People's Democratic Republic of Algeria
Ministry of Higher Education and Scientific Research
University of 8 Mai 1945Guelma

Faculty of mathematics, computer science and sciences of matter
Department of computer science
Domiciliation laboratory of Information and Communication Sciences and Technologies

Thesis

Submitted in Candidacy for the Degree of *Doctorate in Third Cycle*

Field: Computer Science Stream: Mathematics and Computer Science
Speciality: Information and Communication Sciences and Technologies

Presented by:
Mabrek Zahia

Title

IoT Network Dynamic Clustering and Communication for Surveillance UAV's

Defended on : 30/05/2024 Before the jury composed of:

Full name	Rank	University		
Mr Nemissi Mohamed	Professor	Univ. of 8 May 1945,	Guelma	President
Mr Farou Brahim	Professor	Univ. of 8 May 1945,	Guelma	Supervisor
Mr Kouahla Zineddine	Professor	Univ. of 8 May 1945,	Guelma	Co- supervisor
Mr Farah Nadir	Professor	Univ. of Badji Mokhtar,	Annaba	Examiner
Mr Halimi Khaled	MCA	Univ. of 8 May 1945,	Guelma	Examiner
Mr Seridi Hamid	Professor	Univ. of 8 May 1945,	Guelma	Invited

Academic year: 2023/2024

Acknowledgements

First and foremost, I would like to thank God for giving me the strength, knowledge, ability, and opportunity to undertake this research study and to persevere and complete it satisfactorily.

I am immensely grateful to my thesis director, Professor Brahim FAROU, for the outstanding guidance throughout my graduate study. Your invaluable advice over the past four years has not only aided in shaping my future research career but has also instilled in me the confidence to trust in my capabilities. Your mentorship has been a cornerstone of my development as a postgraduate student, and for that, I am eternally thankful.

My sincere appreciation extends to my co-director, Professor Zineddine KOUAHLA, whose support, encouragement, and insightful feedback have been instrumental over the years. Your keen observations and relevant remarks have profoundly impacted my research journey, and I am deeply thankful for your guidance.

I am also indebted to Professor Hamid SERIDI, our esteemed laboratory director, for his unwavering support, encouragement, and invaluable guidance. Your recognition of my efforts and detailed feedback have been crucial to my growth and development within the academic community. It is with heartfelt gratitude that I acknowledge your contributions to my journey.

A special thanks goes to Professor Mohamed NEMISSI, Professor Nadir FARAH, and Doctor Khaled HALIMI for their acceptance of the examination of this work.

I wish to express my gratitude to all the teachers of the Computer Science department at the 8 Mai 1945 Guelma university for their high-quality education. Additionally, my appreciation goes out to the LabSTIC laboratory teams and the laboratory engineer, Miss Madiha KHAROUBI, whose collective efforts and individual contributions have significantly enriched my research experience.

To everyone who has supported me directly or indirectly during this journey, I extend my deepest thanks. Your contributions have not only facilitated this work but have also paved the way for future endeavors.

Abstract

The work presented in this Ph.D. thesis addresses the challenges faced by drones in the Internet of Things (IoT) environment, with a particular focus on the development of communication protocols in a dynamic fog computing (DFC) system. As mobile devices, drones face many challenges, including loss of connectivity, data redundancy due to multiple sensors, and the complexity of collaborative missions. These challenges have the potential to reduce mission effectiveness, increase costs and lead to mission failure and equipment loss. In order to address these concerns, we would like to suggest three communication and monitoring protocols that can enhance the efficiency of drone operations. Additionally, we propose a DFC overload mechanism. The first protocol introduces a new drone recovery system that addresses the limitations of existing systems that only recover drones after a crash. In order to strengthen security, a new authentication mechanism restricts device connections to fog nodes, preventing unauthorized access. The protocol consists of two phases, during the initial phase, the system detects connection attempts and establishes a link through an intermediary. The second phase involves the deployment of additional drones to recover the lost drone using an ad-hoc network. The second protocol addresses the issue of data redundancy in drone data collection within a collaborative drone system. A novel data acquisition algorithm has been developed that divides the fog region into smaller sections using mathematical definitions. The algorithm takes into account data collection factors and employs a shot-by-shot capture approach to minimize redundancy, optimize bandwidth utilization, and reduce network congestion. Collaboration with other drones is crucial for detecting multiple suspects effectively during a mission. Our research has identified a gap in existing collaborative systems regarding the detection of multiple suspects with a single drone. However, our third protocol significantly enhances the effectiveness of drone missions by facilitating cooperation between drones and selecting appropriate assisting drones for the tracking process. This protocol has been thoroughly tested and has proven to be successful in improving the accuracy and efficiency of drone missions. In situations where a drone detects multiple suspects, pertinent information is transmitted to the base station. The base station then coordinates tracking missions with another drone to pursue additional targets, while also taking into account the potential impact on other operations. Additionally, a new (DFC)-based mechanism is proposed to intelligently manage fog node states during saturation. Through a lightweight transition protocol, DFC dynamically monitors fog node capacity and adjusts their states, enabling real-time decision-making to address challenges posed by diverse traffic scenarios. This approach showcases competence and expertise in addressing complex traffic scenarios. The

results obtained demonstrate the effectiveness of proposed methods in terms of communication, computing latency and resource utilization compared to the conventional systems.
Key-words: Internet of Things, Dynamic Fog Computing, Fog Overload, Drone recovery, Multi-target tracking, Minimize redundancy.

Résumé

Les travaux présentés dans cette thèse de doctorat portent sur les défis auxquels sont confrontés les drones dans l'environnement de l'Internet des objets (IdO), avec un accent particulier sur le développement de protocoles de communication dans un système d'informatique dynamique dans le brouillard (DFC). En tant qu'appareils mobiles, les drones sont confrontés à de nombreux défis, notamment la perte de connectivité, la redondance des données due à la multiplicité des capteurs et la complexité des missions collaboratives. Ces défis peuvent réduire l'efficacité des missions, augmenter les coûts et conduire à l'échec des missions et à la perte d'équipements. Afin de répondre à ces préoccupations, nous aimerions suggérer trois protocoles de communication et de surveillance qui peuvent améliorer l'efficacité des opérations des drones. En outre, nous proposons un mécanisme de surcharge DFC. Le premier protocole introduit un nouveau système de récupération des drones qui répond aux limites des systèmes existants qui ne récupèrent les drones qu'après un accident. Afin de renforcer la sécurité, un nouveau mécanisme d'authentification limite les connexions des appareils aux nœuds de brouillard, empêchant ainsi tout accès non autorisé. Le protocole se compose de deux phases : au cours de la phase initiale, le système détecte les tentatives de connexion et établit un lien par le biais d'un intermédiaire. La seconde phase implique le déploiement de drones supplémentaires pour récupérer le drone perdu à l'aide d'un réseau ad hoc. Le second protocole aborde la question de la redondance des données dans la collecte de données par drone au sein d'un système de drone collaboratif. Un nouvel algorithme d'acquisition de données a été développé pour diviser la région de brouillard en sections plus petites à l'aide de définitions mathématiques. L'algorithme tient compte des facteurs de collecte des données et utilise une approche de capture plan par plan pour minimiser la redondance, optimiser l'utilisation de la bande passante et réduire l'encombrement du réseau. La collaboration avec d'autres drones est essentielle pour détecter efficacement plusieurs suspects au cours d'une mission. Notre recherche a identifié une lacune dans les systèmes collaboratifs existants en ce qui concerne la détection de plusieurs suspects avec un seul drone. Cependant, notre troisième protocole améliore considérablement l'efficacité des missions de drones en facilitant la coopération entre les drones et en sélectionnant les drones d'assistance appropriés pour le processus de suivi. Ce protocole a été testé de manière approfondie et s'est avéré efficace pour améliorer la précision et l'efficacité des missions des drones. Lorsqu'un drone détecte plusieurs suspects, les informations pertinentes sont transmises à la station de base. La station de base coordonne alors les missions de repérage avec un autre drone afin de poursuivre d'autres cibles, tout en tenant compte de l'impact potentiel sur d'autres opérations. En outre, un nouveau mécanisme basé sur le DFC est

proposé pour gérer intelligemment les états des nœuds de brouillard pendant la saturation. Grâce à un protocole de transition léger, le DFC surveille dynamiquement la capacité des nœuds de brouillard et ajuste leur état, ce qui permet de prendre des décisions en temps réel pour relever les défis posés par divers scénarios de trafic. Cette approche met en évidence la compétence et l'expertise dans le traitement de scénarios de trafic complexes. Les résultats obtenus démontrent l'efficacité des méthodes proposées en termes de communication, de latence informatique et d'utilisation des ressources par rapport aux systèmes conventionnels.

