the integrity and authentication of the previous message. SEER4US addresses the latency issue introduced due to the waiting time for the next message to be received for authentication of the current one. The addition of a validation message which does not contain any routing information reduces verification time during the integrity and authentication check of a message. Security analysis exhibits the properties like valid signature unforgeability, hash value computation of a revealed key on a packet, discarding of a packet if a key used to sign it is disclosed within the packet lifetime. Performance analysis shows that SEER4US has an average overhead of 3.452Kbytes/s which is lesser than that of related existing protocols. Performance analysis also shows that SEER4US has a total power consumption of 6104 mW which is lesser than that of an existing related protocol and more than that of an existing related protocol (Fournier et al., 2019).

Benzarti et al. have proposed a security architecture for drones, based on Id-based sign-cryption and RFID tags. This architecture has been proposed to ensure authentication and preservation of privacy. Drone registration assignment is done using RFID tags, and temporal identity preserves privacy. The architecture deals with two types of compulsory identities for completion of the communication process of drone entity or inter drone: Physical unique identity for each drone; and generated identity which can change over a certain time duration due to expiration date, and loading errors. Simulations are performed with an assumption that initially, a given area has five drones with temporal identity each. The given area is divided into sub-zones for the definition of a drones' position at a given time. The simulations consider two scenarios: temporal identities’ average renewal with 10 nodes, and temporal identities’ average renewal with 100 nodes. Both the scenarios consider two conditions: with and without memory positions of nodes. For both conditions in the first scenario, the average renewal increases slowly with some nodes, but more rapidly without memory position. In the second scenario, there is a sharp average renewal growth without memory position and then steady for 90 nodes. In the second scenario, with memory position, the similar average renewal growth happens like that for without memory but being steady for 65 nodes.
Memorizing drone positions will increase the efficiency of temporal identities requests. When a drone revisits the previous position, a previous temporal identity will be assigned since there is no request for renewal of temporal identities. At some point, even with the increase in the number of drones, energy and time get saved. The architecture has not focused on secure ID communication among different entities and communication efficiency (Benzarti et al., 2018).

Kim et al. have proposed a remote erasure secure verifiable scheme with a countdown concept that uses random data synchronization for UAV. The proposed scheme consists of two main entities: GCS, and a UAV. Experiments are performed using the UAV flight computer T2080. Two experiments are performed: Communication overhead experiment, and Erasure operation overhead experiment. Communication overhead experiment measures the data transfer amount based on accumulated data rate generation and randomly selected data amount ratio in accumulated data region (alpha). For communication overhead experiments alpha value is set to 2, 10, 50, and 100. During a random data selection, the data transfer amount significantly increases, and the increased data amount depends on the increase in the value of alpha. Generated data amount also affects transferred data amount. Selection of sample of generated data during a sudden increase in generated data helps in stable communication with fewer data during unstable communications. The erasure operation overhead experiment measures the erasure latency based on UAV memory size. Erasure operation overhead experiment sets alpha and Beta (randomly selected data amount ratio in hot data region) values to 2. Erasure latency is evaluated for four different memory sizes of UAV: 1GB, 2GB, 4GB, and 16GB. Erasure latencies for the first three memory sizes of UAV are more than 400 s, and that for 16GB it is between 350 s and 400 s. In a particular situation, UAV puts its best effort into data erasure and erasure proof transfer (Kim et al., 2019).

Chen et al. have proposed a secure and lightweight IoD network coding pseudonym scheme. The network model consists of a set of cellular-connected drones, ground users, and ground base stations. The security model for real-time object tracking application (ROTA) with outsourced database (ODB) consists of cloud ODB, service engine, and a certifying server. The threat model of the proposed scheme considers three types of attackers: malicious observers, link eavesdroppers, and curious users. The system design of the proposed scheme has the proposed scheme integrated with International Mobile Subscriber Identity (IMSI), and encryption of IMSI is required to preserve privacy. The proposed scheme is called a two-tier coding scheme because the scheme generates two keys, i.e., key A and key B for legitimate users’ identity authentication and users’ private data protection, respectively. Experiments use Android smart phones with Qualcomm QSD8250. When hash functions are used for key generation, this reduces the possibility of solving of IMSI security problem by an adversary. Security analysis also shows that the proposed network coding scheme can achieve an unconditional security level. Security analysis shows that the location data ownership privacy is fully preserved and that the proposed scheme is collision-resistant to insider attacker, provides user authentication security feature, and service continuity feature. The proposed scheme provides unconditional security when compared to computational security provided by hash-based pseudonyms. The processing time of standard IMSI encryptions in IoD devices is reduced by more than 95% when network coding technique is used instead of hash functions. Energy consumption of key generation for the proposed scheme based on network coding with Galois Field (GF(2^8)) is about 10% of that with hash functions like Message Digest 5 (MD5) or Secure Hash Algorithm (SHA) (Chen & Wang, 2018).

Cherif et al. have proposed a secure and lightweight server-less protocol for enabling Mobile Data Collectors (MDCs) such as drones for collecting data from active mobile and static RFID nodes and then send the data to an authorized third party. Lightweight cryptography operations such as HMAC and hash functions are used. The data collection system model of the proposed protocol consists of three entities: Active RFID node, Mobile data collector, and base
Active RFID nodes consist of both active static and mobile RFID nodes. UAVs are used as MDCs. The base station consists of a KDC and a data sink. The proposed protocol's formal security analysis is done using the AVISPA tool and Proverif tool. AVISPA and Proverif show that the proposed protocol meets the desired security requirements. Informal security analysis shows that the proposed protocol exhibits different security properties like confidentiality, integrity and data freshness, perfect forward secrecy, mutual authentication, resistance to MITM attack, resistance to de-synchronization attack, and resistance to DoS attack. Performance analysis of the proposed protocol is done initially on Java smart cards to make sure that the proposed protocol can be implemented even for active RFID with more resources. Performance analysis shows that for big sensed data, memory overhead is low enough. Performance analysis also shows that the execution time of cryptography operations depends on the sensing process and that the active RFID nodes can switch to sleep mode at frequencies that are not high (Cherif et al., 2019).

Raja et al. have proposed a secured and efficient swarm-pattern UAV communication. The system model consists of a geographical area with a group of UAVs with a coverage area of about 200 km, a Base station (BS), and a controller. The proposed method uses the DY threat model for security analysis. Encryptions and Decryptions are done using two strong cryptography algorithms: AES and Blowfish. The proposed method's security analysis shows that it is more secure when compared to some previous related security methods. The proposed method is resistant to attacks like GPS spoofing. De-Authentication attack, Intercept data feed attack, Video Replay attack, and Impersonation attack. Performance analysis of AES and Blowfish for the proposed UAV model has been done using text, image, and video of sizes 11KB, 425KB, and 3055KB, respectively. Performance analysis has shown that the AES algorithm takes lesser encryption time, decryption time, and has lesser battery consumption (for performing authorization, communication, and computation) when compared to those of the Blowfish algorithm (Raja et al., 2021).

6.5. Lessons learned

This is an era in which people are surrounded by different IoT devices, among which IoD devices are a subset. IoD devices are also called flying IoT devices, and most of the time these devices are quite dynamic. Though IoD devices have contributed significantly to UAV applications and drone industries, this comes at the cost of vulnerabilities of the UAV data transmissions and storage. Moreover, since the IoD devices are resource-constrained, it is necessary to maintain or improve the efficiency of data storage, as well as data communication among these devices. So, different secure IoD frameworks and mechanisms based on Cryptography concepts have been divided into four subsections: 6.1, 6.2, 6.3, and 6.4. As it can be observed from the review in this section, the review has focused mainly on two main aspects: security of the IoD frameworks, and efficiency of the frameworks. Security of the IoD frameworks has been validated by using different standard security tools, by assuming some threat models of the designed IoD frameworks, and by performing formal and informal security analysis. In Informal security analysis, the resistance of the IoD frameworks against different security attacks has been shown. The efficiency of the frameworks has been analyzed most of the time by considering three main efficiency parameters of the frameworks: computation time, communication time, and storage time.

7. Attack or threat models for UAV communication, and Attacks on IoD

After designing a security mechanism/framework for an IoD network, some threat models should be explored that define the capabilities of an attacker. Hence, the subsection 7.1 explains two basic threat/attack models applicable to IoD networks. Moreover, while designing IoD networks, in addition to designing secure and efficient IoD networks, the designers should also have ample knowledge about possible Cryptography attacks corresponding to their network. Hence, this motivates us to learn about some Cryptography attacks which are
common in IoD networks. The subsection 7.2 speaks about some attacks which are common to IoD networks.

