DroneMap: An IoT Network Security in Internet of Drones

Rajani Reddy Gorrepati and Sitaramanjaneya Reddy Guntur

Abstract Internet of Drones (IoD) is a major role for the central military, agriculture and IoT applications that requires critical information to be processed. It ensures that security and network privacy issues in the Internet of Drones (IoD) have malware/vulnerable attacks and Distributed Denial of Service (DDoS) attacks are highly energy-constrained, which are a direct standard of cryptography protocols and secured key IoD algorithms. IoD is a capable of enhanced state-of-the-art of Drones while providing services from an existing cellular networks. IoD is vulnerable to malicious attacks over radio waves frequency space due to the increasing number of attacks and threats to a wide range of security measures for IoD networks. Low cost of Unmanned Aerial Vehicles (UAV) known as Drones for enabling various IoT applications. UAV are also used in several applications in surveillance, disaster, environment and management search and rescue monitoring solutions that are limited to point-to-point communication patterns, and are not suitable for distributed applications in multi-UAV scenarios. UAV has limited processing and storage capabilities with massive computations requirements for certain applications. In this book chapter, we represent the Drone-map planner that are service-oriented fog-based drone management system that controls, monitors and communicates with Drones over the network. Drone-map planner that allows to communicate with multiple Drones over the internet, which are enables to control anywhere and anytime without any long distance restrictions. Drone-Map planner provides access to fog computing resources for drones to heavy load computations. To classify the attacks based on the threats and vulnerabilities associated with the networking of drone and their incorporation into the existing cellular setups. This chapter of book summarizes the challenges and research directions to be followed for the security of IoD.

Keywords Internet of Drones · Security · UAV · Internet of things · Drone map

R. R. Gorrepati
Department of Computer Science and Engineering, Vignan's Foundation for Science, Technology, and Research, Vadlamudi, Guntur 522013, India

S. R. Guntur (✉)
Department of Electronics and Communication Engineering, Vignan's Foundation for Science, Technology, and Research, Vadlamudi, Guntur, India
e-mail: drgsr_ece@vignan.ac.in

R. Krishnamurthi et al. (eds.), *Development and Future of Internet of Drones (IoD): Insights, Trends and Road Ahead*, Studies in Systems, Decision and Control 332,
https://doi.org/10.1007/978-3-030-63339-4_10

1 Introduction

Internet of Things (IoT) and fog computing attracted a great deal of interest in contact with the Unmanned Ariel Vehicle (UAV). UAV has remotely interacted with fog computing, web technologies, and service-oriented architecture (SOA) through newly developed IoT. Mainly, the concept of the Internet of Drones (IoD) is framed to access and control the moments of drones in airspace using layered control architecture with navigation services between locations [1]. The three major layered architectures are mobile network, air traffic control network, and the IoT, which are provided for different UAV applications that are present implementation of the architecture. The context of fog computing robotics has been coined that are an effort to incorporate robotics across the internet with fog computing. The drawbacks of low-cost UAVs are processing and storage capacities and battery-powered UAVs that are efficient in computing specific applications with real-time data and reliability constraints.

UAV is a flying detected object identification as an autonomous driving capabilities that can perform particular tasks for simple operations of complex objects [2–6]. IoD packages that are monitor to transmission delivery in coastal areas for the identification of wood, fire prevention.

IoD drones that are feasible related to remote-controlled operations that are automatically adjust the speed parameters and to detect directions like planes. UAV is also working as drones mainly are investigate such kind of applications used in for security purposes such as military, medical, live stream operations, and agriculture field [7, 8]. The optimization of IoT security mechanisms for the direct adoption of IoD to feasible and secured protocols. Protocols can operate in various network layers by providing services such as mobility, real-time, and clock synchronization communication. In the recent study, some of the authors investigated and found the vulnerabilities attacks on IoT applications in existing security mechanisms and standards were implemented such kinds of systems.

The critical security mechanisms and optimized algorithm for variable cryptography solutions for IoDT [9]. Some researchers found security attacks in the IoD, however, reported successful hacking and hijacking of an AR. Drone 2.0 (equipped with a 32-bit ARM processor) resulted by the crystallographic lack of secure communication channels is suggesting that the majority of commodity drone telemetry systems do not use cryptography to protect your correspondence [10]. Thus, they suggested a method of fingerprinting that could provide some protection for drones. A lot of advanced work is to identify the security attacks of the current drone configurations [11–13], they work on how to determine the frequency of the FHSS series of drone controllers used to describe radio frequencies [14], and to demonstrate the attacks due to the cause of drones to crash by radiofrequency of MEMS gyroscopes. MAV link protocols to get results that disable the drone attack mission.

UAVs can be considered a crucial solution in many areas of medical monitoring, agriculture, and transport [15, 16]. UAV-assisted can operate wireless network connectivity where to development of an expensive physical infrastructure. Drones are robotic flying network systems, which can be considered dynamics of drone flight

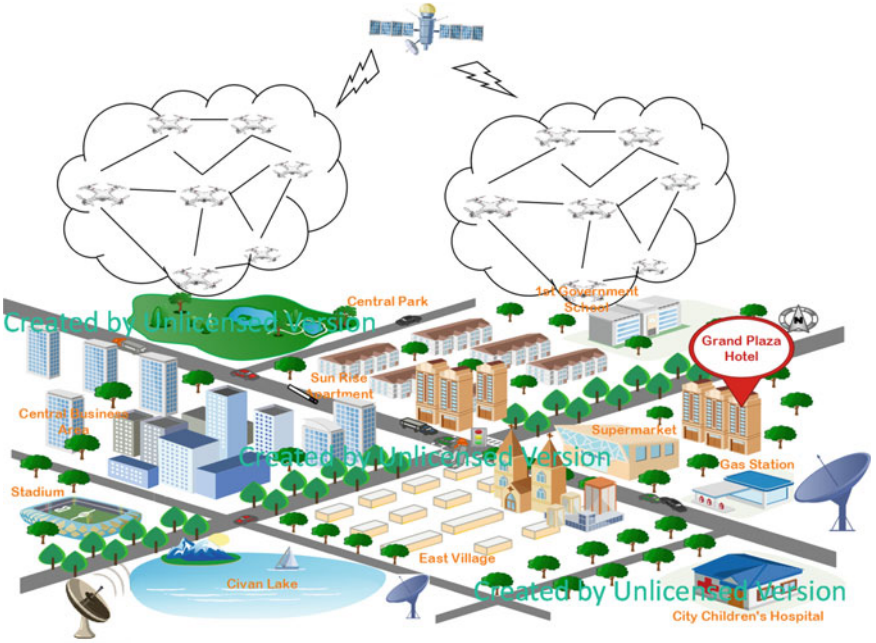

Fig. 1 Communication of the societal environment through the Internet of Drones (IoD) to Geo Satellite