Mots-clés: Internet des objets, Calcul en Brouillard Dynamique, Sursaturation du brouillard, Perte de données, Saturation de la capacité, Récupération de drone, Drone perdu, Suivi multi-cibles, Minimiser la redondance.

ملخص

يتناول العمل المقدم في أطروحة الدكتوراه هذه التحديات التي تواجهها الطائرات بدون طيار في بيئة إنترنت الأشياء، مع التركيز بشكل خاص على تطوير بروتوكولات الاتصال في نظام حوسبة الضباب الديناميكي . وباعتبارها أجهزة متنقلة، تواجه الطائرات بدون طيار العديد من التحديات، بما في ذلك فقدان الاتصال، وتكرار البيانات بسبب أجهزة الاستشعار المتعددة، وتعقيد المهام التعاونية. هذه التحديات لديها القدرة على تقليل فعالية المهمة، وزيادة التكاليف، وتؤدي إلى فشل المهمة وفقدان المعدات. من أجل معالجة هذه المخاوف، نود أن نقترح ثلاثة بروتوكولات للاتصال والمراقبة يمكن أن تعزز كفاءة عمليات الطائرات بدون طيار. وبالإضافة إلى ذلك، نقترح آلية للحمل الزائد للطائرات بدون طيار.

يقدم البروتوكول الأول نظاماً جديداً لاستعادة الطائرات بدون طيار يعالج قيود الأنظمة الحالية التي لا تستعيد الطائرات بدون طيار إلا بعد تعطلها. ومن أجل تعزيز الأمان، تعمل آلية مصادقة جديدة على تقييد اتصالات الأجهزة بعُقد الضباب، مما يمنع الوصول غير المصرح به. يتكون البروتوكول من مرحلتين، خلال المرحلة الأولى، يكتشف النظام محاولات الاتصال وينشئ رابطاً من خلال وسيط. تتضمن المرحلة الثانية نشر طائرات بدون طيار إضافية لاستعادة الطائرة بدون طيار المفقودة باستخدام شبكة مخصصة. يعالج البروتوكول الثاني مشكلة تكرار البيانات في جمع بيانات الطائرات بدون طيار ضمن نظام تعاوني للطائرات بدون طيار. تم تطوير خوارزمية جديدة لجمع البيانات تقسم منطقة الضباب إلى أقسام أصغر باستخدام تعريفات رياضية. وتأخذ الخوارزمية في الاعتبار عوامل جمع البيانات وتستخدم نهج التقاط كل لقطة على حدة لتقليل التكرار وتحسين استخدام النطاق الترددي وتقليل ازدحام الشبكة. يعد التعاون مع الطائرات بدون طيار الأخرى أمراً بالغ الأهمية للكشف عن عدة مشتبه بهم بفعالية أثناء المهمة. وقد حدد بحثنا وجود فجوة في الأنظمة التعاونية الحالية فيما يتعلق بالكشف عن عدة مشتبه بهم بطائرة واحدة بدون طيار. ومع ذلك، فإن بروتوكولنا الثالث يعزز بشكل كبير من فعالية مهام الطائرات بدون طيار من خلال تسهيل التعاون بين الطائرات بدون طيار واختيار الطائرات المساعدة المناسبة لعملية التتبع. وقد تم اختبار هذا البروتوكول بدقة وأثبت نجاحه في تحسين دقة وكفاءة مهام الطائرات بدون طيار. في الحالات التي تكتشف فيها طائرة بدون طيار عدة مشتبه بهم، يتم إرسال المعلومات ذات الصلة إلى المحطة الأساسية. تقوم المحطة الأساسية بعد ذلك بتنسيق مهام التعقب مع طائرة أخرى بدون طيار لملاحقة أهداف إضافية، مع مراعاة التأثير المحتمل على العمليات الأخرى.

بالإضافة إلى ذلك، تم اقتراح آلية جديدة قائمة على لإدارة حالات عقدة الضباب بذكاء أثناء التشبع. ومن خلال بروتوكول انتقالي خفيف الوزن، تراقب آلية قدرة عقدة الضباب بشكل ديناميكي وتعدّل حالاتها، مما يتيح اتخاذ القرارات في الوقت الحقيقي لمواجهة التحديات التي تفرضها سيناريوهات حركة المرور المتنوعة. يُظهر هذا النهج الكفاءة والخبرة في معالجة سيناريوهات حركة المرور المعقدة. تُظهر النتائج التي تم الحصول عليها فعالية الأساليب

المقترحة من حيث الاتصال والكمون الحاسوبي واستخدام الموارد مقارنةً بالأنظمة التقليدية.
الكلمات الرئيسية: انترنت الأشياء، الحوسبة الضبابية الديناميكية، تحميل الضباب، فقدان البيانات، تشبع السعة

Acronyms

IoT Internet of Things

DFC Dynamic Fog Computing

UAV Unmanned Aerial Vehicle

FSR Force Sensing Resistor

MR Magneto Resistive

IPv6 Internet Protocol Version 6

BLE Bluetooth Low Energy

NFC Near Field Communication

LPWAN Low Power Wide Area Network

NB-IoT Narrowband Internet of Things

IaaS infrastructure-as-a-service

PaaS platform-as-a service

SaaS software-as-a-service

CoT Cloud of Things

IoE Internet of Everything

SoA Service-oriented Architectures

RPV Remotely Piloted Vehicle

UVS Unmanned Vehicle Systems

ROA Remotely Operated Aircraft

NSMV Near Space Maneuvering Vehicle

HMMWV High Mobility Multipurpose Wheeled Vehicle

STOL short take-off and landing

MAVs Micro Air Vehicles

NAVs Nano Air Vehicles

PAVs pico air vehicles

SAR Search and Rescue

MILP Mixed-Integer Linear Programming

ITS Intelligent Transportation Systems

V2I Vehicle to Infrastructure

VANET Vehicular Ad hoc NeTworking

NDN Named Data Networking

ISTAR Intelligence, Surveillance, Target Acquisition, and Reconnaissance

UCAV Unmanned Combat Aerial Vehicles

Contents

List of Figures

List of Tables

Introduction

General context and issues

Unmanned Aerial Vehicles (UAVs), also known as drones, have become increasingly popular in IoT applications. They offer a wide range of benefits, including enhancing public safety, responding quickly to emergencies, managing disasters, and performing daily tasks such as surveillance and tracking of suspicious objects. Their mobility and rapid tracking abilities allow them to move seamlessly across locations, navigate challenging areas, and provide precise information on critical situations or the extent of a threat in various scenarios. To optimize speed and operational efficiency, it is important to maintain a compact and lightweight design. This can be challenging as it limits the number and functionality of components used. In such a situation, it's important to prioritize reliable connectivity, robust protection, and swift real-time data transmission, given the drone's limited storage and processing capabilities. Integrating drones into the Fog Computing framework presents challenges due to the potential disruption of their continuous communication with ground stations caused by factors such as wind and the inherent movement of drones. Communication breakdowns can critically hamper drone operations, preventing the reception of guidelines from the base station and inhibiting the transmission of position data. As a result, drones may become disoriented, potentially losing valuable mission-collected information. There have been instances of drones falling unexpectedly due to connection re-establishment failures. Furthermore, the architecture of the IoT tree has been specifically designed to ensure secure device communication with fog or edge nodes. It is important to note, however, that this can present a challenge when a drone moves beyond the range of its parent fog node, as it may be unable to connect with another fog node. In the other hand, in high traffic situations, fog nodes may become overloaded, leading to critical issues due to limited resources. This overload can directly impact both computing and network latency, compromising the efficiency and responsiveness of the entire IoT system. Despite extensive research on the conceptual and theoretical foundations of fog computing, there exists a gap in effectively addressing real-time overloading issues without compromising data integrity or the overall performance of the system.