7.1. Attack or threat models for UAV communication
Dolev Yao threat model was proposed by D Dolev and A C Yao in the year 1983. The threat model studies families of cryptography protocols, which have certain characteristics, and characteristics of an adversary. It is assumed that the data is exchanged in an insecure channel. A perfect public key system has different properties like zero probability of breaking one-way functions, perfect security of public directory, everyone has access to ciphertext but only the sender knows the plaintext. An adversary has different characteristics like impersonating other entities of the network, is a legitimate user of the network, can extract any information passing through the network, inability to decrypt a ciphertext without the corresponding private key, and inability to derive a private key for a particular public key (Dolev & Yao, 1983).

The CK threat model was proposed by Ran Canetti and Hugo Krawczyk in the year 2002. The threat model has provided secure key exchange protocols’ notions and proved that these notions can be used for the construction of secure channels. The threat model has got each instance to handle a single pairwise session. This aspect has to take care of two issues: multi-session extensions, and a long-term authentication module. The threat model has explained concepts of universally composable key exchange and universally composable secure channels with their corresponding theorems (Canetti & Krawczyk, 2002).

7.2. Attacks on drones
A sinkhole attack is a type of attack in which, an adversary UAV tries to provide fake routes for network traffic and change the routing information. A black Hole Attack is a type of DoS attack in which an adversary UAV which acts as a fake relay which instead of forwarding the packets to the desired destination UAVs, discards the packets. Grey Hole attack is a type of DoS attack which is similar to a Black Hole Attack. But in this case, the adversary UAV which acts as a fake relay selectively forwards some network packets to the desired destination UAVs and discards the rest of the packets (Faraji-Biregani & Fotohi, 2021).

Drones are vulnerable to physical threats which act as obstacles in drone operations and missions. Different physical threats could be animals, humans, electric cables, trees, buildings, and environmental conditions like wind and temperature which can interfere in the path of UAVs and can cause UAV accidents. These types of threats can be avoided using collision avoidance techniques. Other examples of attacks on drones are spoofing, jamming, eavesdropping, hijacking, DoS attacks (Koubâa et al., 2019).

Security attacks on public safety networks that use drones can be classified into 2: passive attacks, and active attacks. Passive attacks which affect confidentiality are MITM attacks, traffic analysis, Trojans, malware, viruses, etc. Active attacks which affect integrity are modification of existing information, fabrication of new information, etc. Active attacks which affect authenticity are forgery of messages, UAV spoofing, GPS spoofing, etc. Active attacks which affect availability are routing attacks, channel jamming, DoS attack, etc. (D. He et al., 2017).

Mitchell et al. have explained three types of UAV attacker archetypes: reckless attackers, random attackers, and opportunistic attackers. Reckless attackers are those who perform attacks on UAVs whenever there are chances and they try to impair the UAV functionality as fast as possible. Random attackers randomly perform attacks to avoid detection. An opportunistic attacker decides the attack probability based on the sensed value of mis-monitoring probability which helps in environmental noise modeling. The more the mis-monitoring
probability, the higher is the attack probability by an opportunistic attacker (Mitchell & Chen, 2013).

False Data Injection Attack (FDIA) is an attack in which an attacker targets the uplink wireless data link from GCS to UAV. FDIA signals and FDIA codes have their corresponding powers. FDIA signals have the same pseudo-random spreading codes and carrier codes as the desired trajectory signals. When FDIA is launched, the UAV cannot receive the desired trajectory (Gu et al., 2021).

7.3. Lessons learned
Section 6 speaks about different security frameworks related to IoD networks. These frameworks are vulnerable to different types of security attacks. Moreover, it is also necessary to consider the vulnerability level of the frameworks, as well as to know certain capabilities of the attackers. Hence, subsection 7.1 speaks about two popular attack or threat models: DY, and CK threat models. The threat models consider different aspects like the security of the communicating channels, probability of breaking the keys, ciphertext knowledge to the public, etc. Subsection 7.2 discusses some common attacks that can be performed on IoD networks. Different types of physical as well as cyber threats have been discussed. Cyber threats include Trojans, Malwares, and Viruses too. These types of attacks can cause threats to any of the three security goals, or all the three security goals (Confidentiality, Integrity, and Availability). These attacks also cause threats to the Authentication security feature.

8. Security analysis tools, models and logics for UAV communication
Security validation of a designed secure IoD network has to be done by using some methods which use some security logic or models and use some tool for the validation part. Hence, this section gives brief explanations on security analysis tools, security analysis models, and security analysis logics that are used for analysis of IoD communication. This section explains six security analysis tools: Scyther, AVISPA, Proverif, Athena, NRL, and Hermes. Three security analysis models are explained in this section: Real or Random model, Ouafi and Phan model, and ROM. Three security analysis logics have been explained in this section: BAN, Mao Boyd, and GYN.

8.1. Security analysis tools
- Scyther: Scyther is a security analysis tool used for verification, falsification, and analysis of security protocols. The tool is based on a pattern refinement algorithm that provides concise and infinite representations of sets of traces. The tool provides a GUI for understanding and verifying a security protocol. The tool can simultaneously terminate and prove the correctness of a protocol for an unbounded number of sessions (Cremers, 2008).

- AVISPA: AVISPA tool is a push-button tool and stands for Automated Validation of Internet Security-sensitive Protocols and Sensitive Applications. It has got a web-based GUI that supports protocol specifications editing and allows the selection and configuration of different back ends of the tool by the user. It uses High-Level Protocol Specification Language for the implementation and specification of a security protocol. AVISPA integrates 4 basic back ends: Constraint-Logic-Based Attack Searcher, SAT-based Model-Checker, On-the-fly Model-Checker, and Tree Automata based on Automatic Approximations for the Analysis of Security Protocols (Armando et al., 2005).

- Proverif: Proverif tool considers these aspects as inputs: protocol model; extension of pi-calculus with cryptography; and security properties to be verified like authentication and secrecy. The tool automatically translates the input into the Horn clauses section and derivability queries section. The tool outputs whether a desirable security property is proved or whether there is a potential attack on the desirable property (Blanchet, 2013).
• Athena: Athena is a fully automatic and formal security analysis tool that uses arbitrary configurations to prove the correctness of security protocols. The tool reduces state space explosion problems by using several state space reduction techniques. Athena uses the different fundamental representations of protocol executions when compared to previous approaches. Athena uses the standard ML language of New Jersey for implementation which can be done on Windows and Linux. Athena consists of protocol description, and a set of security properties in an intuitive and simple input language as inputs (Song et al., 2001).

• NRL: NRL tool is based on the DY threat model. NRL tool specifies the protocols as a set of state machines transitions. The tool completely describes the preceding states for a corresponding specified state, following which the user can query each of the preceding states turns wise. NRL tool is capable of proving the security of a protocol against interleaving attacks (Meadows, 1994).

• Hermes: Hermes is a formal security analysis tool for secrecy properties verification of cryptography protocols. Hermes does not restrict the message size, the number of participants, and the number of sessions. Hermes models the cryptography protocols as a set of transitions with terms that are constructed by the application of encryption operator and pairing. In the Hermes tool, an intruder is modeled based on the DY threat model (Bozga et al., 2003).

8.2. Security analysis models and logics
Real or Random analysis model is used for password-based cryptography protocols. A protocol that is proven to be secure in the Real or Random model will be proven secure even in the Find-Then-Guess model, but not necessarily the other way round. Hence, Real or Random model is stronger than the Find-Then-Guess model. Real or Random models can use different oracle queries like Execute, Send, and Test (Abdalla et al., 2005).

Table 8 shows details of some security analysis models and logics used for analysis of IoD communication.

8.3. Lessons learned
This section explains about two types of methods that are used for security validations of IoD networks: Security analysis tools (explained in subsection 8.1), and Security analysis models or logics (explained in subsection 8.2). These methods consider different security goals and features into the picture. The method of regarding the Cryptography protocols varies from one security validation method to another (security analysis tool, model, or logic).

9. Challenges and future work
Based on the major reviews conducted in the sections 5 and 6, the subsections 9.1 and 9.2 have, respectively, shown some challenges in the review and future directions for the budding researchers.