that are mathematical representations by physical laws [17]. UAV modelling is strongly enhanced deep learning by solving connected robotic operations like recovering navigation, path planning, localization, and control [18]. Remote control systems [19] refer to a class of software that interfaces the on-board UAV between the operator and the pilot to ensure that each flight operation corresponds to what the pilot intended.

Figure 1 shows the communication of societal environment like central military, agriculture, stadium, central Park, supermarket through IoD to Geo Satellite. The application of IoTs to transmit and processes critical information. It ensures that the security and network privacy issues related to malware/ vulnerable attacks and distributed denial of service (DDoS) attacks are highly energy-constrained, which are the direct standard of cryptography protocols and secured IoD key algorithms. IoD is capable of enhanced state-of-proof of drone's communication existing through mobile network services. IoD is vulnerable to malicious attacks over radio waves frequency space due to the increasing number of attacks and threats that are alert to the attention of security measures for IoD networks.

Low cost of UAV, known as Drones, to enable various IoT applications [20–24]. UAVs are also used in many rescue operations, environmental disaster management, and surveillance applications. However, point-to-point communication is limited and may not be suitable for distributed applications in multi-UAV scenarios. UAV has

limited processing and storage abilities with enormous quantitative prerequisites of specific applications. In this chapter, the Drone-map organizer is a service-oriented fog-based automation framework that controls to communicate with drones over the network. A Drone-map organizer is allowed to communicate with multi drones over the internet, which empowers them to control anywhere and anytime without any restrictions for long-distance.

The emerging IoT technology is continuous with fog edge computing environment by special software that generates their behavior and objectives in which the local concept of orchestration for large smart objects utilized and global users. IoT enables the objects and everyday activities of various communications tools in the context of smart-home vision [25]. IoT objects are more complex than the flexibility and transformation with a low-cost, fusion of heterogeneous networks highly distribution security problems in sensor networks, challenges the privacy protection specific network issues that are generated [26]. IoT needs to support network security and privacy challenges that are present features in handling of internal and external security threats/attacks, authentication, access control, data protection, malware detection, and high-level authorization [27].

Drone-Map planner gives admittance to fog computing resources for drones to heavy load computations. Air traffic control network is relevant to the Internet of drones it provides the security to maintain the free collisions navigation to utilize any types of drones. The main role of the air traffic controller to keep all drones in place as new systems motivate the the scalability of drones to be more autonomous. Automatic dependent surveillance-broadcasting (ADS-B), uses the navigation of drones and broadcast air crafts position [28]. The attacks are classified on the basis of a quantitative analysis of threats and vulnerabilities associated with the networking of drones and their incorporation in to existing mobile setups. This chapter summarizes the overview of the Internet of Drones (IoD) , UAV applications domains and IoT 5G challenges and analyses the IoT.

The privacy and security of the dronecommunication require specified sensors mechanisms that focus on the view of IoD. Recently established 3GPP service standardization with mission-critical push (MC-PTT) [29] features that allow D2D communication to create more robust and heterogeneous UAVs. D2D enables devices to communicate directly through D2D cell spectrum sharing to increase spectrum performance.

2 Overview of IoD and UAV

The IoD architecture for controlling and access over the internet was shown in Fig. 2. Drones are becoming increasingly common the various aspects of missions of drones multiple controlled connected to IoT Gateway, whereas the security terminology of UAV components includes processes, storage, sensors as well as increasing the efficiency of battery life and drone components and lower expectations. IoD supplies a vehicle of the Internet of things with robotics technology to allow remote control

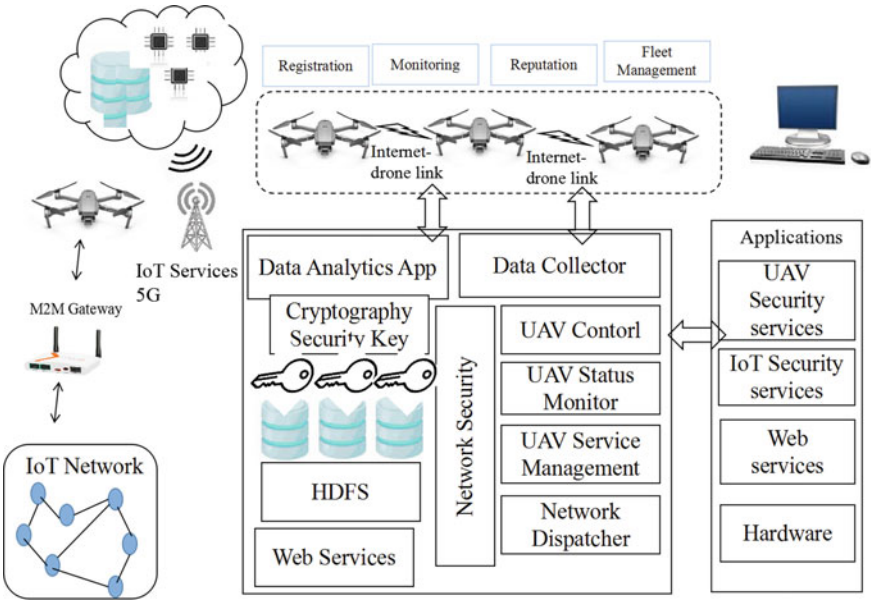

Fig. 2 Internet of Drones (IoD) security architecture

of drones as the seamless scalable of remote storage. UAV challenges associated with the point-to-point communication connected to the internet of drone wireless connectivity through the efficiency of resources (Fig. 2).