New communication, authentication, and collaboration mechanisms are necessary to integrate drones into an IoT environment. Adapting the fog computing system to control and coordinate the overload of fog nodes in real-time is essential in sensitive and high-traffic situations, which is the main focus of this thesis.

Objectives

This thesis confidently presents the design of an intelligent surveillance drone mechanism that is both efficient and novel within a dynamic fog computing environment. The system confidently addresses the central problem.

"How to integrate autonomous surveillance drones in dynamic fog computing system."

Tracking a set of targets in real-time, with minimal cost and high quality, is indispensable in large-scale surveillance drones in IoT Dynamic Fog-based environment. However, coordinating multiple drones to track these targets with these constraints is not impossible. With careful planning and execution, it can be achieved. This is mainly due to the following practical questions:

Recovery of lost drones Losing connection with a drone while on a mission can be a frustrating and hazardous situation, particularly if the drone is being used for an important task such as search and rescue or surveillance.

Flexible and adaptive collaboration: A collaborative drone surveillance system is necessary following the existence of multi-target capture from cameras. To achieve this goal, a versatile algorithm for mission management is essential.

Achieve a stable latency: The constrained resources of fog nodes render them vulnerable to overloading or crashes, affecting both capacity and service quality, particularly in times of high traffic. Moreover, the involvement of a third-party manager introduces challenges related to communication and computing latency.

Real-time performance: Diminishing the efficacy of predictive overload solutions in addressing real-time decision-making during instances of processing or storage saturation.

Scientific Contributions

First contribution: We have introduced a new drone recovery protocol designed to recover misplaced drones before any potential crashes occur. This protocol is executed in two phases. Initially, it attempts to identify whether there is a connection attempt between the lost drone and an adjacent fog node. If such an attempt is detected, an indirect connection will be established with the responsible fog node until the drone returns within its range. The second phase is activated if the first one proves unsuccessful. In this scenario, the fog node in charge directs available drones to relocate to the last known position and make an effort to recover the lost drone through an ad-hoc network.

Second contribution: This study introduces a Dynamic Fog Computing (DFC)-based mechanism to intelligently manage fog node states during saturation. Our solution primarily focuses on dynamically monitoring fog node capacity and the adjustment of their states to accommodate fluctuations in traffic volumes through a new lightweight transition protocol. This enables effective real-time decision-making to address challenges posed by diverse traffic scenarios. The protocol introduces two modes: the "Default Mode" for standard fog node operations, including receiving, storing, and processing tasks, and the "Relay Mode" strategically activated during overload, temporarily suspending the processing and storage of incoming tasks.

Third contribution: We have proposed novel solution that involves dividing the fog area into smaller parts and optimizing data distribution among drones. We have introduced the concepts of fog area division, data distribution factors, and shot-by-shot capture approach. By implementing these techniques, we aim to minimize redundancy, optimize bandwidth utilization, reduce network congestion, and lower costs in IoT-based drone networks.

Fourth contribution: This contribution introduces a novel collaborative algorithm designed to enhance multi-target surveillance and tracking in such environments. The algorithm fosters cooperation among drones by dynamically selecting suitable assisting drones to engage in the tracking process. When a drone identifies multiple suspects, it transmits relevant information, including positional data and imagery, to the base station. Subsequently, the algorithm orchestrates the assignment of new tracking missions to assisting drones, enabling them to effectively follow the additional targets.

Thesis Roadmap

The thesis is confidently divided into two main parts, The first section comprises three state-of-the-art chapters, while the second section includes four contribution chapters and concludes with a decisive general conclusion.

Part I: Backgrounds, Preliminaries and Basic Concepts

- *Chapter 01: Internet Of Things*
  This chapter presents a comprehensive overview of the emerging modern computing paradigms in the IoT, including their relevant concepts, definitions, and technologies. The operating principles and current and future applications of IoT technology are thoroughly reviewed. The functional principles of these paradigms are clearly identified, and their similarities and differences are confidently highlighted.
- Chapter 02: Unmanned Aerial Vehicles(UAVs)
  This chapter offering a comprehensive overview of drone technology, defining their charac-

teristics and providing an understanding of their various classifications. The chapter also explores the diverse landscape of drone types, considering their performance and mission aspects. Moving beyond technicalities, the applications of drones across different industries are discussed. The narrative also touches upon the challenges inherent in drone technology, such as privacy concerns, airspace management, noise pollution, limited battery life, traffic and obstacle detection, navigation, and communication issues.

Part II: Propositions

- *Chapter 03: Drone Recovery System*
  A new drone recovery protocol is introduced, aimed at preventing potential crashes by efficiently recovering misplaced drones.
- *Chapter 04: Fog Node Overload: Dynamic Solution for Enhanced IoT Efficiency*
  This study introduces a Dynamic Fog Computing (DFC)-based mechanism to intelligently manage fog node states during saturation.
- *Chapter 05: Optimizing Data Transmission in IoT-based Drone Networks through Fog Area Division*
  The proposed solution to enhance the efficiency of IoT-based drone networks involves dividing the fog area into smaller parts and optimizing data distribution among drones using concepts such as fog area division.
- *Chapter 06: Enhanced Multi-Target Surveillance and Tracking Algorithm for Collaborative Drones in IoT Environment*
  This chapter presents a collaborative algorithm designed to improve multi-target surveillance and tracking in drone environments.

Part I

Backgrounds, Preliminaries and Basic Concepts

Chapter 1

Internet Of Things

1.1 Introduction

The IoT empowers entities worldwide to collaborate seamlessly towards achieving daily objectives. It is a paradigm that envisions the seamless connection of all elements. This paradigm goes beyond the conventional notion of smart devices, as every object has the potential to become a device by integrating sensors and connectivity.
The history of the IoT can be traced back to the early 2000s, when the concept was first proposed by Kevin Ashton [16]. Since then, the field has seen significant growth, with a focus on security, wireless sensor networks, management, and privacy [17]. The potential applications of IoT are vast, including precision agriculture, environmental monitoring, smart health, smart manufacturing, and smart cities [18]. However, the rapid development of IoT has also raised concerns about security and privacy [17].
The IoT holds great promise for individuals, homes, companies, and institutions, offering numerous benefits [16]. In essence, the IoT brings together different aspects of our daily lives, from personal computing to surveillance and entertainment, creating a network where devices communicate and collaborate. The continued evolution of the Internet and the rise of wireless communications are contributing to the growing innovation of the IoT, transforming the way we interact with technology [19] [20].

1.2 IoT Definition and Overview

The IoT is an advancing technology that integrates various sensors and objects to enable direct communication without human intervention [21]. This technology has the potential to revolutionize various aspects of human life [22]. The IoT is characterized by its connectivity, active engagement, use of sensors, and artificial intelligence [23]. It has the potential to significantly impact the lives of the elderly and differently abled individuals [24]. However, the implementation of IoT faces serious challenges and issues [22].
"Internet of Things envisions a self-configuring, adaptive, complex network that interconnects 'things' to the Internet through the use of standard communication protocols. Interconnected things have physical or virtual representation in the digital world, sensing and actuation capability, a programmability feature, and are uniquely identifiable. The representation contains information

including the thing's identity, status, location or any other business, social or privately relevant information. The things offer services, with or without human intervention, through the exploitation of unique identification, data capture and communication, and actuation capability. The service is exploited through the use of intelligent interfaces and is made available anywhere anytime, and for anything taking security into consideration." (IEEE-IoT, [25])
"The Internet of things describes the many uses and processes that result from giving a network address to a thing and fitting it with sensors. These conjunctures of sensors, things and networks have become an increasingly important part of internet experiences. When we equip the things around us with sensors and connect them to networks, they gain new capabilities ... we mean a particular ability that things did not have before - such as seeing, speaking to, or tracking people." (Mercedes Bunz & Graham Meikle,[26])

1.3 Key Technologies in IoT

The key technologies in IoT, as identified by [27, 28, 29, 30], include sensor technologies, network communications technology, data aggregation and intelligent technology, cloud computing, 5G networks, and Semantic Web. These technologies are crucial for the development and application of IoT, and have the potential to significantly impact various aspects of human life, industrial development, and science and technology.