9.1. Challenges
Based on the review done for proposed UAV application frameworks, and based on the security frameworks for IoD communications, the following challenges have been identified:

• AirSim simulator provides advantages in terms of different Physics engines. There are an ample number of papers on frameworks for UAV applications based on the AirSim simulator. However, the major challenge that has been identified from Section 5 is that AirSim does not take into account the throughput of the data communicated between 2 drones, as the distance between 2 drones increases/decreases (Zafar et al., 2021)[Shin et al., 2020][Koutras et al., 2020][Goh et al., 2021][Zuluaga et al., 2018][Lombard et al., 2020][Mazdin & Rinner, 2019][Vemprala & Saripalli, 2018].
• Resolutions of the images captured by drones may vary from application to application. Sometimes there might also be a need to capture high-resolution images for even those applications which might require low-resolution images. But based on the section 5, we can observe that at times AirSim simulations have generated only low-resolution images for the necessary datasets. (Shamwell et al., 2019)(J. Li et al., 2019)(Deng et al., 2020).

• GCS is used to analyze and process data received from ‘n’ number of UAVs in a network. But, based on Section 5, a major challenge that has been observed is that the AirSim simulator does not use a separate virtual GCS in any of the AirSim simulation environments (Ho et al., 2018)-(Bondi et al., 2018).

• When clusters of secure IoD framework/mechanism, the related frameworks fail to anticipate that even cluster head UAVs can also be attackers (Hong et al., 2020)(Y. Tan et al., 2020)(Abdallah et al., 2019).

• When a secure IoD framework is designed, a related framework does not consider the data security in GCS (Steinmann et al., 2016).

• Secure IoD frameworks have been designed to provide the best security features with the least compromise in the performance metrics. But based on a review done in Section 6, it has been observed that there is a framework that does not satisfy any of the 3 performance metrics i.e. computation cost, communication cost, and storage cost (Wazid, Das, et al., 2020).

• Several secure IoD frameworks have used digital signatures. One such framework has got a high signature generation time and high signature verification time, which is a major drawback (He et al., 2021).

9.2. Future work
Based on the challenges that have been identified for the review, the following future directions have been identified for the subsequent researchers:

• Future directions related to AirSim simulations: The AirSim simulator has an ample number of Physics engines and complete freedom for customization of the configuration file. Future researchers can try to introduce virtual GCS into simulations. Future researchers can introduce inter-drone communications by considering the obstacles between the communicating entities during the simulations, and analyze the throughput of the data communications by varying the distance between two drones, or that between a drone and a GCS. The above 2 future directions would be significant contributions to the AirSim simulations. Moreover, the researchers should also focus on generating images with high resolutions of the order n*m (n > 1500, m > 1500) for generating the required datasets, which would at least provide the IoD designers an idea about the efficiency of processing high-resolution images, if the simulations were converted into real-time.

• Future directions related to secure IoD frameworks: Researchers have tried their best to maintain the security of IoD networks. However, when IoD networks are designed, GCS will most probably come into the picture. So, researchers should also focus more on keeping the data stored in the GCS, as well as command signals from GCS to UAVs secure. Moreover, when clusters of drones are used in experiments, researchers can work more on designing proper attack detection and mitigation mechanisms that can even anticipate the cluster heads to be attackers. Researchers have contributed significantly to making IoD communications efficient in terms of computation time, communication time, and storage time. However, based on the review in Section 6, it has been observed that researchers can still improve the efficiency of IoD networks in terms of computation cost, communication
cost, and storage cost. Finally, researchers can design better digital signature algorithms, which could reduce both the signature generation time and signature verification time, eventually, reducing the authentication time of the communicating entities.

- **Future direction related to integration of AirSim simulator with secure IoD frameworks:** Once researchers manage to significantly incorporate the first set of future directions, the AirSim simulations would have improved in terms of availability of a sufficient number of communication entities, communication between the entities as that during real-time. Future researchers can then simulate UAV applications and tasks by considering Cryptography aspects during communication between a GCS and a UAV or between 2 UAVs.

## 10. Conclusion

UAVs have been used in various applications like construction site monitoring, agriculture, monitoring of irregular terrains like mountains, monitoring of areas affected by a natural disaster, medicine delivery, country border surveillance, etc. Drones capture different types of data in different file formats like text files, audio, video, etc., and transmit them to neighboring drones, or a GCS. UAVs might vary in their architectures. There are different types of UAVs, and their regulations can vary. Hence, considering these aspects, it is necessary to analyze the feasibility and efficiency of UAV tasks before the actual deployments to prevent UAV accidents, loss of UAV data, loss to life, loss to property, and unwanted deployment costs. Hence, a review has been done on papers that have shown their work on how the open-source UAV simulator AirSim has been used for the implementation of different types of UAV tasks. The AirSim implementation has used different simulation environments built on the Unreal Engine platform. IoD devices communicate a vast amount of data among each other. These communications are vulnerable to different types of attacks like MITM, replay, impersonation, etc. Hence, an extensive review has been conducted on different secure IoD frameworks which are implemented in real-time or by using network simulators like NS3, OMNeT++, etc. The IoD frameworks have used different cryptography concepts like digital signatures, key agreement, encryption and decryption, blockchain, etc. Analysis of the frameworks has been done both in terms of security features (authentication, forward secrecy, backward secrecy, etc.) and performance metrics (communication cost, computation cost, storage cost, signature generation time, signature verification time, etc.). The review paper has been concluded with challenges and future directions for the subsequent researchers.

### Author details

Snehal Samanth
E-mail: snehal.samanth@gmail.com
Prema K V
E-mail: prema.kv@manipal.edu
ORCID ID: http://orcid.org/0000-0002-8847-0749

Mamatha Balachandra
E-mail: mamtha.bc@manipal.edu
ORCID ID: http://orcid.org/0000-0003-2201-8730

1 Department of Computer Science and Engineering, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, India.

2 Department of Computer Science and Engineering, Manipal Institute of Technology Bengaluru, Manipal Academy of Higher Education, Manipal, India.

3 Department of Computer Science and Engineering, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, India.

### Disclosure statement

No potential conflict of interest was reported by the authors.

### Correction

This article has been republished with minor changes. These changes do not impact the academic content of the article.

### Citation information

Cite this article as: Security in Internet of Drones: A Comprehensive Review, Snehal Samanth, Prema K V & Mamatha Balachandra, Cogent Engineering (2022), 9: 2029080.

### References

Abdalla, M., Fouque, P.-A., & Pointcheval, D., “Password-based authenticated key exchange in the three-party setting,” in International Workshop on Public Key Cryptography. Berlin, Heidelberg. Springer, 2005, pp. 65-84.

Abdalrah, A., Ali, M. Z., Mišić, J., & Mlodić, V. B. (2019). Efficient security scheme for disaster surveillance uav communication networks. Information, 10(2), 43. https://doi.org/10.3390/info10020043

Abdel-Malek, M. A., Akkaya, K., Saputo, N., & Ibrahim, A. S., “Efficient authentication of drones to mmwave wireless mesh networks in post-disaster scenarios,” in GLOBECOM 2020-2020 IEEE Global Communications Conference. Taipei, Taiwan. IEEE, 2020, pp. 1-6.

Aggarwal, S., Shojafar, M., Kumar, N., & Conti, M., “A new secure data dissemination model in internet of drones,” in ICC 2019-2019 IEEE International Conference on Communications (ICC). Shanghai, China. IEEE, 2019, pp. 1-6.

Agron, D. J. S., Ramli, M. R., Lee, J.-M., & Kim, D.-S., “Secure ground control station-based routing protocol for uav networks,” in 2019 International Conference on...
Information and Communication Technology Convergence (ICTC). Jeju, Korea (South). IEEE, 2019, pp. 794–798.

Ahn, O., Kim, J., & Lim, C., “Smart uav research program status update: Achievement of tilt-rotor technology development and vision ahead,” in 27th Congress of International Council of the Aeronautical Sciences, ICAS. KARI (Korea Aerospace Research Institute), South Korea, vol. 6, p. 2010.

Akram, R. N., Mankonakakis, K., Mayes, K., Habachi, O., Sauvener, D., Steven, A., & Choumette, S., “Security, privacy and safety evaluation of dynamic and static fleets of drones,” in 2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC). St. Petersburg, FL, USA. IEEE, 2017, pp. 1–12.

Albolawi, M., & Song, H., “Data security and privacy issues in swarms of drones,” in 2019 Integrated Communications, Navigation and Surveillance Conference (ICNS). Herndon, VA, USA. IEEE, 2019, pp. 1–11.