IoD security and quality of service (QoS) is criticle and big challenge in accessing drone resources with an authenticated and secured. IoD system various attacks like drone impersonate, sniffing, flooding, and technical details using a service-oriented approach, usually implemented the applications are UAV and IoT security services, and SOAP or REST web services [30]. Users may not be used as a technical programme or as missions to develop web services based on on-board access resources through various APIs. This architecture represents the Internet of Drone planning system to find out the system that addresses functional specifications.

The service layer provides services using a collection of resources represented by the UAV exposed at the end of the user. On top of the hardware, the robot operating system (ROS) and MAV link layer are used to develop the robotics application abstracts for network and processing systems like navigation, movements of object organizing, communication of information control at low-level devices. MAV link built over various transmission protocols such as TCP and UDP, which permits the exchange of predefined drones and ground station data to a high-level application interface for developers to automatically control and direct drones without any hardware intervention.

The server-side storage components for data streams captured by each IoT climate change, societal data, and transmission of information sources including sensor and time stored image data. Storage is a distributed system that assists with performs

enormously manage stored data on a scale using software like the Hand-hoop chart. The real-time stream processing sample images are obtained from IoT and process data streams to detect possible attacks or threats requiring immediate action to perform a dynamic distribution environment. The real-time processing of data may be the necessary bases for the application, or new events are detected that required dynamic rescheduling of drones. Network interfaces to implement a server-side network sockets and web socket interfaces that manage sent UAV protocol can handle stream applications, context of drone map, and MAV communication information is collected via network sockets and sent to client device web sockets. The web service interface permits users to control drones and their applications. Web services are utilized to give the end-clients and users application services to control commands and observed the drones through parameters. The client layer can provide interfaces for both end-users and drones web applications that provide interfaces for both the IoT service layer and the UAV layer. The client layer provides several users who have registered multiple UAVs, transform parameters, and data analysis and decision making based on APIs for various programming languages to interact with drones.

2.1 Layers of UAV Drone

A specialized onboard data acquisition software is used to record the GNSS data automatically, which will not require manual intervention to on/off logging and can operate robustly in unattended mode. Figure 3 shows the layered architecture for UAV Drones IoT communication. The GPS recorded every tracing point with the coordinates of GNSS geo-tagged data and communicates wirelessly to the ground station as shown in Fig. 3. However, the drone is arranged with RTK GPS, and the exact coordinates are used for geotaging data. Drones are located in large-area surveys to collect the data and transform to ground stations via wireless communication. The drone moments are controlled by the operator from the ground station using GNSS and are able to monitor how the GNSS works to trace current data, record the data of start/stop, settings and mode changes of GPR, etc. GNSS software interfaces with the hardware of drone and ground station data log and wireless communication BUS, which can transform the data link to ground control in to task management and information monitoring.

UAV enables communication networks to suffer an allocations dedicated spectrum that is a high impact on energy efficiency. IoD enables the connectivity of drones via mobile networks in order to facilitate the data gathering in airspace and enhance storage capabilities and information management service. UAVs are remotely controlled and commanded by the operator from base stations using coordinated IoD through various channels deployed in UAVs. IoD acquires the related information from the sensors arranged on drones. IoD is being deployed for next-generation applications like smart car parking, smart health, smart military, and

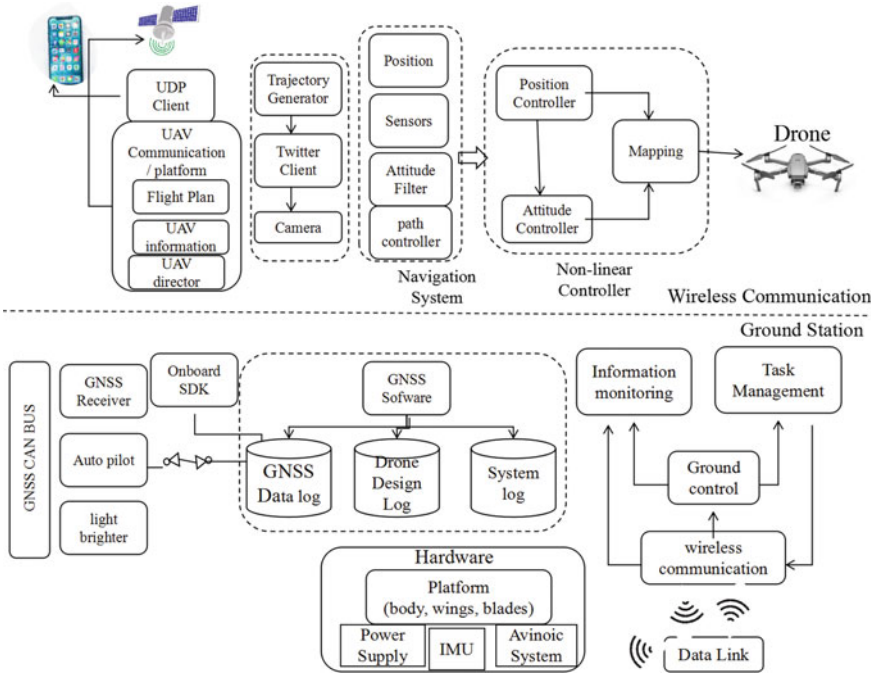

Fig. 3 Layered architecture for UAV drones IoT communication to a ground station

cellular networks. The next generation of IoD is integrated into third party object-oriented systems with the variety of tasks in collaboration modes and abilities for multitasking and operate the rural and urban environments. The attacks or threats are considered to be important factors for exploiting and vulnerabilities sensitive pieces of information are gathered to the IoD security and protect information. The drone controller of the central processing unit of the IoD and the communication to read process the data provided by the various sensors is useful it in the information. The drone controller implements the commutation interface between drones and the ground control station. The ground control station is located on the ground floor and provides human operations to monitor their activities in order to communicate with drones to send commands and receive data in real-time. The data link communicates to the wireless network that is controlled information between the drones and the ground control station via the communication network.