1.3.1 Sensor technologies

Sensor technologies, which encompass a wide range of sensing and signal transformation approaches, are critical in various sectors due to their ability to detect and measure physical properties or changes in the environment. [31] highlights the widespread use of portable and lightweight sensors in industries such as consumer electronics, biomedical engineering, and the military. [32] further discusses the strengths and weaknesses of different sensing mechanisms, including microelectromechanical systems (MEMS), optical, mechanical, electrochemical, semiconductor, and biosensing. [33] emphasizes the role of smart sensors in IoT applications, providing a multidisciplinary view of sensor technology and its real-world applications. [32] also emphasizes the importance of key hardware and software features in the design of sensors and sensor systems that enable signal conditioning, data processing, transmission, storage, and display of sensor measurements. Typical sensor technology categories include the following:

- **Temperature sensors:** Are crucial in various industries, with fiber optic sensors offering precise measurements and rapid response in harsh environments [34]. The evolution of temperature sensor technologies has significantly improved accuracy, control, and efficiency in safety-critical systems [35]. Polymer fiber optic interferometer-based sensors have the potential to reduce production costs and simplify installation, making them increasingly

popular in industrial solutions [36]. The development of smart temperature sensors, capable of providing digital outputs and easily interfacing with measurement and control systems, has further enhanced their accuracy and performance [37].

- **Pressure sensors:** Particularly silicon-based ones, have become integral in various industries due to their small size, low cost, and high volume production capabilities [38]. The automotive industry, in particular, has seen a significant impact from these sensors, with a shift towards microelectromechanical (MEMS) technology [39]. The need for smaller, adaptable, and highly accurate pressure sensors has also been emphasized in the aerospace and medical technology sectors [40]. In medical equipment, pressure sensors are used to monitor pressure distribution, particularly in 3D contoured and deformable surfaces [41].
- **Motion sensors:** Research on smartphone sensors, particularly gyroscopes and accelerometers, has revealed both their potential and limitations. [42] found that while these sensors are not reliable for life-critical applications, they can be used for general monitoring. [43] provided an overview of MEMS technology and the mechanical systems underlying these sensors, highlighting their role in motion tracking and indoor navigation. [44] further explored the use of these sensors in physical activity recognition, finding that their combination can improve performance. However, [45] raised concerns about the potential misuse of these sensors for tracking users, suggesting the need for mitigation techniques.
- **Proximity sensors:** Which are widely used in robots, touchscreens, and smartphones, have been the subject of several studies.[46] and [47] both developed dual-mode capacitive proximity sensors for robot applications, with the former focusing on a flexible platform and the latter on a polymer platform. These sensors can detect both proximity and touch, and can switch between the two modes. [48] provided an overview of different types of proximity sensors used in robot systems, including inductive, capacitive, photoelectric, acoustic, and time-of-flight ranging sensors. [49] introduced tactile proximity sensors for close human-robot interactions, which were developed as robot skin and integrated into a robot hand. These sensors are designed to detect proximity and touch, enhancing the robot's ability to interact with its environment.
- **Light sensors:** Are integral to a range of applications, from color monitoring in displays [50] to indoor lighting control [51]. The latter study presents a wireless sensing system that uses a low-power light sensor to measure illuminance levels, while the former proposes a filter-less RGB color sensor for ambient light monitoring. Cameras can also serve as light sensors, as demonstrated by [52] in a prototype system for lighting and shading control. However, the potential for privacy concerns in using cameras for this purpose is noted. [53] further explores the use of ambient light sensors in smart devices, highlighting the potential for unauthorized access to user environment information.
- **Gas sensors:** Play a crucial role in industrial safety and environmental monitoring by

detecting the presence and concentration of various gases in the air [54]. These sensors, particularly those based on unstructured materials, offer high selectivity and can operate at lower temperatures [54]. Solid-state gas sensors, including those based on semiconductor, capacitor, and solid-electrolyte technologies, are compact, robust, and cost-effective, making them suitable for real-time field applications [55]. Gas sensors that utilize membrane diffusion, combined with electrochemical or optical transducers, have been developed for environmental monitoring, offering the potential for real-time and continuous gas concentration measurement. The future of gas sensors lies in the development of multivariable sensors that can detect individual gas components in mixtures, reject interferences, and provide stable responses [56].

- **Image sensors:** A range of applications for image sensors have been explored in the literature. [57] and [58] both discuss the use of image sensors in terrestrial thermal imaging and traffic and vehicle control, respectively. [59] focuses on the application of image sensors in detecting and locating electrical discharges, particularly in high-voltage systems. [60] presents a smart range image sensor designed for sheet of light range imaging, which measures the projection of a light stripe on an object. These studies collectively highlight the diverse and innovative uses of image sensors in various fields.
- **Biometric sensors:** Such as fingerprint scanners and iris recognition systems, are crucial for security and identity verification [61]. However, their implementation raises significant security and privacy concerns. These sensors analyze biological data to establish an individual's identity, and have been successfully deployed in various fields [62]. The range of biometric systems includes handwriting, fingerprints, iris patterns, human faces, and speech [63].
- **Microphones, or sound sensors:** A range of studies have explored the potential of microphone arrays in various applications. [64] introduced multi-sensory microphones for robust speech detection, enhancement, and recognition, particularly in noisy environments. [65] and [66] both demonstrated the advantages of microphone arrays over single microphones in speech recognition, with Parry focusing on spatial sensitivity patterns and Kiyohara on SNR improvement and speech period detection. [67] further expanded on the benefits of microphone arrays, particularly in speech source localization, highlighting their ability to electronically aim and track active talkers while attenuating interference and ambient noise. These studies collectively underscore the potential of microphone arrays in enhancing speech recognition and communication systems.
- **Infrared sensors:** A range of infrared sensors have been developed for various applications, including thermal detection using bolometers, thermocouples, and pyroelectric detectors, as well as photon detection using semiconductor photoconductors and photodiodes [68]. These sensors have been integrated into CMOS technology, enabling their use in smart sensor

systems for applications such as intrusion alarm detection [69]. Infrared thermography, which utilizes the intensity of infrared radiation to measure temperature and conduct non-destructive testing, has also been explored [70]. The emergence of microbolometer technology has further expanded the use of infrared sensors, particularly in automotive safety applications [71].

- **Force sensors:** Such as those developed by [72] and [73], have been applied in a range of industries, including robotics, medicine, and industrial gear. [72] highlights their use in robotic applications, such as grinding, deburring, and assembly, while [73] introduces a new type of force sensor specifically designed for human-robot interaction. [74] further contributes to this field by describing the development of a silicon-based force sensor for robotics and medicine, which is compatible with standard integrated circuit processes. [75] provides an overview of the Force Sensing Resistor (FSR) sensors, which are commonly used in robotic grippers and biomechanical fields, and presents the results of experiments testing the effectiveness of these sensors.
- **Magnetic sensors:** Particularly magnetoresistive (MR) sensors, are widely used in various automobile applications, navigation systems, and compasses due to their ability to detect magnetic fields with high sensitivity and resolution [76, 77]. In navigation systems, these sensors are crucial for determining heading direction, with electronic compasses based on MR sensors capable of resolving rotation to better than 0.1 degree [78]. The Earth's geomagnetic field is a key source of information for these sensors, making them reliable and cost-effective for orientation. Furthermore, in automotive applications, magnetic position sensors play a crucial role in functions such as ignition timing, engine misfire detection, and wheel speed sensing [77].
- **Strain sensors:** A range of innovative strain sensors have been developed for industrial and structural health monitoring applications. [79] introduced a wireless deformation sensor based on an inverted-F antenna, offering a promising method for remote deformation assessment. [80] presented flexible and highly sensitive graphene-based strain sensors, with potential for structural health monitoring due to their high gauge factor and stability. [81] designed a wireless strain sensor network for dynamic strain monitoring, demonstrating its feasibility for large structural applications. These studies collectively highlight the diverse and effective applications of strain sensors in industrial and structural health monitoring.