Ali, Z., Chaudhry, S. A., Ramzan, M. S., & Al-Turjman, F. (2020). Securing smart city surveillance: A lightweight authentication mechanism for unmanned vehicles. IEEE Access, 8, 43711–43724. https://doi.org/10.1109/ACCESS.2020.3001498

Alladi, T., Chamola, V., Naren, and Kumar, N. et al. (2020). Parth: A two-stage lightweight mutual authentication protocol for uav surveillance networks. Computer Communications, 160, 81–90. https://doi.org/10.1016/j.comcom.2020.05.025

Alladi, T., Naren, N., Bonsol, G., Chamola, V., & Guziani, M. (2020). Secuuthue: A novel authentication scheme for uav-base station scenario. IEEE Transactions on Vehicular Technology, 69(12), 15068–15077. https://doi.org/10.1109/TVT.2020.3030560

Allouch, A., Chekhrouhou, O., Koubba, A., Khalgui, M., & Abbès, T., “Movsec: Securing the movlink protocol for ardupal/tlxpx unmanned aerial systems,” in 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC). Tangier, Morocco. IEEE, 2019, pp. 621–628.

Almalki, F. A., Soufiene, B. O., Alsamhi, S. H., & Sakli, H. (2021). A low-cost platform for environmental smart farming monitoring system based on low uavs. Sustainability, 13(11), 5908. https://doi.org/10.3390/su13115908

Alsamhi, S. H., Afgah, F., Sahal, R., Hawbani, A., Alqaness, A., Lee, B., & Guziani, M. (2021). Green internet of things using uavs in 5g networks: A review of applications and strategies. Ad Hoc Networks, 117, 102505. https://doi.org/10.1016/j.adhoc.2021.102505

Alsamhi, S. H., Almalki, F., Ma, O., Ansari, M. S., & Lee, B. (2021). Predictive estimation of optimal signal strength from drones over ion frameworks in smart cities. IEEE Transactions on Mobile Computing, 1–1, 101002/etl/4255. https://doi.org/10.1109/TMC.2021.3074442

Alsamhi, S. H., Lee, B., Guziani, M., Kumar, N., Qiao, Y., & Liu, X. (2021). Blockchain for decentralized multi-drone to combat covid-19 and future pandemics: Framework and proposed solutions. Transactions on Emerging Telecommunications Technologies. 32, e4255.

Alsamhi, S. H., Ma, O., Ansari, M. S., & Almalki, F. A. (2019). Survey on collaborative smart drones and internet of things for improving smartness of smart cities. IEEE Access, 7, 128125–128152. https://doi.org/10.1109/ACCESS.2019.2934998

Alsamhi, S. H., Ma, O., Ansari, M. S., & Gupta, S. K. (2019). Collaboration of drone and internet of public safety things in smart cities: An overview of qos and network performance optimization. Drones, 3(1), 13. https://doi.org/10.3390/drones3010013

Altawy, R., & Youssef, A. M. (2016). Security, privacy, and safety aspects of civilian drones: A survey. ACM Transactions on Cyber-Physical Systems, 1(2), 1–25. https://doi.org/10.1145/3001836

Arce, S., Vernon, C. A., Hammond, J., Newell, V., Janson, J., Franke, K. W., & Hedengren, J. D. (2020). Automated 3d reconstruction using optimized view-planning algorithms for iterative development of structure-from-motion models. Remote Sensing, 13(12), 2169. https://doi.org/10.3390/rs13122169

Armando, A., Basín, D., Boichut, Y., Chevalier, Y., Compagna, L., Cuellar, J., Drielsma, P. H., Héam, P.-C., Kouchanrenko, O., Montavon, J., Mødersheim, S., and Von Oheimb, D. et al., “The avisa tool for the automated validation of internet security protocols and applications,” in In International Conference on computer aided verification. Berlin, Heidelberg. Springer, 2005, pp. 281–285.

Armour, C., & Ross, J. (2017). The health and well-being of military drone operators and intelligence analysts: A systematic review. Military Psychology, 29(2), 183–193. https://doi.org/10.1037/mil0000149

Ataei, S., Kwon, O.-J., Kim, C.-Y., Lee, S.-H., Choi, Y.-R., & Kwon, K.-R., “The secure uav communication link based on otp encryption technique,” in 2019 Eleventh International Conference on Ubiquitous and Future Networks (ICUFN). Zagreb, Croatia. IEEE, 2019, pp. 1–3.

Boe, M., & Kim, H. (2019). Authentication and delegation for operating a multi-drone system. Sensors, 19(9), 2066. https://doi.org/10.3390/s19092066

Boidyo, S., Shaikh, Z., & Levorato, M., “Flynetsim: An open source synchronized uav network simulator based on ns-3 and ardulpax,” in Proceedings of the 21st ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems. UC Irvine, CA, United States, 2018, pp. 37–45.

Bolldini, F., Anandikumar, A., & Murray, R. M., “Learning pose estimation for uav autonomous navigation and landing using visual-inertial sensor data,” in 2020 American Control Conference (ACC) Denver, CO, USA. IEEE, 2020, pp. 2961–2966.

Bauk, S., “Performances of some autonomous assets in maritime missions,” 2020.

Bellare, M., & Rogaway, P., “Random oracles are practical: A paradigm for designing efficient protocols,” in Proceedings of the 1st ACM Conference on Computer and Communications Security Watson Research Cent, United States, 1993, pp. 62–73.

Benzarti, S., Triki, B., & Korbao, O. (2018). Privacy preservation and drone authentication using id-based signcryption. In SoMet (IOS Press) (pp. 226–239).

Bera, B., Chattaraj, D., & Das, A. K. (2020). Designing secure blockchain-based access control scheme in iot-enabled network of drones. Computer Communications, 153, 229–249. https://doi.org/10.1016/j.comcom.2020.02.011

Bera, B., Das, A. K., Garg, S., Piran, M. J., & Hossain, M. S. (2021). Access control protocol for battlefield surveillance in drone-assisted iot environment. IEEE Internet of Things Journal 9, 1. https://doi.org/10.1109/JIOT.2020.3049003

Bera, B., Das, A. K., & Sutrula, A. K. (2020). Private blockchain based access control mechanism for unauthorized uav detection and mitigation in network of drones environment. Computer Communications, 166, 91–109. https://doi.org/10.1016/j.comcom.2020.12.005
Bera, B., Saha, S., Das, A. K., Kumar, N., Lorenz, P., & Alazab, M. (2020). Blockchain-envisioned secure data delivery and collection scheme for 5G-based IoT-enabled internet of drones environment. *IEEE Transactions on Vehicular Technology*, 69(8), 9097–9111. https://doi.org/10.1109/TVT.2020.3000576

Blanchet, B. (2013). Automatic verification of security protocols in the symbolic model: The verifier proverif. In *Foundations of security analysis and design VII* (pp. 54–87). Springer.

Boccadoro, P., Striccoli, D., & Grieco, L. A. (2021). An extensive survey on the internet of drones. *Ad Hoc Networks*, 122, 102600. https://doi.org/10.1016/j.adhoc.2021.102600

Bondi, E., Dey, D., Kapoor, A., Plavis, J., Shah, S., Fang, F., Dilkina, B., Hannaford, B., Iyer, A., Joppa, L., and Tambe, M. et al., “Airim-w: A simulation environment for wildlife conservation with uavs,” in *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies Menlo Park and San Jose*, 2016, pp. 1–12.

Bondi, E., Jain, R., Agrawal, P., Anond, S., Hannaford, R., Kapoor, A., Plavis, J., Shah, S., Joppa, L., Dilkina, B., and Tambe, M. et al., “Birdsio: A dataset for detection and tracking in aerial thermal infrared videos,” in *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision Snowmass, CO, USA*, 2020, pp. 1747–1756.

Borisy, K., Lubushkina, I., & Panasenko, S., “Adaptation of an authentication protocol based on asymmetric keys for use in uav c2 link security systems,” in *Proceedings of the 12th International Conference on Security of Information and Networks ANCU, Moscow, Russian Federation*, 2019, pp. 1–4.

Bouffard, H., Kamoun, F., & Iqbal, F. (2020). Towards a better understanding of drone forensics: A case study of parrot drone 2.0. *International Journal of Digital Crime and Forensics (IJDCF)*, 12(1), 35–57. https://doi.org/10.4018/IJDCF.202010101

Boyd, C., & Mao, W., “On a limitation of ban logic,” in *Workshop on the Theory and Application of Cryptographic Techniques Berlin, Heidelberg*, Springer, 1993, pp. 240–247.