UAVs are used to provide individual Internet access to rural areas that are not protected by traditional communication areas. In Fig. 3, the four function layers are defined by various levels of quantitative complexity that can be described by the layer operator as a task related to the current flight status of the camera. The flight machine can be launched by installing a ground control station that is monitoring on smart-phones, PCs, and tablets. The simple guidance framework produces a route based on the different paths of the twitter client to the camera. UAV produces the

route based on many ways that the first layer in this system can provide robots with the ability to automatically track the location of the multiple drones by mapping the direction.

2.2 *UAV Sensor Technologies in 5G Networks*

5G Technology is designed to improve the network traffic and high availability security control and mobile broadband applications that are required in a very low latency, supported by industrial applications, remote manufacturing, and tracking. UAV drones can be used for smart agriculture, smart buildings, virtual and augmented reality without limitations of scope including home enterprises, critical machine-to-machine communication. In the sense of 5G devices that can be integrated with deferential devices, communications may be implemented in appropriate gateways in the context of 5G architecture that is presented. Accelerometers are used to define flight control sensors to determine the location and orientation of the drone flight. Drones and UAV manage to flight.

Figure 4 demonstrates the sensor technologies that are assisted as part of drones that can be separated into three categories. The main categories are drone power, data collection, and communication sensors. The evaluation of drone internal control

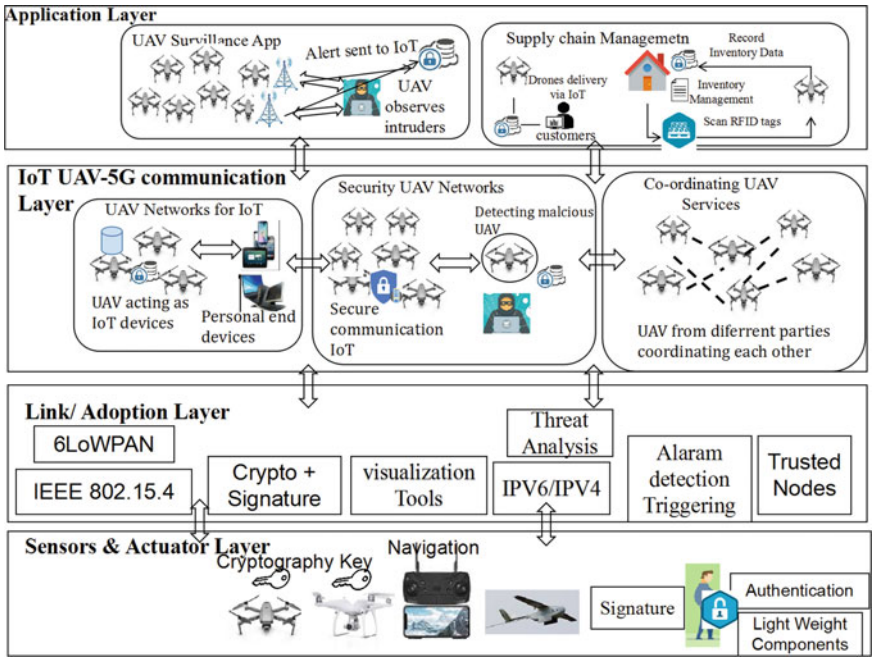

Fig. 4 Secured 5G mobile communication layers in UAV drones IoT

sensors that are accelerometers is used to measureof drone's position of the trajectory in the flight. The 5G technology is designed to enhance mobile broadband applications that requiring very low latency and to enhance the traffic protection and control provided by industrial applications, remote monitoring, security logistics, and fleet management. It also utilizes the smart agriculture, a virtual augmentation without the limitations of scope of enterprises that are vital device-to-device communications. Drones assisted by 5G network use cases linked to communication / linking involved automatic detection trajectory paths and robotics. Accelerometers are used to determine the position and oriented flight of the drones can manage to flight paths and directions using the flight control sensors with GNSS navigation. The flight control framework is designed to maintain the level of flight feedback from the tilting sensors coupled with accelerometers and gyroscopes. When the applications are required at a high level of scalability and effectively monitor and sensors to estimate the proper reduces estimations and consumption are reduced.

Data Acquisition Sensors: Drones are equipped with many sensors to collect the data needed for certain activities, depending on the function of the sensor to be used for data acquisition by drones. UAV may be equipped with high-end sensors and radar of air-bone systems that provide resolutions, surveillance and monitoring of applications sensors environmental and weather parameters sensors are used in the control of disaster.

UAV Communication systems: Manage and control tasks performed in communication systems and multiple network technologies of drones that are required to communicate with one another. A comprehensive list of network protocols and communication methods allowing multiple applications for IoT architecture complex network segments interconnected to multimedia streaming surveillance. It is based on the data rates and latency specifications available in 5G drone communications technology, which are allowed worldwide applications. In the conceptual model, UAVs can interconnect complex network segments of IoT networks for demanding services. Security services must be implemented in the Link/Approval layer of IPV6. The adoption layer that provides end-to-end encryption, continuous security key management mechanisms for authentication schemes, is designed to provide robust communication at the endpoint security channels protocols were proposed. Secure connections with firewalls link and intrusion protection system are allowed. Physical losses are the key security risks in the data link layer that include routing attacks such as selective forwarding, sinkhole, and hot-hole attacks [31]. Primary security threats in the 5 G network communication layer that cause physical damage to the hardware framework, like intrusion and detection of processes, should ensure that only users can access sensitive data generated by physical devices.

Privacy and protection for UAVs: Privacy of the IoT domain and protection for receiving, storing, and transmitting sensitive object information and building patterns and a variety of links that can be used as IoT device signatures. One of the core challenges in the design of cooperative applications involving several UAV networks that can simultaneously provide coordination between the different types of protection and the fleet task of developing and sustaining scalable aerial networks, which are fleet management techniques. Drone Map applications support various

drone applications over the internet and we need to build some real-world applications with drone map planners to demonstrate the efficiency of IoT applications enabling. All services of the Drone map planner are designed to destroy applications with predefined IP address port number and primary entity, including IP address, port number, and MAV link device ID. When a drone communicates over the internet, it communicates the drones automatically and is shown on the web interface. The web interface contains all data about drones, including altitude, air/ground speeds, battery level, GPS coordinate location address. These real-time data are accessed via the web services interface using a remote device.