By supplying real-time data and permitting automation across a range of industries, these sensor technologies work together to foster the development of smart systems, the Internet of Things, and other technical innovations.

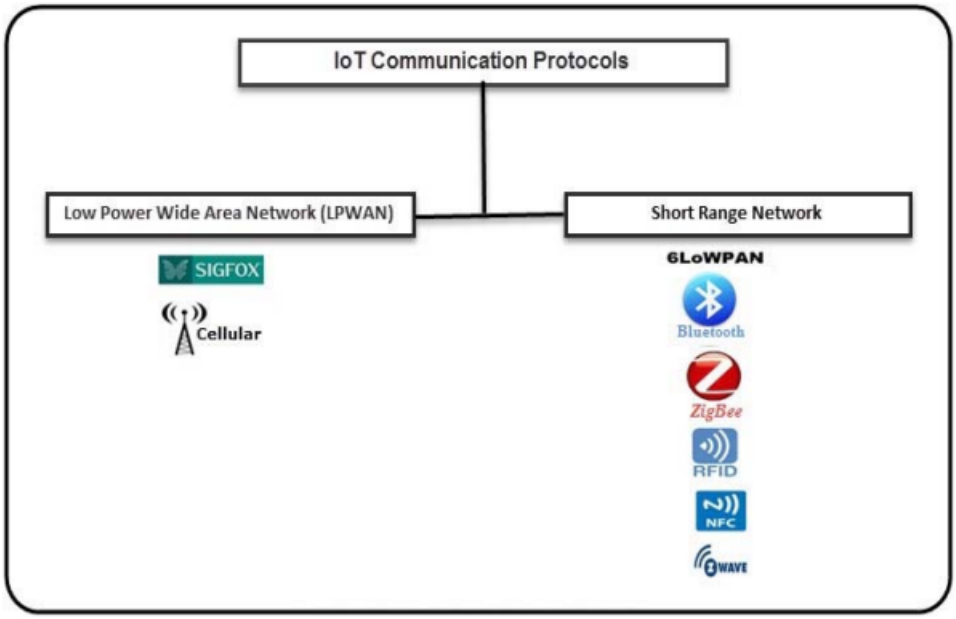

Figure 1.1: IoT communication protocols [1]

1.3.2 Communication protocols

The IoT is a network of smart devices that communicate with each other, enabling data collection and exchange [1]. Various communication protocols are used in IoT Figure 1.1, including IPv6, 6LoWPAN, ZigBee, Bluetooth Low Energy, Z-Wave, NFC, SigFox, and Cellular [1, 82]. These protocols differ in power consumption, security, data rate, and other features [1]. They can be classified based on the OSI model hierarchy, IEEE 802 protocol standard, or network types [83]. The choice of protocol depends on the specific IoT application, considering factors such as communication distance, signal frequency spectrum range, and information security [83, 84].

Wireless Communication Technologies and Protocols

- **Internet Protocol Version 6 (IPv6):** Is a crucial technology for IoT, providing unique addresses to IoT nodes [85]. However, its industrial adoption, particularly in smart manufacturing systems, faces challenges such as incomplete tool support and manual IP communication configuration [86]. Despite these challenges, the adoption of IPv6 is inevitable due to its larger address space and stateless configuration, making it suitable for smart object networks [87]. The potential of IPv6 to support global IoT deployment and integration with legacy systems has been highlighted [88].
- **6LoWPAN (Low power Wireless Personal Area Networks):** A low-power, short-range wireless communication protocol, is a key enabler of IoT applications, particularly in home and building automation [89]. Its implementation on memory-constrained and

power-efficient wireless sensor nodes has been successfully demonstrated, making it suitable for a wide range of IoT devices [90]. The protocol's effectiveness in integrating wireless sensor networks with the IoT has been evaluated, with a focus on header compression and fragmentation of IPv6 datagrams [91]. Its suitability for IoT, given the expected increase in the number of devices and the resulting traffic, has been analyzed, highlighting its support for various features such as addressing, header compression, and network auto-configuration [92].

- **ZigBee:** Is a wireless communication technology known for its low power consumption and suitability for low data rate, short-range communication [93]. It is particularly well-suited for industrial control systems and home automation, where cost-effective, low-power communication is essential [94]. The technology's potential in industrial control applications has been highlighted, with its ability to ensure connection security, real-time communication, and cost reduction [93]. Its use in wireless sensor networks for industrial automation has also been explored, with a focus on its low cost, low power consumption, and low-rate communication capabilities [95]. Furthermore, the ZigBee standard, IEEE 802.15.4, has been discussed, along with its device types, protocol stack architecture, and applications [96].
- **Bluetooth Low Energy (BLE):** Is a low-power wireless technology suitable for short-range communication with low-power devices [97, 98]. It is characterized by a trade-off between energy consumption, latency, piconet size, and throughput, with parameters such as connInterval and connSlaveLatency playing a significant role in its performance [97]. BLE's potential applications include wearable technology, health monitoring, and smart home devices [97, 98]. However, its performance can be affected by implementation constraints [97, 98]. Furthermore, the accuracy and performance of BLE applications, such as indoor positioning and medical monitoring, are influenced by environmental factors and interference [99].
- **Z-Wave:** A wireless communication protocol, is a key player in the field of home automation due to its reliability, low radio rebirth, and easy usage [100]. It enables the creation of a stable network for smart home devices, allowing for remote control of lighting, safety, security, and energy efficiency [101]. However, its security has been called into question, with a vulnerability discovered in AES encrypted Z-Wave door locks [102]. Despite this, efforts are being made to enhance and secure smart homes using Z-Wave technology, with a focus on reliability, scalability, and security.
- **Near Field Communication (NFC):** NFC is a short-range wireless communication technology that enables data transfer between devices in close proximity [103]. It is particularly useful in smartphones, allowing for contact-less transactions and over-the-air ticketing [104]. The technology has the potential to unify various contact-less card standards and could be

used for a range of applications, including payments, ticketing, and access control [105]. The NFC Forum is working to standardize and promote the technology [106].

Low Power Wide Area Network (LPWAN) Protocols

- **SigFox:** A low-power, long-range LPWAN technology, is well-suited for applications with irregular data transmission, such as asset tracking and smart agriculture [107]. It operates at 868 MHz and can send small packages over long distances at very low power [108]. In comparison to LoRa, another leading LPWAN technology. SigFox has been found to have lower collision and packet error rates [109]. The choice between SigFox and LoRa depends on factors such as capacity, interference, co-existence, and link budget [109].
- **Cellular:** The introduction of Narrowband Internet of Things (NB-IoT) in 3GPP Release 13 has significantly enhanced the capabilities of cellular networks for IoT applications [110]. This technology offers wide-area coverage, low device complexity, and long battery life, making it suitable for industrial monitoring and smart city applications [111]. Despite its advantages, NB-IoT deployment can be challenging, particularly in partial deployment scenarios, due to high path loss and interference [111]. However, ongoing enhancements in LTE Rel-14 are expected to address these issues [111]. In comparison to other LPWAN technologies, NB-IoT stands out for its quality of service and latency [112].

Selection of communication technologies and protocols

The selection of communication protocols and technologies in IoT environments is a critical aspect that impacts the design and performance of IoT applications. A range of standard system protocols, including Bluetooth LE, 3GPP, LTE, 6LoWPAN, ZigBee, and IEEE 802.15.4, are available for this purpose [113]. These protocols can be compared based on metrics such as power consumption, security, data rate, and other features [1]. The selection process can be guided by a three-dimensional design space that considers duty cycle, device to gateway distance, and battery life [114]. The continuous evolution of these technologies and the need for innovation further complicate the decision-making process [114]. Despite these challenges, the seamless interconnection of devices to the Internet offered by IoT networks presents significant potential for expanding device functionalities and improving situational control [115]. The communication flow between the different layers of the IOT is shown in (Figure 1.2).