Bozga, L., Lokheche, Y., & Périn, M., “Hermes: An automatic tool for verification of secrecy in security protocols,” in *International Conference on Computer Aided Verification Berlin, Heidelberg*, Springer, 2003, pp. 219–222.

Burrows, M., Abadi, M., & Needham, R. M., “A logic of authentication,” *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences Univ of Cambridge Computer Lab, United Kingdom*, vol. 416, pp. 233–271, 1989.

Canetti, R., & Krawczyk, H., “Universally composable notions of key exchange and secure channels,” in *International Conference on the Theory and Applications of Cryptographic Techniques Amsterdam*, Springer, 2002, pp. 337–351.

Chaudhry, S. A., Yahya, K., Karuppusamy, M., Kharel, R., Bashir, A. K., & Zikria, Y. B. (2021). Grocs-iod: A certificate based generic access control scheme for internet of drones. *Computer Networks*, 191, 107999. https://doi.org/10.1016/j.comnet.2021.107999

Chen, C.-L., Deng, Y.-Y., Weng, W., Chen, C.-H., Chiu, Y.-J., & Wu, C.-M. (2020). A traceable and privacy-preserving authentication for uav communication control system. *Electronics*, 9(11), 62. https://doi.org/10.3390/electronics9110062

Chen, L., Qian, S., Lim, M., & Wang, S. (2018). An enhanced direct anonymous attestation scheme with mutual authentication for network-connected uav communication systems. *China Communications*, 15(5), 61–76. https://doi.org/10.1109/CC.2018.8387987

Chen, Y.-J., & Wang, L.-C. (2018). Privacy protection for internet of drones: A network coding approach. *IEEE Internet of Things Journal*, 6(2), 1719–1730. https://doi.org/10.1109/JIOT.2018.2875065

Cheon, S.-H., Ho, S.-W., & Moon, Y.-H., “Hardware-in-the-loop simulation platform for image-based object tracking method using small uav,” in *2016 IEEE/IAAA 35th Digital Avionics Systems Conference (DASC)* Sacramento, CA, USA, IEEE, 2016, pp. 1–5.

Cheon, J. H., Han, K., Hong, S.-M., Kim, H. J., Kim, J., Kim, S., Seo, H., Shim, H., & Song, Y. (2018). Toward a secure drone system: Flying with real-time homomorphic authenticated encryption. *IEEE Access*, 6, 24325–24339. https://doi.org/10.1109/ACCESS.2018.2819189

Cherif, A., Belkadi, M., & Sauveron, D. (2019). A lightweight and secure data collection serverless protocol demonstrated in an active rfid scenario. *ACM Transactions on Embedded Computing Systems (TECS)*, 18(3), 1–27. https://doi.org/10.1145/3274667

Cho, G., Kim, J., Hyun, S., & Kim, H. (2020). Sentinel: A secure and efficient authentication framework for unmanned aerial vehicles. *Applied Sciences*, 10(9), 3149. https://doi.org/10.3390/app10093149

Cho, S.-M., Hong, E., & Seo, S.-H. (2020). Random number generator using sensors for drone. *IEEE Access*, 8, 30343–30354. https://doi.org/10.1109/ACCESS.2020.2927958

Choi, H., Geeves, M., Alsalam, B., & Gonzalez, F., “Open source computer-vision based guidance system for uavs on-board decision making,” in *2016 IEEE aerospace conference Big Sky, MT, USA*. IEEE, 2016, pp. 1–5.

Cremers, C. J., “The scytter tool: Verification, falsification, and analysis of security protocols,” in *International conference on computer aided verification ETH Zurich, Zurich 8092, Switzerland*. Springer, 2008, pp. 414–418.

Deebak, B., & Al-Turjman, F. (2020). A smart lightweight privacy preservation scheme for iot-based uav communication systems. *Computer Communications*, 162, 102–117. https://doi.org/10.1016/j.comcom.2020.08.016

Deng, H., Arif, U., Yang, K., Xi, Z., Quan, Q., & Cai, K.-Y. (2020). Global optical flow-based estimation of velocity for multicopters using monocular vision in gps-denied environments. *Optik*, 219, 164923. https://doi.org/10.1016/j.ijleo.2020.164923

Dobrea, D.-M., & Dobrea, M.-C. (2020). An autonomous uav system for video monitoring of the quarantine zones. *Roman Journal of Information Science and Technology*, 23, 553.

Dolev, D., & Yao, A. (1983). On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2), 198–208. https://doi.org/10.1109/TIT.1983.1056650

Dong, J., Wu, G., Yang, T., & Li, Y. (2018). The improved image scrambling algorithm for the wireless image transmission systems of uavs. Sensors, 18(10), 3430. https://doi.org/10.3390/s18103430

Ebeid, E., Skrivar, M., Terkildsen, K. H., Jensen, K., & Schultz, U. P. (2018). A survey of open-source uav flight controllers and flight simulators. *Microprocessors and Microsystems*, 61, 11–20. https://doi.org/10.1016/j.micpro.2018.05.002

Estrada, M. A. R., & Ndome, A. (2019). The uses of unmanned aerial vehicles-uav’s-(or drones) in social logistic: Natural disasters response and humanitarian
relief aid. *Procedia Computer Science*, 149, 375–383. https://doi.org/10.1016/j.procs.2019.01.151

Ever, Y. K. (2020). A secure authentication scheme framework for mobile-sinks used in the internet of drones applications. *Computer Communications*, 155, 143–149. https://doi.org/10.1016/j.comcom.2020.03.009

Fan, J., Qiao, L., Cao, Y., Liu, S., Zhang, W., & Tang, L. (2021). A new password-and position-based authenticated key exchange. *Security and Communication Networks*, 2021, 1–9. https://doi.org/10.1155/2021/6613392

Foraji-Biregani, M., & Fotofi, R. (2021). Secure communication between uavs using a method based on smart agents in unmanned aerial vehicles. *The Journal of Supercomputing*, 77(5), 5076–5103. https://doi.org/10.1007/s11227-020-03462-0

Fernando, M., Jayalath, D., Comtepe, S., & Foo, E., “Reed solomon codes for the reconciliation of wireless phy layer based secret keys,” in *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)* Toronto, ON, Canada. IEEE, 2017, pp. 1–6.

Ferrag, M. A., & Mogaras, L. (2019). Deliverycoy: An ids and blockchain-based delivery framework for drone-delivered services. *Computers, 8*(3), 58. https://doi.org/10.3390/computers8030058

Fotouhi, A., Qiang, H., Ding, M., Hassan, M., Giordano, L. G., Garcia-Rodriguez, A., & Yuan, J. (2019). Survey on uav cellular communications: Practical aspects, standardization advancements, regulation, and security challenges. *IEEE Communications Surveys & Tutorials*, 21(6), 3417–3462. https://doi.org/10.1109/COMST.2019.2906228

Fournier, B., Guette, G., Tong, V. T. T., & Lanet, J.-L., “Seerkus, secured energy efficient routing for uav swarms,” in 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) Barcelona, Spain. IEEE, 2019, pp. 1–6.

Fuller, B., Kok, J., Nelson, N., & Gonzalez, F., “Hardware design and implementation of a movilink interface for an fpga-based autonomous uav flight control system,” in *Proceedings of the 16th Australasian Conference on Robotics and Automation 2014* Queensland University of Technology, Australia. Australian Robotics and Automation Association Inc., 2014, pp. 1–6.

Garcia, R., & Barnes, L., “Multi-uav simulator utilizing x-plane,” in *Selected papers from the 2nd International Symposium on UAVs*, Reno, Nevada, USA June 8–10 Aberdeen Proving Ground, United States, 2009. Springer, 2009, pp. 393–406.

Ge, C., Zhou, L., Hancke, G. P., & Su, C. (2020). A provenance-aware distributed trust model for resilient unmanned aerial vehicle networks. *IEEE Internet of Things Journal* 8(6):2327462 301109/.