3 Security Threats and Attacks of IoDT (Internet of Drones Things)

Figure 5 shows the vulnerability of IoT drones to detect contact pathways and attack as a variety of vulnerabilities. These are the techniques used to hacking the UAV drones from channel jamming and to Spoof malware, such as the Middle-Man attack

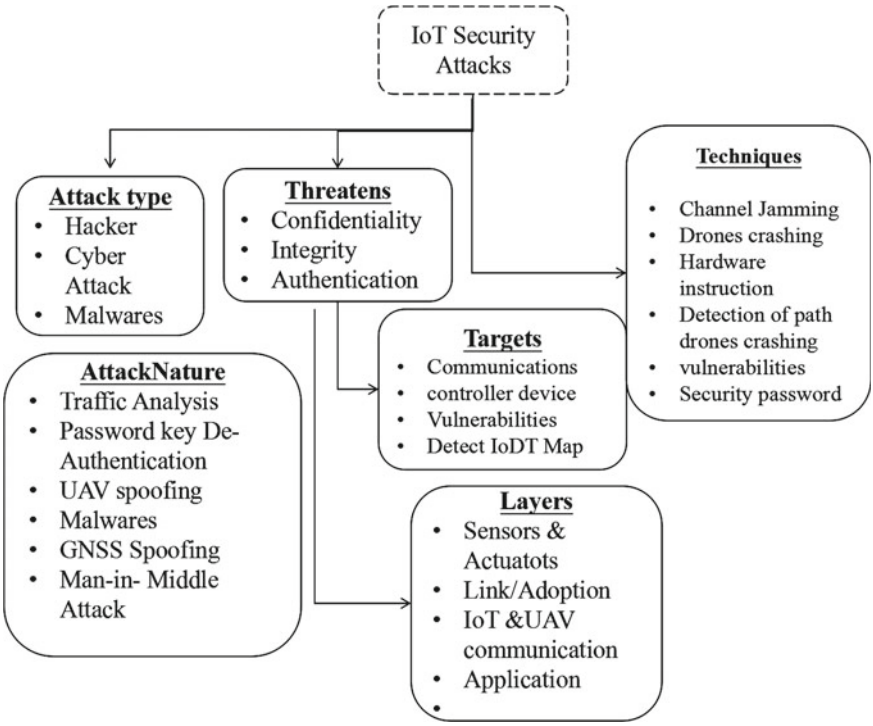

Fig. 5 IoT security attacks for communication with IoT

and the GNSS spoofing. The adoption of link layers non-lethal solutions to counter these threats to be various malware such as highly inefficient and the data presents some of the issues related to drone communication pathways that threats are in highly-ineffective and unreliable. UAV fault-tolerant control present in the device architecture, using a neural network adaptive framework for the identification and isolation of the network design. In this scheme, real-time detection in drones ensures real-time identification and isolation of faults in actuators to configure network issues that are tolerant in order to reconfigure the controller or have an impact on efficiency. In this Wi-Fi jamming, the approach is observed to be implemented as these drones use a 2.4 GHz frequency.

All these jams are wireless contact within a specific area of coverage. However, very small jamming capacity cannot be easily identified in the environment, and other nearby frequencies are jammed. This approach is based on a three-way handshake router and newly installed rogue computers. It allows the attacker to de-authenticate, or jam, the connection between the drones and the control unit. The Wi-Fi attack that was present enables the attacker to search for drones to communicate the DDoS attack, which interprets the transfer of the particular data, either delaying it, which allows the attacker to leads the de-authenticated attack. A DOS assault that intercepts network traffic and floods with a request to interrupt a drone/device link. Denial of service will be performed either by de-authenticated of the UAV drones that access can be sent periodically to the drone network security event commands . This leads to the estimation of the location of the drone unit for the GNSS signal simulator used by drones to launch a GPS spoofing attack, which transmits false signals to the control system of each drone, normally more powerful than the fake signals instead of the original ones.

GNSS allows drone navigation non-encryption of easily spoofed signals that are directly managed by anti-spoof algorithms operator that can help mitigate GPS spoof attacks. A drone that uses GPS could be targeted by jamming the GNSS signal that makes the drones unable to determine their location. Jamming the objective of disrupting all satellite communication during antenna selection and orientation can help to minimize jamming attacks. Eavesdropping successfully dealt with in Man-in-Middle attacks allows the attacker to track violation of drone confidentiality. Some of the confidential information that collects through IoT when it classifies them in terms of privacy and trust, with their respective tasks. If the data is interferes with the data access to adjust the cluster controller and the malicious actions of the controller to gain control of the drones. The main task is to safely store IoT data integrity, data protection, and encrypted data that is not available to anyone without any key for decryption (Table 1).

4 Security Issues Associated by IoD

The IoT security attacks and Jamming attack, which is interference with radio signals that causes communication problems for drones to function efficiently as well as the

Table 1 IoDT security detects malware, threats, and vulnerabilities

Attacker	Security impact parameters	Target components
An attacker signature key and capture the network communications	Privacy, integrity, and confidentiality	Network platforms
An attacker can produce transmission information	The user can misguide the falsified integrity data	Network platforms services
By obtaining access control an attacker may alter authentication or access permission	Non-legitimate users can be caught and permission alerted which leads to system crash	Network platforms services
DOS and physical attacks by excessive false request	The main target of the attacker is to disable the IoT devices used for some applications	Network platforms services
IoT coordination can be warned by hacking or GNSS spoofing	The attacker caught by the IoT devices or altered the coordination which could result in collision attacks	Network platforms services
The attacker can affect the performance of IoT by increasing the resource depletion rate.	The performance of IoT in the target missions which may lead to mission failure	Network platforms services
The attacker can capture the IoDT services	The IoT is assigned for dedicated tasks of component services lead to facilities	Network platforms services

effect of energy usage. Data exploitation is an intrusion into the sensitive data of the server, and access to confidential information. Some of the collisions when two or more drones operate at the same frequency in order to operate the unreliability of the network. Attackers can degrade the entire system by causing other drone nodes to do real-time based transmissions. Malicious node that causes all types of packet disruption/corruption to pass through them and other associated packet loss attacks that impact packets and through put delivery ratio methods are needed.