1.3.3 Cloud computing

The idea of cloud computing was established by internet service providers to enable the best possible support for large numbers of customers and scalable services with the least amount of resources. Cloud computing has become a cutting-edge technology in a comparatively short

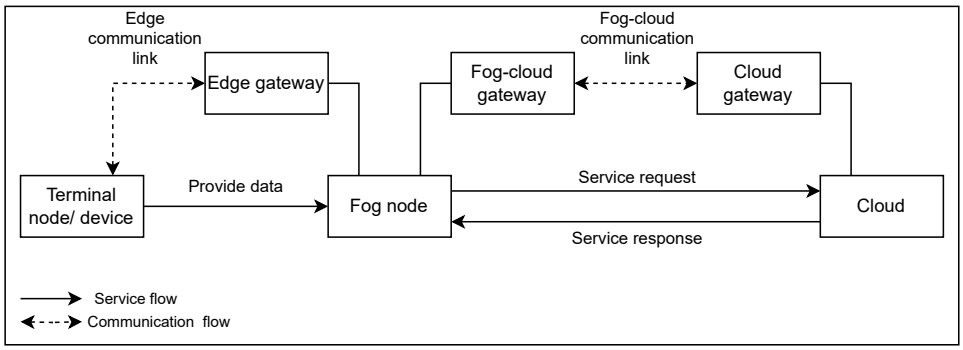

Figure 1.2: Iot Communication flow

amount of time. From Google's groundbreaking papers published in 2003 to Amazon EC2's commercial debut in 2006 and the subsequent arrival of services like AT&T Synaptic Hosting, cloud computing has evolved from an internal IT system to a public utility. It has changed from being only a tool for cutting costs to bringing in money, and from being connected to internet service providers to being essential to the telecom industry [116].

Cloud computing Definition and overview

Cloud computing, based on grid computing, offers a new computing model with key techniques like data storage, management, and programming models and has broad development prospects [117]. Furthermore, cloud computing enables convenient, on-demand access to a shared pool of configurable computing resources, promoting availability and promoting five essential characteristics, three service models, and four deployment models [118]. Moreover, scientific cloud computing offers reliable, customized, and QoS-guaranteed computing environments for end-users, with potential applications in data centers. (Figure 1.3) shows the architecture of cloud computing.

Cloud computing characteristics

loud computing services encompass five key characteristics that define their functionality and appeal:

- **On-Demand Self-Service:** Users have the autonomy to independently acquire computing resources such as server time and network storage as needed, with minimal or no interaction with service providers [118].
- **Broad Network Access:** These services are accessible over diverse networks, such as the Internet, and can be utilized by various client applications deployed on different platforms, including mobile phones, laptops, and PDAs [118].
- **Resource Pooling:** Cloud service providers consolidate their computing resources to efficiently serve multiple consumers. This consolidation is achieved through either a multi-

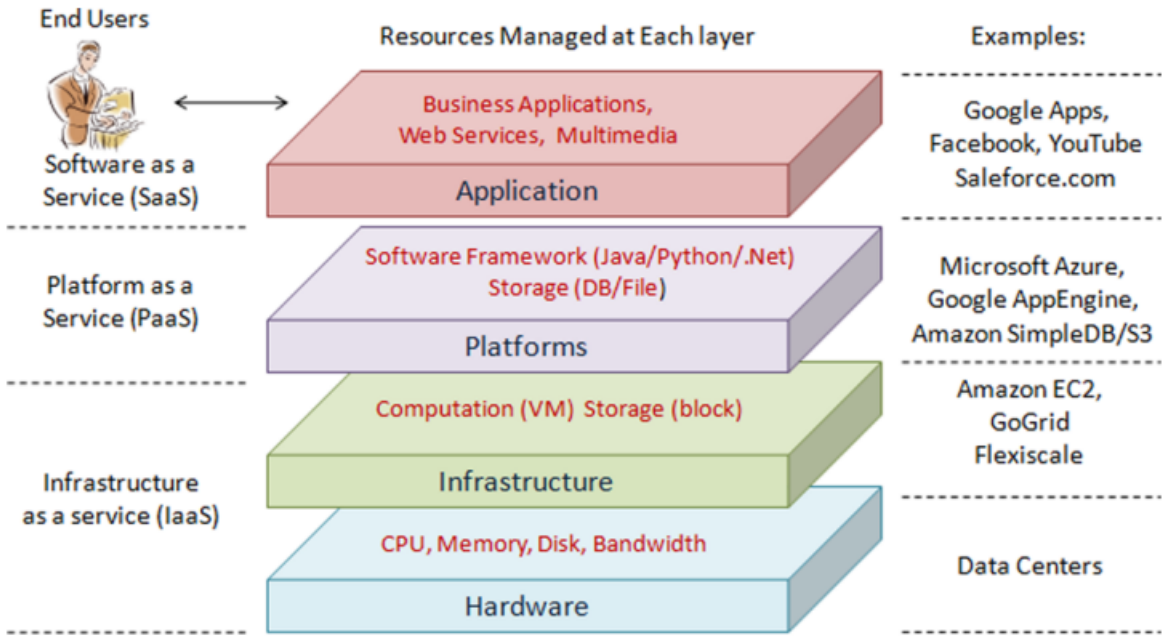

Figure 1.3: Cloud computing architecture [2]

tenancy or virtualization model, dynamically allocating and reallocating resources based on consumer demands [118].

- **Rapid Elasticity:** Cloud services can quickly adapt to changing demands by elastically provisioning and releasing resources. This flexibility provides consumers with the perception of unlimited capacity, available in any quantity at any given time [118].
- **Measured Service:** Cloud systems employ automated mechanisms to assess and optimize resource allocation, leveraging measurement capabilities tailored to specific service types (e.g., storage, processing, and bandwidth). This ensures transparent monitoring, control, and reporting of resource usage for both service providers and consumers [118].

Cloud deployment models

- **Public clouds:** Are computing platforms providing scalable and elastic IT capabilities as a service to external customers using Internet technologies [119].
- **Private Cloud:** Is a cloud computing platform within an organization's own infrastructure, offering features like computation, storage, and network resource management [120] with improved security, scalability, and flexibility for enterprise applications and business development [121].
- **Hybrid Cloud:** Is a combination of public and private clouds, integrating resources and services for improved efficiency, security, and flexibility in managing applications and data

[122, 123, 124].

- **Community Cloud:** Is computing model that integrates cloud infrastructures into community networks, allowing a specific group of users with shared interests, goals, and concerns to utilize spare resources and collaborate on services such as security, compliance, and jurisdiction [125, 126].

Cloud service offering models

cloud service offering models include infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS), with various deployment options such as public, private, hybrid, and community clouds [127, 128, 129].

- **IaaS:** Is cloud computing model that provides on-demand IT resources, such as virtual machines, storage, and networking, in a pay-per-use manner [130], reducing maintenance costs and allowing users to manage their infrastructure services[131].
- **PaaS:** Is a cloud-based approach for developing, deploying, and managing applications, providing managed middleware and infrastructure services, and automating the application workflow lifecycle [132, 133, 134].
- **SaaS:** Is on-demand, internet-based software provided by service providers, accessed via a web browser, and often offered on a pay-per-use basis [135].

Cloud computing limitations

cloud computing limitations can be categorized into security and privacy concerns, resource and network constraints, and challenges in managing IoT and mobile devices. Notably:

- Cloud computing limitations include diverse security and privacy issues, lagging defensive solutions, and the need for future research [136]. Security concerns related to managing data, applications, and interactions and addressing efficiency, scalability, and provable security [137].
- Resource constraints on mobile devices that prevent users from performing complex security operations locally [138].
- Data maintainability, network elasticity, IoT management, user privacy, cloud security, uninterrupted data access between different IoTs, and lack of location awareness [139].
- Latency, cloud computing relies on data centers that might be located far away from the IoT devices. This geographical separation can introduce latency, which is critical in applications where real-time processing is essential, such as industrial automation, healthcare monitoring, or autonomous vehicles.