Genc, H., Zu, Y., Chiu, T.-W., Holpern, M., & Reddi, V. J. (2017). Flying iot: Toward low-power vision in the sky. *IEEE Micro*, 37(6), 40–51. https://doi.org/10.1109/MM.2017.4241339

Gharibi, M., Bouthaib, R., & Waslander, S. L. (2016). Internet of drones. *IEEE Access*, 4, 1146–1162. https://doi.org/10.1109/ACCESS.2016.2537208

Ghiribi, E., Khoei, T. T., Gorji, H. T., Ranganathan, P., & Kaebouch, N., “A secure blockchain-based communication approach for uav networks,” in *2020 IEEE International Conference on Electro Information Technology (EIT)* Chicago, IL, USA. IEEE, 2020, pp. 411–415.

Goh, K. C., Ng, R. B., Wong, Y.-K., Ho, N. J., & Chua, M. C. (2021). Aerial filming with synchronized drones using reinforcement learning. *Multimedia Tools and Applications*, 12, 1–26. https://doi.org/10.1109/s11462-020-10388-5.

Gong, L., Needham, R. M., & Yahalom, R., “Reasoning about belief in cryptographic protocols,” in *IEEE Symposium on Security and Privacy Comput Lab*, Univ of Cambridge, UK. Citeseer, 1990, pp. 234–248.

Gope, P., Millwood, O., & Saxena, N. (2021). A provably secure authentication scheme for rfid-enabled uav applications. *Computer Communications*, 166, 19–25. https://doi.org/10.1016/j.comcom.2020.11.009

Gope, P., & Sikdar, B. (2020). An efficient privacy-preserving authenticated key agreement scheme for edge-assisted internet of drones. *IEEE Transactions on Vehicular Technology*, 69(11), 13621–13630. https://doi.org/10.1109/TVT.2020.3018778

Griece, G., Artuso, R., Boccadura, P., Piro, G., & Grieco, L. A., “An open source and system-level simulator for the internet of drones,” in *2019 IEEE 30th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC Workshops)* Istanbul. IEEE, 2019, pp. 1–6.

Gu, Y., Yu, X., Guo, K., Qiao, J., & Gao, L. (2021). Detection, estimating, and compensation of false data injection attack for uavs. *Information Sciences*, 546, 723–741. https://doi.org/10.1016/j.ins.2020.08.055

Gynnid, A. (2016). The robot eye witness: Extending visual journalism through drone surveillance. *Digital Journalism*, 2(3), 334–343. https://doi.org/10.1080/21670811.2016.1481364

Haque, M. S., & Chowdhury, M. U., “A new cyber security framework towards secure data communication for unmanned aerial vehicle (uav),” in *International Conference on Security and Privacy in Communication Systems Deakin University- Burwood Campus*, Melbourne, Australia. Springer, 2017, pp. 113–122.

Hayajneh, A. M., Zaidi, S. A. R., McIernon, D. C., & Ghogho, M., “Optimal dimensioning and performance analysis of drone-based wireless communications,” in *2016 IEEE Globecom Workshops (GC Wkshps)* Washington. IEEE, 2016, pp. 1–6.

He, D., Chan, S., & Guizani, M. (2017). Drone-assisted public safety networks: The security aspect. *IEEE Communications Magazine*, 55(8), 218–223. https://doi.org/10.1109/MCOM.2017.1600799CM

He, L., Mo, J., Mo, R., & Wei, D. (2019). Designated verifier proxy blind signature scheme for unmanned aerial vehicles (dubss) in *Proc. of Mobile edge computing*. Security and Communication Networks, 2019, 1–12. https://doi.org/10.1155/2019/8583130

He, L., Mo, J., Shen, L., & Wei, D. (2021). Certificateless designated verifier proxy signature scheme for unmanned aerial vehicle networks. *Science China Information Sciences*, 64(1), 1–15. https://doi.org/10.1007/s11432-019-2903-2

Hentati, A. I., Kirchen, L., Fourati, M., & Fourati, L. C., “Simulation tools, environments and frameworks for uav systems performance analysis,” in *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)* Limassol. IEEE, 2018, pp. 1495–1500.

Ho, C. Y., Tseng, S. Y., Lai, C. F., Wang, M. S., & Chen, C. J., “A parameter sharing method for reinforcement learning model between airsim and uavs,” in *2018 1st International Cognitive Cities Conference (IC3)* Okinawa. IEEE, 2018, pp. 20–23.

Hofmajeed, N., & Rizos, C. (2015). Application of multiple categories of unmanned aircraft systems (uas) in different airspaces for bushfire monitoring and response. *International Archives of the Photogrammetry, Remote Sensing & Spatial
Information Sciences, 40 55–60 doi:10.5194/isprsarchives-XL-1-W4-55-2015.

Hong, W., Jianhua, L., Chenghe, L., & Zhe, W. (2020). A provably secure aggregate authentication scheme for unmanned aerial vehicle cluster networks. Peer-to-Peer Networking and Applications, 13(1), 53–63. https://doi.org/10.1007/s12083-019-0718-9

Hsieh, Y.-Y., Lin, W.-Y., Li, D.-L., & Chung, J.-H., “Deep learning-based obstacle detection and depth estimation,” in 2019 IEEE International Conference on Image Processing (ICIP) Taipei, IEEE, 2019, pp. 1635–1639.

Hussain, S., Chaudhry, S. A., Alomari, O. A., Alsharif, M. H., Khan, M. K., & Kumar, N. (2021). Amassing the security: An ecc-based authentication scheme for internet of drones. IEEE Systems Journal, 15(3), 4431–4438. https://doi.org/10.1109/JSYST.2021.3057047

Hussein, M. N., Megahed, M. H., & Azeem, M. H. A., “Design and simulation of authenticated encryption aenot stream cipher algorithm,” in 2017 13th International Computer Engineering Conference (ICENC) Giza, IEEE, 2017, pp. 393–398.

Islam, A., Sadia, K., Masuduzzaman, M., & Shin, S. Y., “Bumar: A blockchain-empowered uav-assisted smart surveillance architecture for marine areas,” in Proceedings of the International Conference on Computing Advancements Dhaka, 2020, pp. 1–5.

Jan, S. U., Qayum, F., & Khan, H. U. (2021). Design and analysis of lightweight authentication protocol for securing iot. IEEE Access 69287–69306 doi:10.1109/ACCESS.2021.3076692.

Keith, J., & Hall, D., “Rapid sizing methodologies for vtol uavs,” in 47th AIAA Aerospace Sciences Meeting including The New Horizons Forum and Aerospace Exposition United States, 2009, p. 1617.

Khan, M. A., Qureshi, I. M., Ullah, I., Khan, S., Khanzada, F., & Noor, F. (2020). An efficient and provably secure certificateless blind signature scheme for flying ad-hoc network based on multi-access edge computing. Electronics, 9(1), 30. https://doi.org/10.3390/electronics9010030

Khan, M. A., Ullah, I., Kumar, N., Oubbati, O. S., Qureshi, I., Noor, F., & Ullah, F. (2021). An efficient and secure certificate-based access control and key agreement scheme for flying ad hoc networks. IEEE Transactions on Vehicular Technology, 70(5), 4839–4851. https://doi.org/10.1109/TVT.2021.3055895

Khan, M. A., Ullah, I., Nisar, S., Noor, F., Qureshi, I. M., Khanzada, F. U., & Amin, N. U. (2020). An efficient and provably secure certificateless key-encapsulated signature scheme for flying ad-hoc network. IEEE Access, 8, 36807–36828. https://doi.org/10.1109/ACCESS.2020.2974381

Khan, M. A., Ullah, I., Nisar, S., Noor, F., Qureshi, I. M., Khanzada, F., Khattak, H., & Aziz, M. A. (2020). Multiaccess edge computing empowered flying ad hoc networks with secure deployment using identity-based generalized signature. Mobile Information Systems, 2020, 1–15. https://doi.org/10.1155/2020/8861947

Khán, T. D., Komarov, I., Don, L.D., Iurev, R., and Chuprov, S. et al., “Tra: Effective authentication mechanism for swarms of unmanned aerial vehicles,” in 2020 IEEE Symposium Series on Computational Intelligence (SSCI) Canberra. IEEE, 2020, pp. 1852–1858.

Kim, K., & Kang, Y., “Droone security module for uav data encryption,” in 2020 International Conference on Information and Communication Technology Convergence (ICTC) Jeju Island. IEEE, 2020, pp. 1672–1674.