A flooding attack can cause huge packet flow resulting in a complete network congestion De-synchronization attack is a malicious node that moves messages by transmitting sequence numbers to more than one network operating node. Network Jamming attacks are disrupt some of the nodes on the Man-in-Middle attacker network, which deploy a malicious drone between the operating network, causing leakage of information, disruption, and other security attacks. Drones instability and other non-compatibility with IoT-based operations. Apart from other problems, limited capital, less processing power, and limited storage space, the overall IoT functions as a back door. Service Denial attacks, privacy threats, malicious access points, unauthorized threats, IoT application services intrusion attack. Real-time applications also need to be addressed, depending on the application scenario of the drone fleet management. Device control, considering into account the quality of the service

parameter, will become a key issue and a further significant obstacle to 5G network access.

5 Evaluation of IoD Control Sensors

The accelerometer used to determine the direction and orientation of the drone in flight, and one of the technologies used to detect embedded devices, which did not have any moving drones, and the UAV systems managed to maintain the drone route measurement units together with the GNSS. As a results, this process helps to evaluate the paths of the drone.

UAVs monitor the airflow sensors effectively to estimate the correct rate at the required speed in order to reduce the overall optimizing power consumption and to detect system engine failures. IoT based UAV is a more complex concept architecture in which machines can interact with dynamic processes of smart objects and technological ecosystems. Security mechanisms such as restricted application protocol access control and user application protection that allow for protected messages and are minimal configurations such as filtering and perimeter protection [32]. Privacy security is a wide range of sensors that measure different types of information to ensure the group signature and data of all communication protocol devices with an authentication mechanism.

The integrated community of signature methods tends to be effectively securing and preserving the identity of data encrypted measuring devices to prevent interpretation of dummy data by the reporting service. Most of these devices have focused on the processing of video content through computer vision. In this case, privacy-protected solutions concerns are handheld devices that can be used from drone targets and displays from multiplepoints of view, introducing a new dimension. Jamming is used for the proposed scheme that goes beyond malicious transmission activities to all radio communications. The transmitter and receiver can be exchanged while cooperative jamming enables the content of the two parties to communicate without restoring the encryption of data. The GNSS jammer could be adopted to attack the signal correlation mechanism by transmitting the location, navigation, and timing (PNT) capabilities of a particular receiver [33]. Conflicting concepts in many safety scenarios to prevent unintended communication between the different methods used to determine the position of a radio receiver by manipulating the distribution of radio signals and inferring the distance to be a transmitter following well-known propagation models [34, 35]. In most cases, the implementation of the above techniques or drones is feasible ; such techniques rely on available radio-level knowledge. One of the most reliable Received Signal Strength (RSS) information, without loss of attack and scenario in general. Several strategies were conceived to counteract malicious jammers. The jamming attacks are intended to mitigate the harmful impact on frequency spread spectrum of satellite communication by exploiting the solution provided by a cooperative spatial algorithm that allows drones to cooperatively mitigate jammer action [36].

Figure 6 shows the drones that use the Jamming signal to estimate the range, the secret behind the solution that enables a drone to push forward its mission by the presence of a jammer that can be used by any other radio communication to calculate the distance to the transmitting source. Although typical localization techniques suffer from traditional propagation phenomena such as multi-path transmission, the jamming case is radically different, enabling drone communication capabilities to access the GPS location service.

The scenario mentioned above is the ideal situation for estimating the distance between drones and the estimated direction of transmission of the jammer signal, at which distance d can be calculated as [37, 38].

$$d = \frac{\lambda}{4\pi}\sqrt{G\frac{T}{R}} \tag{1}$$

where λ is the radio frequency wavelength, T and R are transmitted and receiver power by jammer and drone, G sums up the transmitter-receiver gains. In the presence of a more practical pathway, the transmitter power and transmitter antennas have again been evaluated for localization variation as the drone moves closer to the jamming signal. We note that the model from Eq. 1 could be strengthened by further statistical definition of the channel due to the multi-path fading of the approximate width. The jamming signal is used to estimate the line-of-sight portion and to follow a tracking mechanism by which the drone first estimates the obtained power

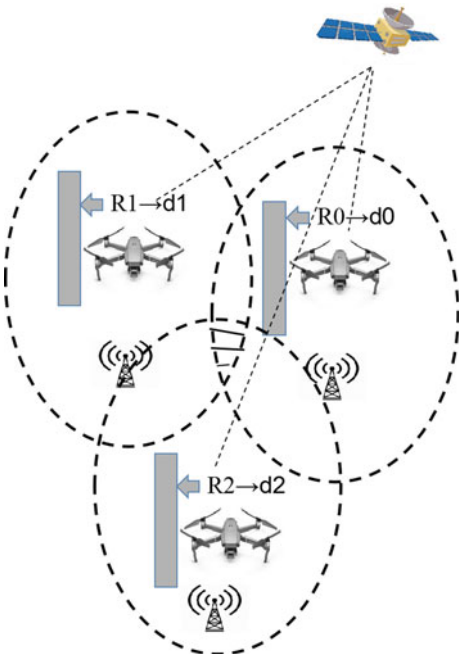

Fig. 6 Drones exploiting the Jamming signal to estimate the range

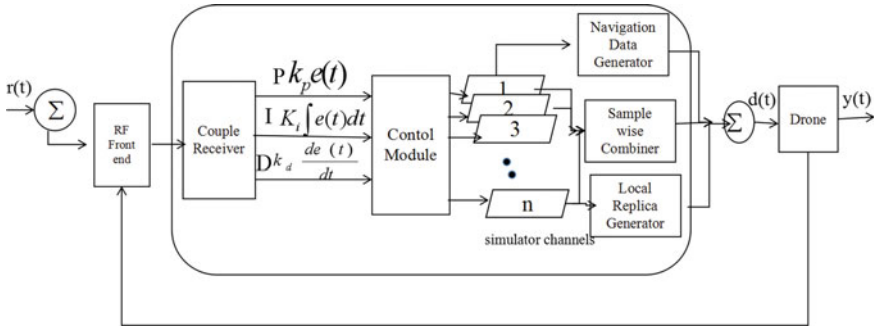

Fig. 7 UAV flight controller spoofing and navigation attack system

$R_1 = 2 \times R_0(+3\,\text{dB})$, the drone can be estimated jammer by a factor of $\frac{d_1}{d_2} = \frac{1}{\sqrt{2}}$, according to the firmware done that has been compromised by a malicious entry. We can implement a navigation device that acts as odd when drones receive radio commands from the remote controller while changing the mode when a jamming attack is detected. It can be presumed that the mode is triggered by the data interruption and communication links of the GNSS [31, 39]. The jammer will deploy various techniques to interrupt contact with the drone, while the same jamming pattern broadcasts the signal in front of the antenna. We believe that our drone is a typical commercial radio feature and that the antenna of the drone is perfectly omnidirectional or a command antenna for more information about the jammer and its location [40, 41].