1.3.4 Cloud of things

The growth of smart devices, where virtually everything becomes an intelligent entity, has led to an explosion in the amount of data generated by these interconnected devices. In response to this explosive growth, cloud computing has evolved into what can aptly be called the "Cloud of Things" (CoT). In this paradigm, the traditional role of cloud computing transcends its traditional boundaries and adapts to the evolving landscape where every conceivable object is imbued with intelligent capabilities. The merging of the vast network of smart devices and the vast expanse of cloud computing resources within the CoT framework represents a harmonious synergy, providing the infrastructure necessary to harness, process, and derive actionable insights from the vast amounts of data generated by this interconnected ecosystem of smart entities [140].

1.3.5 Fog computing

Fog computing is an innovative approach that plays a crucial role in improving the performance, efficiency, and security of IoT networks by bringing computation and storage capabilities closer to the edge [141, 142]. This technique addresses key architectural requirements, especially in critical networks where speed and responsiveness are essential. In the realm of IoT applications, fog computing proves particularly advantageous for a variety of tasks. However, despite its potential benefits, complete migration to the cloud is hindered by concerns related to computing latency [143]. This cautious approach recognizes the sensitivity of data and the need for reliable and secure processing, prompting a strategic integration of fog computing to strike a balance between the advantages of cloud services and the imperative to uphold computing and networkng latency in IoT sensitive applications.

Characteristics of fog computing

Fog computing performs computation, communication, and storage tasks on devices located near the user's network edge. Its primary feature is its proximity to end users, representing the fundamental and most notable advantage over traditional computing models [3]. Additionally, the following characteristics and advantages can be outlined:

- Low latency and real time interactions
- Save bandwidth
- Support for mobility
- Geographical distribution and decentralized data analytic
- Heterogeneity
- Interoperability
- Data security and privacy protection
- Low energy consumption

The hierarchical architecture of fog computing

The hierarchical architecture is composed of the following three layers,(Figure 1.4) shows the hierarchical architecture of fog computing [3]:

- Terminal layer: situated near end users and the physical environment in IoT systems, encompasses a variety of devices like sensors, mobile phones, smart vehicles, smart cards, and readers. Notably, although mobile phones and smart vehicles have computing capabilities, they are employed primarily as smart sensing devices in this context. These devices are widely spread geographically and are responsible for detecting feature data from physical objects or events, sending the sensed data to higher layers for further processing and storage [3].
- Fog Layer: Positioned at the network's edge, the fog computing layer comprises numerous fog nodes, which typically include routers, gateways, switchers, access points, base stations, and specific fog servers. These nodes are widely dispersed between end devices and the cloud, such as in cafes, shopping centers, bus terminals, streets, and parks. They may be stationary at fixed locations or mobile on moving carriers. End devices can easily connect with fog nodes to access services, and these nodes possess the ability to compute, transmit, and temporarily store received sensed data. The fog layer is capable of executing real-time analysis and latency-sensitive applications. Additionally, fog nodes are connected to the cloud data center via the IP core network, playing a role in interaction and collaboration with the cloud to leverage more robust computing and storage capabilities [3].
- Cloud layer: In an IoT system comprises high-performance servers and storage devices, delivering diverse application services like smart home, smart transportation, and smart factory. It possesses robust computing and storage capabilities to support extensive computational analysis and the permanent storage of large datasets. Unlike traditional cloud computing, not all computing and storage tasks pass through the cloud; instead, the cloud core modules are efficiently managed and scheduled based on demand-load using control strategies to enhance resource utilization [3].

Fog computing limitations and challenges

Fog computing issues can be categorized into four main areas: security and privacy concerns, performance and Platform, resource challenges, and Energy management. Notably:

- Security and Privacy Issues [144, 145, 146, 147]:
  - Concerns about data security during processing and transmission.
  - Complex authentication and authorization in a distributed environment.
  - Challenges in ensuring data privacy compliance.
- Control and Management [148, 149, 150, 151]:

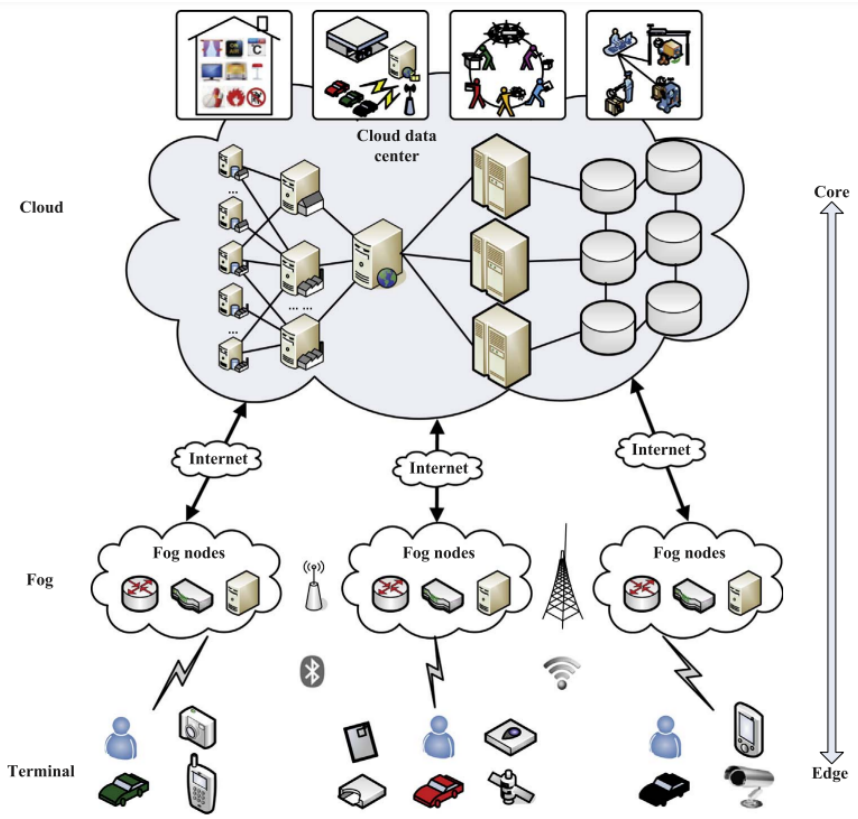

Fig. 1. The hierarchical architecture of fog computing.

Figure 1.4: Fog Computing architecture [3]

  - Difficulty in resource management and optimization across a distributed fog infrastructure. Challenges in Organizing tasks and ensuring scalability. Complexities in coordinating a diverse range of fog nodes.
- Programming Platform [152, 153]:
  - Heterogeneity in hardware and protocols demands adaptable programming frameworks.
  - Increased complexity in application development due to distributed processing.
- Energy Management [154, 155, 156]:
  - Limited power resources in edge devices pose challenges for efficient energy management.
  - Dynamic environments require adaptive strategies to handle changes in energy availability.

Comparison of cloud computing and fog computing

In fact, cloud computing and fog computing represent two distinct paradigms in distributed computing, each with its own unique characteristics and attributes. The Table 1.1 outlines the key differences between cloud computing and fog computing.

	Cloud Computing	**Fog Computing**
Latency	High	Low
Real-time interactions	Supported	Supported
Mobility	Limited	Supported
Location awareness	Partially supported	Supported
Number of server nodes	Few	Large
Geographical distribution	Centralized	Decentralized and distributed
Distance to end devices	Far (multiple network hops)	Near (single network hop or few network hops)
Location of service	Within the Internet	At the edge of the local network
Working environment	Specific data center building with air conditioning systems	Outdoor (streets, base stations, etc.) or indoor (houses, cafes, etc.)
Communication mode	IP network	Wireless communication: WLAN, WiFi, 3G, 4G, ZigBee, etc. or wired communication (part of the IP networks)
Dependence on the quality of core network	Strong	Weak
Bandwidth costs	High	Low
Computation and storage capabilities	Strong	Weak
Energy consumption	High (especially the energy consumption of data center coolant system)	Low

Table 1.1: Comparison of cloud computing and fog computing [2].