Kim, S., Yoon, T.-Y., Choi, D., & Park, K.-W. (2019). Uav-undertaker: Securely verifiable remote erasure scheme with an eavesdropping-concept for uav via randomized data synchronization. Wireless Communications and Mobile Computing, 2019, 1–11. https://doi.org/10.1155/2019/8913910

Ko, Y., Kim, J., Dugumna, D. G., Astill, P. V., You, I., & Pau, G. (2021). Drone secure communication protocol for future sensitive applications in military zone. Sensors, 21(6), 2057. https://doi.org/10.3390/s21062057

Koubâa, A., Qureshi, B., Sriti, M.-F., Allouach, A., Javed, Y., Alaljani, M., Cheikhrouhou, O., Khalgui, M., & Tovar, E. (2019). Dronemap planner: A service-oriented cloud-based management system for the internet-of-drones. Ad Hoc Networks, 86, 46–62. https://doi.org/10.1016/j.adhoc.2018.09.013

Koutras, D. I., Karpouzis, A. C., & Kosmatopoulos, E. B. (2020). Autonomous and cooperative design of the monitor teams for a uav to maximize the quantity and quality of detected objects. IEEE Robotics and Automation Letters, 5(3), 4986–4993. https://doi.org/10.1109/LRA.2020.3004238

Krishna, C. L., & Murphy, R. R., “A review on cybersecurity vulnerabilities for unmanned aerial vehicles,” in 2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR) Shanghai. IEEE, 2017, pp. 194–199.

Lee, H., Yoon, I., Jang, M.-S., & Park, K.-J. (2021). A robot operating system framework for secure uav communications. Sensors (Switzerland), 21(4), 1–20 doi:10.3390/s21041369.

Lei, Y., Zeng, L., Li, Y.-X., Wang, M.-X., & Qin, H. (2021). A lightweight authentication protocol for uav networks based on security and computational resource optimization. IEEE Access, 9, 53769–53785. https://doi.org/10.1109/ACCESS.2021.3070683

Li, J., Chen, S., Zhang, F., Li, E., Yang, T., & Lu, Z. (2019). An adaptive framework for multi-vehicle ground speed estimation in airborne videos. Remote Sensing, 11(10), 1241. https://doi.org/10.3390/rs11101241

Li, Y., Du, X., & Zhou, S., “A lightweight identity authentication scheme for uav and road base stations,” in Proceedings of the 2020 International Conference on Cyberspace Innovation of Advanced Technologies Guangzhou China (ACM), 2020, pp. 54–58.

Li, T., Ma, J., Ma, G., Cao, C., Wang, H., Mo, C., Yu, J., Lu, D., & Zhang, J., “Lightweight secure communication mechanism towards uav networks,” in 2019 IEEE Globecom Workshops (GC WKSHPS) Waikoloa. IEEE, 2019, pp. 1–6.

Lindgren, K., Leung, S., Nothwang, W. D., & Shamwell, E. J., “Boom-via: Bootstrapped monocular visual-inertial odometry with absolute trajectory estimation through unsupervised deep learning,” in 2019 19th International Conference on Advanced Robotics (ICAR) Belo Horizonte. IEEE, 2019, pp. 516–522.

Liu, Q., Qian, H., & Hu, F., “Random label based security authentication mechanism for large-scale uav swarm,” in 2019 IEEE Int’l Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDClou&SocialCom/SustainCom) Xiamen. IEEE, 2019, pp. 229–235.

Liu, Y.-C., Tian, J., Mo, C.-Y., Glaser, N., Kuo, C.-W., & Kira, Z., “Who2com: Collaborative perception via learnable handshake communication,” in 2020 IEEE International Conference on Robotics and Automation (ICRA) Paris. IEEE, 2020, pp. 6876–6883.
Liu, J., Wang, X. A., Liu, Z., Wang, H., & Yang, X. (2020). Privacy-preserving public cloud audit scheme supporting dynamic data for unmanned aerial vehicles. *IEEE Access*, 8, 79428–79439. https://doi.org/10.1109/ACCESS.2020.2991033

Lombard, A., Durand, L., & Golland, S., “Velocity obstacle based strategy for multi-agent collision avoidance of unmanned aerial vehicles,” in *2020 IEEE International Conference on Sensing, Communication and Networking (SECON Workshops)* Como, Italy. IEEE, 2020, pp. 1–6.

Lugo, J. J., & Zell, A. (2014). Framework for autonomous on-board navigation with the ar. drone. *Journal of Intelligent & Robotic Systems*, 73(1), 401–412. https://doi.org/10.1007/s10846-013-9969-5

Lv, Z., Qiao, L., Hossain, M. S., & Choi, B. J. (2021). Analysis of using blockchain to protect the privacy of drone big data. *IEEE Network*, 35(1), 44–49. https://doi.org/10.1109/MNET.011.2000154

Maghazi, O., &Netland, T. (2019). Drones in manufacturing: Exploring opportunities for research and practice. *Journal of Manufacturing Technology Management*, 31(6), 1237–1259. https://doi.org/10.1108/JMTM-01-2019-0099

Mao, W., & Boyd, C., “Towards formal analysis of security protocols,” in *[1993 Proceedings Computer Security Foundations Workshop* VI Franconia]. IEEE, 1993, pp. 147–158.

Mazdin, P., &Rinner, B., “Coordination of mobile agents for simultaneous coverage,” in *International Conference on Principles and Practice of Multi-Agent Systems Turin*. Springer, 2019, pp. 170–185.

Meadows, C., “A model of computation for the nrf protocol analyzer,” in *Proceedings The Computer Security Foundations Workshop VII Franconia*. IEEE, 1994, pp. 84–89.

Minu, M., & Aroul Canessone, R. (2021). Secure image transmission scheme in unmanned aerial vehicles using multiple share creation with optimal elliptic curve cryptography. *Indian Journal of Computer Science and Engineering*, 12(1), 129–134. https://doi.org/10.1017/S1843309018000607

Mitchell, R., & Chen, R. (2013). Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 44(5), 593–604. https://doi.org/10.1109/TSMCS.2013.2265083

Nagoudi, H., & Harshahani, J., “Re: Relay-assisted physical-layer key generation in unmanned aerial vehicles,” in *2018 IEEE 87th Vehicular Technology Conference (VTC Spring) Porto*. IEEE, 2018, pp. 1–5.

Nikooghadam, M., Amintooei, H., Islam, S. H., & Moghadam, M. F. (2020). A provably secure and lightweight authentication scheme for internet of drones for smart city. *Journal of Systems Architecture* 115 , 101955 doi:10.1016/j.sysarc.2020.101955.

Okoli, F., Lang, Y., Kermorgant, O., & Coro, S. (2019). Cable-driven parallel robot simulation using gazebo and ros. In *ROMANSY 22:Robot design, dynamics and control* (pp. 288–295). Springer.

Ouffi, K., & Phan, R. C.-W., “Privacy of recent rfid authentication protocols,” in *International Conference on Information Security Practice and Experience Switzerland*. Springer, 2008, pp. 263–277.

Ozdemir, U., Aktas, Y. O., Vuruskan, A., Dereli, Y., Tarhan, A. F., Demirbag, K., Erdem, A., Kalaycioğlu, G. D., Ozkol, I., & Indah, G. (2014). Design of a commercial hybrid vtol uav system. *Journal of Intelligent & Robotic Systems*, 74(1), 371–393. https://doi.org/10.1007/s10846-013-9900-0

Ozmen, M. O., & Voyvuz, A. A., “Dronecrypt-an efficient cryptographic framework for small aerial drones,” in *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)* Los Angeles. IEEE, 2018, pp. 1–6.

Pastor, E., Lopez, J., & Royo, P., “A hardware/software architecture for uav payload and mission control,” in *2006 ieee/aiaa 25TH Digital Avionics Systems Conference Portland, OR, USA*. IEEE, 2006, pp. 1–8.

Pellerito, V., Olivas, M., & Hassanaliali, M. (2020). Design a fixed-wing unmanned aerial vehicle with dynamic soaring capability for titan exploration. AIAA Scitech 2020 Forum 1, 2018 doi:10.2514/6.2020-2018.

Pienjroj, P., Schönborn, S., & Birke, R., “Exploring deep reinforcement learning for autonomous powerline tracking” in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* Paris. IEEE, 2019, pp. 496–501.

Pirker, D., Fischer, T., Lesjøk, C., & Steger, C., “Global and secured uav authentication system based on hardware-security,” in *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud) Oxford*. IEEE, 2020, pp. 84–89.

Propulla, N., Veeno, S., & Srinivasulu, G., “Development of algorithms for mav security,” in *2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT) Bangalore*. IEEE, 2016, pp. 799–802.