Figure 7 shows the UAV flight navigation path of the target system controller block diagram, as the drone approximate RSS (Received Signal Strength) of the jammer controller c(t) depends on the output process variable y(t). Y(t) = r(t) is an error e(t) when the signal control variable r(t) is converted . As the error control increases, c(t) compensates for the return to the original value r(t) = y(t) of the output y(t). The three main elements are described by the PID controller: proportional, integrative, and derivative controller via [37, 38]:

$$C(t) = k_p e(t) + k_i \int_0^t e(T)dT + K_d \frac{\partial}{\partial t} e(t) \tag{2}$$

where K_p, K_i, and K_d respectively represent the additive, integral derivative gains. Lastly, we follow methods for tuning the above mentioned parameters. The architectural drone controller must be able to targeting a drone in the presence of a received signal resistance (RSS) jammer and a standard loop control system consisting of a proportional integral and derivative controller (PID) and a drone controller. The GPS systems together have a high degree of complexity of the different subsystems , while the operation of the satellites retains the monitoring and updating tasks of the

stations. IoT cryptography energy consumption for various primitives such as efficient elliptical curve storage techniques while avoiding the overheads cryptography systems and optimising digital key signature and public-key encryption.

6 Conclusions

In this book chapter, we describe the spoofing techniques for the development of a portable system, and the recreation of unauthorized UAV signal form the unauthorised UAV communication system using the low cost SDR equipment, and GNSS receiver vulnerability with partially applicable. We have defined the UAV drones for fleet navigation and coordination for different layers of IoT applications that this framework needs to implement. We suggested an operating model that recognizes the role of private and public entities as an appropriate IoT framework was addressed. We used the information gained from three main networks, the cellular network, air traffic control, and the Internet. Lastly, addressed the gaps and potential studies that could benefit from the large current literature on the solutions.

References

1. Philip, K., Nagi, M.: A framework for sensing radio frequency spectrum attacks on medical delivery drones. IEEE Access (2020). https://www.researchgate.net/publication/341148312
2. Schmidt, E., Akopian, D., Pack, D.J.: Development of a real-time software-defined GPS receiver in a LabVIEW-based instrumentation environment. IEEE Trans. Instrum. Meas. **67**(9), 2082–2096 (2018). https://doi.org/10.1109/TIM.2018.2811446
3. Shvetsova, S.V., Alexey, V.: Safety analysis of goods transportation by unmanned aerial vehicles. World Transp. Transp. **17**(5), 286–297 (2020). https://doi.org/10.30932/1992-3252-2019-17-5-286-297
4. Sciancalepore, S., Ibrahim, O., Oligeri, G., Pietro, R.D.: Picking a needle in a Haystack: detecting drones via network traffic analysis. arXiv: 1901.03535v1 [cs.CR] (2019). https://www.researchgate.net/publication/33035767
5. Khan, N.A., Jhanjhi, N.Z., Brohi, S.N., Usmani, R.S.A., Nayyar, A.: Smart traffic monitoring system using unmanned aerial vehicles (UAVs). Comput. Commun. (2020)
6. Khan, N.A., Jhanjhi, N.Z., Brohi, S.N., Nayyar, A.: Emerging Use of UAV's: Secure Communication Protocol Issues and Challenges. Elsevier (2020)
7. Guntur, S.R., Gorrepati, R.R., Dirisala, V.R.: Internet of medical things remote healthcare and health monitoring perspective. Medical Big Data and Internet of Medical Things: Advances, Challenges, and Applications, chap. 11. CRC Press Taylor & Francis Group, Boca Raton (2018)
8. Guntur, S.R., Gorrepati, R.R., Dirisala, V.R.: Robotics in healthcare: an Internet of Medical Robotic Things (IoMRT) perspective. Machine Learning in Biosignal Analysis and Diagnosis Imaging, chap. 12. Elsevier, Amsterdam (2019)
9. Nayyar, A., Bao-Le, N., Nguyen, N.G.: The Internet of Drone Things (IoDT): future envision of smart drones. In: First International Conference on Sustainable Technologies for Computational Intelligence. Advances in Intelligent Systems. Springer (2020). https://doi.org/10.1007/978-981-15-0029-9_45
10. Caparra, G., Ceccato, S., Formaggio, F., Laurenti, N., Tomasin, S.: Low power selective denial of service attacks against GNSS. In: Proceedings of the 31st International Technical Meeting of