Pu, C., & Li, Y., “Lightweight authentication protocol for unmanned aerial vehicles using physical unclonable function and chaotic system,” in *2020 IEEE International Symposium on Local and Metropolitan Area Networks Orlando, FL, USA (LANMAN). IEEE, 2020*, pp. 1–6.

Putera, A. S., & Ramdani, F. (2018). Software testing by standard software metrics method; study case “mission planner” uav ground station software. *Journal of Telecommunication, Electronic and Computer Engineering (ITEC)*, 10(1–8), 123–128.

Putranto, D. S. C., Aji, A. K., & Wahyudono, B., “Design and implementation of secure transmission on internet of drones,” in *2019 IEEE 6th Asian Conference on Defence Technology (ACDT) Bali*. IEEE, 2019, pp. 128–135.

Rabiei, K., Mercan, S., Akkaya, K., Baboolal, V., & Aygun, R. S., “Privacy-preserving and efficient sharing of data needed in public safety scenarios using proxy re-encryption,” in *2020 IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI) Virtual, Las Vegas*. IEEE, 2020, pp. 45–52.

Roja, G., Anbolagans, S., Subramaniyan, A. G., Selvakumar, M. S., Bashir, A. K., & Mumtaz, S. (2021). Efficient and secured swarm pattern multi-uav communication. *IEEE Transactions on Vehicular Technology*, 70(7), 7050–7058. https://doi.org/10.1109/TVT.2021.3082308

Rajendran, S., & Srinivas, S. (2020). Air taxi service for urban mobility: A critical review of recent developments, future challenges, and opportunities. *Transportation Research Part E: Logistics and Transportation Review*, 143, 102090. https://doi.org/10.1016/j.tre.2020.102090

Ramirez-Atencio, C., & Camacho, D. (2018). Extending agroundcontrol for automated mission planning of uavs. *Sensors*, 18(7), 2339. https://doi.org/10.3390/s18072339

Ranyal, E., & Jain, K. (2021). Unmanned aerial vehicle’s vulnerability to gps spoofing a review. *Journal of the Indian Society of Remote Sensing*, 49(3),
Sharma, D., Gupta, S. K., Rashid, A., Gupta, S., Rashid, M., & Srivastava, A. (2020). A novel approach for securing data against intrusion attacks in unmanned aerial vehicles integrated heterogeneous network using functional encryption technique. Transactions on Emerging Telecommunications Technologies 31, e4114. doi:10.1002/ett.4114

Sharma, A., Vanjani, P., Paliwal, N., Basnayaka, C. M. W., Jayakody, D. N. K., Wang, H.-C., & Muthuchildibaramanathan, P. (2020). Communication and networking technologies for uavs: A survey. Journal of Network and Computer Applications, 168, 102739. https://doi.org/10.1016/j.jnca.2020.102739

Shavaran, S. M., Nejad, M. G., Rismanchian, F., & Izbirak, G. (2018). Application of hierarchical facility location problem for optimization of a drone delivery system: A case study of Amazon prime air in the city of San Francisco. The International Journal of Advanced Manufacturing Technology, 95(9), 3141–3153. https://doi.org/10.1007/s00170-017-2136-1

Shin, S.-Y., Kang, Y.-W., & Kim, Y.-G. (2019). Obstacle avoidance drone by deep reinforcement learning and its racing with a human pilot. Applied Sciences, 9(24), 5571. https://doi.org/10.3390/app9245571

Shin, S.-Y., Kang, Y.-W., & Kim, Y.-G. (2020). Reward-driven u-net training for obstacle avoidance drone. Expert Systems with Applications, 143, 113064. https://doi.org/10.1016/j.eswa.2019.113064

Shoufan, A., “Continuous authentication of uav flight command data using behaviometrics,” in 2017 IFIP IEEE International Conference on Very Large Scale Integration (VLSI-SoC) Dubai. IEEE, 2017, pp. 1–6.

Shoufan, A., Al-Angari, H. M., Sheikh, M. F. A., & Damiani, E. (2018). Drone pilot identification by classifying radio-control signals. IEEE Transactions on Information Forensics and Security, 13(10), 2439–2447. https://doi.org/10.1109/TIFS.2018.2819126

Šiljeg, A., Domazetović, F., Maric, I., Lončar, N., & Pana, I. (2021). New method for automated quantification of vertical spatio-temporal changes within gully cross-sections based on very-high-resolution models. Remote Sensing, 13(2), 321. https://doi.org/10.3390/rs13020321

Singh, A. D., & Alvarez, F. V., “Simulating gps-denied autonomous uav navigation for detection of surface water bodies,” in 2020 International Conference on Unmanned Aircraft Systems (ICUAS) Athens. IEEE, 2020, pp. 1792–1800.

Song, D. X., Berezin, S., & Perrig, A. (2001). Athena: A novel approach to efficient automatic security protocol analysis. 1. Journal of Computer Security, 9(1–2), 47–74. https://doi.org/10.3233/JCS-2001-9-1-203

Sparrow, R. D., Adelkunle, A., & Berry, R. J., “Leopard: Lightweight encryption operation permutation addition rotation and diffusion,” in 2016 10th International Conference on Signal Processing and Communication Systems (ICSPCS Surfers Paradise). IEEE, 2016, pp. 1–5.

Srinivas, J., Das, A. K., Kumar, N., & Rodrigues, J. J. (2019). Tcalos: Temporal credential-based anonymous lightweight authentication scheme for internet of drones environment. IEEE Transactions on Vehicular Technology, 68(7), 6903–6916. https://doi.org/10.1109/TVT.2019.2911672

Steinemann, J. A., Babicoum, R. F., & Seker, R., “Uas security: Encryption key negotiation for partitioned data,” in 2016 Integrated Communications Navigation and Surveillance (ICNS) Herndon. IEEE, 2016, pp. 164–1.
Samanth et al., Cogent Engineering (2022), 9: 2029080
https://doi.org/10.1080/23311916.2022.2029080

© 2022 The Author(s). This open access article is distributed under a Creative Commons Attribution (CC-BY) 4.0 license.

You are free to:
Share — copy and redistribute the material in any medium or format.
Adapt — remix, transform, and build upon the material for any purpose, even commercially.
The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:
Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made.
No additional restrictions
You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

Cogent Engineering (ISSN: 2331-1916) is published by Cogent OA, part of Taylor & Francis Group.
Publishing with Cogent OA ensures:
- Immediate, universal access to your article on publication
- High visibility and discoverability via the Cogent OA website as well as Taylor & Francis Online
- Download and citation statistics for your article
- Rapid online publication
- Input from, and dialog with, expert editors and editorial boards
- Retention of full copyright of your article
- Guaranteed legacy preservation of your article
- Discounts and waivers for authors in developing regions

Submit your manuscript to a Cogent OA journal at www.CogentOA.com

Yang, Y., H. D., Majeed, F. (2021). A distributed framework of autonomous drones for planning and execution of relief operations during flood situations. International Arab Journal Of Information Technology, 18(1), 16–24. https://doi.org/10.34028/ijit/18/1/3

Zema, N. R., Trotto, A., Natalizio, E., Di Felice, M., & Bononi, L. (2018). The cucus simulator for distributed networked control systems: Architecture and use-cases. Ad Hoc Networks, 68, 33–47. https://doi.org/10.1016/j.adhoc.2017.09.004

Zhang, Y., He, D., Li, L., & Chen, B. (2020). A lightweight authentication and key agreement scheme for internet of drones. Computer Communications, 154, 455–464. https://doi.org/10.1016/j.comcom.2020.02.067

Zhang, H., Kumari, S., Obaidat, M. S., & Wei, F. (2020). Gateway-oriented two-server password authenticated key exchange protocol for unmanned aerial vehicles in mobile edge computing. IET Communications, 14(15), 2427–2433. https://doi.org/10.1049/iet-com.2019.1009

Zhi, Y., Fu, Z., Sun, X., & Yu, J. (2020). Security and privacy issues of uav: A survey. Mobile Networks and Applications, 25(1), 95–101. https://doi.org/10.1007/s11036-018-1193-x

Zuluaga, J. G. C., Leidig, J. P., Trefftz, C., & Wolffe, G., “Deep reinforcement learning for autonomous search and rescue,” in NAECON 2018-IEEE National Aerospace and Electronics Conference Dayton. IEEE, 2018, pp. 521–524.