the Satellite Division of the Institute of Navigation (ION GNSS + 2018). Institute of Navigation (2018). https://doi.org/10.33012/2018.15909
11. Wang, Q., Nguyen, T., Khanh, P., Kwon, H.: Mitigating jamming attack: a game-theoretic perspective. IEEE Trans. Veh. Technol. **67**(7), 6063–6074 (2018)
12. Jameel, F., Wyne, S., Kaddoum, G., Duong, T.Q.: A comprehensive survey on cooperative relaying and jamming strategies for physical layer security. IEEE Commun. Surv. Tutor. **21**, 2734–2771 (2018)
13. Perez Marcos, E., Caizzone, S., Konovaltsev, A., Cuntz, M., Elmarissi, W., Yinusa, K., Meurer, M.: Interference awareness and characterization for GNSS maritime applications. In: 2018 IEEE/ION Position, Location and Navigation Symposium (PLANS), pp. 908–919 (2018)
14. Shi, X., Yang, C., Weige, X., Chen, J.: Anti-drone system with multiple surveillance technologies: architecture, implementation, and challenges. IEEE Commun. Mag. (2018). https://doi.org/10.1109/MCOM.2018.1700430
15. Son, Y., Noh, J., Choi, J., Kim, Y.: Gyrosfinger: fingerprinting drones for location tracking based on the outputs of MEMS gyroscopes. ACM Trans. Priv. Secur. **21**(2), 10:1–10:25 (2018)
16. Sanjab, A., Saad, W., Baskar, T.: Prospect theory for enhanced cyber-physical security of drone delivery systems: a network interdiction game. arXiv preprint arXiv:1702.04240 (2018)
17. Khan, M.A., Alvi, B.A., Safi, E.A., Khan, I.U.: Drones for good in smart cities: a review. In: International Conference on Electrical, Electronics, Computers, Communication, Mechanical and Computing (EECCMC) 28 & 29 Jan 2018. https://www.researchgate.net/publication/31684633
18. Mabodi, K., Mehadi, Y., Zandiyan, S.: Multi-level trust-based intelligence schema for securing of the internet of things (IoT) against security threats using cryptographic authentication. J. Supercomput. (2020). https://doi.org/10.1007/s11227-019-03137-5
19. Fotohi, R.: Securing of unmanned aerial systems (UAS) against security threats using the human immune system. Reliab. Eng. Syst. Saf. **193**, 106675 (2020)
20. Qin, T., Wang, B., Chen, R., Qin, Z.: Wang L IMLADS: intelligent maintenance and lightweight anomaly detection system for internet of things. Sensors **19**(4), 958 (2019)
21. Zhang, J., Rajendran, S., Sun, Z., Woods, R., Hanzo, L.: Physical layer security for the internet of things: authentication and key generation. IEEE Wirel. Commun. **26**(5), 92–98 (2019). https://doi.org/10.1109/mwc.2019.1800455
22. Carrio, A., Sampedro, C., Rodriguez-Ramos, A., Campoy, P.: A review of deep learning methods and applications for unmanned aerial vehicles. J. Sens. **2017** (2017)
23. Fotouhi, A., Ding, M., Hassan, M.: Understanding autonomous drone maneuverability for the internet of things applications. In: 2017 IEEE 18th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), pp. 1–6 (2017)
24. Motlagh, N.H., Bagaa, M., Taleb, T.: UAV-based IoT platform: a crowd surveillance use case. IEEE Commun. Mag. **55**, 128–134 (2017)
25. Kersnovski, T., Gonzalez, F., Morton, K.: A UAV system for autonomous target detection and gas sensing. In: Proceedings of the Aerospace Conference, Big Sky, MT, USA, pp. 1–12 (2017)
26. Kumbhar, A., Guvenc, I., Singh, S., Tuncer, A.: Exploiting LTE-advanced HetNets and FeICIC for UAV-assisted public safety communications. IEEE Access **6**, 783–796 (2018)
27. Butun, I., Österberg, P., Song, H.: Security of the internet of things: vulnerabilities, attacks, and countermeasures. IEEE Commun. Surv. Tutor. (2019). https://doi.org/10.1109/COMST.2019.2953364
28. Eldosouky, A., Ferdowsi, A., Saad, W.: Drones in distress: a game-theoretic countermeasure for protecting UAVs against GPS spoofing. arXiv:1904.11568v1 [cs.SY] 16 (2019). https://www.researchgate.net/publication/332726565
29. Jansen, K., Schafer, M., Moser, D., Lenders, V., Popper, C., Schmitt, J.: Crowd-GPS-Sec: leveraging crowdsourcing to detect and localize GPS spoofing attacks. In: IEEE Symposium on Security and Privacy (SP), San Francisco, CA, pp. 1018–1031 (2018)
30. French, A., Mohammad, M., Eldosouky, A., Saad, W.: Environment-Aware Deployment of Wireless Drones Base Stations with Google Earth Simulator (2018). https://www.researchgate.net/publication/325414049

31. Mozaffari, M., Saad, W., Bennis, M., Nam, Y.-H., Debbah, M.: A Tutorial on UAVs for Wireless Networks: Applications, Challenges, and Open Problems (2018)
32. Mozaffari, M., Kasgari, A.T.Z., Saad, W., Bennis, M., Debbah, M.: Beyond 5G with UAVs: foundations of a 3D wireless cellular network. IEEE Trans. Wirel. Commun. **18**(1), 357–372 (2019)
33. Mozaffari, M., Saad, W., Bennis, M., Debbah, M.: Wireless communication using unmanned aerial vehicles (UAVs): optimal transport theory for hover time optimization. IEEE Trans. Wirel. Commun. **16**(12), 8052–8066 (2017)
34. Zhang, A., Liu, X., Gros, A., Tiecke, T.: Building detection from satellite images on a global scale (2017)
35. Granjal, J., Monteiro, E., Silva, J.S.: Security for the internet of things: a survey of existing protocols and open research issues. IEEE Commun. Surv. Tutor. **17**, 1294–1312 (2015)
36. Caparra, G., Ceccato, S., Formaggio, F., Laurenti, N., Tomasin, S.: Low power selective denial of service attacks against GNSS. In: Proceedings of the 31st International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS + 2018). Institute of Navigation (2018)
37. Pietro, R., Oligeri, G., Tedeschi, P.: JAM-ME: exploiting jamming to accomplish drone mission. In: IEEE Conference on Communications and Network Security (CNS) (2019)
38. Tedeschi, P., Oligeri, G., Pietro, R.: Leveraging jamming to help drones complete their mission. IEEE Access **4**, 1–16 (2016)
39. Zhang, Q., Mohammad, M., Saad, W.: Machine Learning for Predictive On-Demand Deployment of UAVs for Wireless Communications. arXiv:1805.00061v1 [eess.SP] (2018)
40. Mohammad, M.: Performance optimization for UAV-enabled wireless communications under flight time constraints. In: IEEE Global Communications Conference (GLOBECOM) (2018)
41. Zeng, Y., Zhang, R.: Energy-efficient UAV communication with trajectory optimization. IEEE Trans. Wirel. Commun. **16**(6), 3747–3760 (2017)