1.3.6 Edge computing

With the swift evolution of the Internet of Everything (IoE), there is a rising influx of smart devices connecting to the Internet, leading to the generation of extensive data. This surge in data has given rise to challenges such as increased bandwidth load, sluggish response times, compromised security, and diminished privacy within traditional cloud computing models. Recognizing the inadequacy of traditional cloud computing in meeting the diverse demands of today's intelligent society for data processing, edge computing technologies have surfaced as a viable solution. This novel computing paradigm focuses on executing computations at the network's edge, diverging from cloud computing by prioritizing proximity to users and data sources. At the network's edge, it adopts a lightweight approach, facilitating local, small-scale data storage, and processing. This article predominantly reviews pertinent research and outcomes related to edge computing. It begins by outlining the concept of edge computing, drawing comparisons with

cloud computing. Subsequently, it encapsulates the architecture of edge computing, highlights keyword technologies, addresses security and privacy concerns, and ultimately summarizes the varied applications of edge computing [157].

Comparison of fog computing and edge computing

Fog and edge computing exhibit similarities, but they also have distinct differences. The table (Table 1.2) below highlights key variances between the two.

	Edge Computing	**Fog Computing**
Location of data collection, processing, storage	Network edge, edge devices	Near-edge and core networking, network edge devices and core networking devices
Handling multiple IoT applications	Unsupported	Supported
Resource contention	Serious	Slight
Focus	Things level	Infrastructures level

Table 1.2: Comparison between edge computing and fog computing [2].

1.4 IoT Applications

The Internet of Things has permeated various sectors, revolutionizing how we interact with technology. Several prominent IoT applications have emerged, each with distinct benefits and implications. These diverse IoT applications showcase the technology's adaptability and transformative impact across various domains. As IoT continues to evolve, its applications are likely to expand, offering innovative solutions and enhancing efficiency in numerous facets of our interconnected world (Figure 1.5).

1.4.1 Smart City services

In the realm of urban development, IoT facilitates the creation of smart cities by integrating connected devices and sensors. These devices collect and analyze data to optimize resource management, enhance public services, and improve overall urban living. Examples include smart traffic management, waste management, and efficient energy consumption [158, 159, 160].
This domain has focused on improving the quality of services in smart cities. Services require high levels of privacy and collaboration. however [161] designed the Intelligent Offloading Method (IOM) for smart city services to balance privacy preservation and collaborative service performance. This approach promotes edge utility and efficiency in edge computing. Web-scale service delivery [162] for smart cities improves scalability and extensibility by enabling domain-independent,

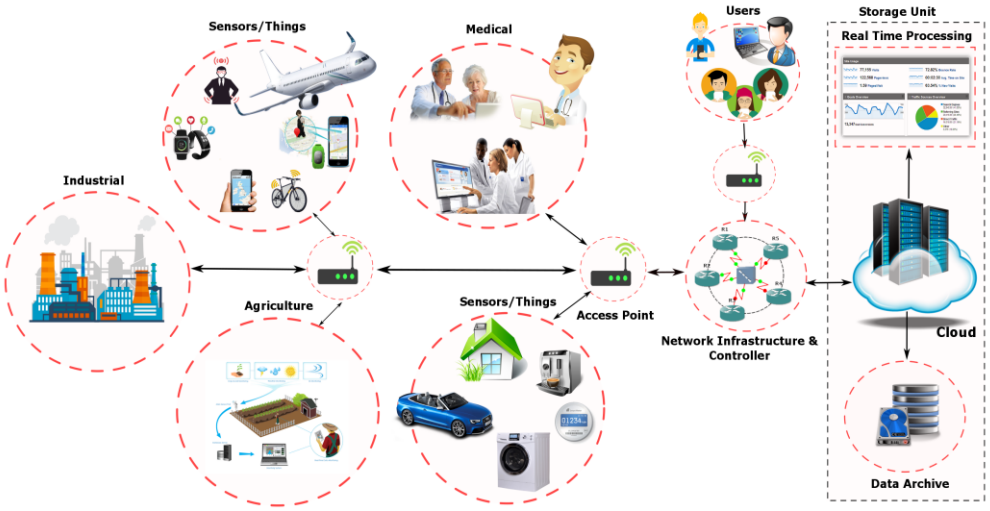

Figure 1.5: IoT applications domain [4]

cloud-based service-delivery platforms.
Smart city services developed using microservices-based [163] architecture, address security and privacy concerns while leveraging IoT data for intelligent management of heterogeneous end systems. Moreover, smart city services necessitate robust information platforms.The proposed information-centric platform [164] effectively supports Smart City ICT services, enhancing e-government, public administration, and safety applications. Additionally, [165] proposes an IoT-based framework for smart city services, addressing the challenges of internet connectivity, data collection, and processing across heterogeneous technologies.
The Smart City Service System, an ontology-based system developed by [166], can improve and optimize city services by utilizing citizen information and supporting decision-making processes at the government level.

1.4.2 Environmental Monitoring

Environmental monitoring is a scientific process that collects and analyzes data to evaluate environmental changes [167]. It uses methods like remote sensing and sensor networks to monitor various parameters [167]. The goal is to understand ecosystem interactions, detect abnormal conditions, and assess the impact of human activities [167]. This information is crucial for managing environmental risks and promoting sustainability [167]. It also addresses challenges like climate change and pollution [167].

Air Quality Monitoring

Like particulate matter, carbon monoxide, nitrogen dioxide, and ozone are measured by IoT devices. This information aids in determining the degree of air quality in industrial and urban

zones.
The proposed IoT-based air quality monitoring system by [168] using fog computing techniques provides real-time and accurate measurements, improving the quality of services and reducing latency issues. [169] proposed a green air quality monitoring system that uses photovoltaic energy, reducing pollution and promoting healthier air for people and the environment. [170] made a real-time air quality monitoring system using the Internet of Things and mobile computing technologies, providing a cost-effective solution for monitoring and improving air quality in smart cities.

Water Quality Monitoring

In Water bodies, such as rivers and lakes, can have sensors installed to monitor many characteristics, including turbidity, dissolved oxygen, pH levels, and pollution concentrations. This helps evaluate the condition of water resources and aquatic habitats.
[171] designed low-cost wireless water quality monitoring system allows for cost-effective, high-resolution monitoring, aiding catchment managers in maintaining aquatic ecosystems and understanding aquatic animal behavior.Moreover, [172] presents a real-time water quality monitoring and control system using PLC, Arduino, and Bluetooth modules, which can effectively detect and control water quality issues in swimming pools, ponds, and other manmade water bodies.However, water quality monitoring programs should address various information needs, including trend assessment, compliance, mass transport estimation, and general surveillance, to effectively address various information needs [173].

Monitoring of the Weather and Climate

Real-time data on temperature, humidity, wind speed, and atmospheric pressure are collected by IoT devices that are outfitted with weather sensors. Understanding long-term climate trends, doing climate research, and weather forecasting all depend on this data.
However, [174] proposed IoT-based weather monitoring system uses arduino-based wireless sensor networks to provide real-time climate data, including temperature, humidity, and gas presence, for remote applications and visualization.Additionally, IoT technology and solar panels effectively provide efficient weather forecasting by monitoring various climatic factors and predicting atmospheric conditions [175]. Opportunistic sensors, such as smartphones and personal weather stations, can effectively monitor hydrometeorological conditions in urban areas, enhancing our understanding of urban heat islands and front passage [176]. The IoT-based weather monitoring system accurately proposed by [177] predicts climate conditions with high accuracy, making it low-cost and user-friendly for various industries.

Environmental Noise Monitoring

This technique uses sensors to gauge noise levels in cities in order to evaluate noise pollution. When building a city and putting policies in place to lessen the negative effects of noise pollution on citizens, this data is invaluable. Environmental IoT enables fast and effective traffic noise monitoring and simulation, enabling accurate simulation and real-time network distribution[178]. However, [179] proposed an IoT-based urban noise monitoring system that accurately classifies real-time environmental audio sounds with 95% accuracy, aiding in safe area selection.Furthermore, an IoT-based air and sound pollution monitoring system was proposed by [180], This paper uses wireless embedded computing systems to effectively detect and manage environmental issues. Additionally, the Underpinning IoT for Road Traffic Noise Management in Smart Cities paper [181] presents an IoT-based approach that effectively monitors and manages road traffic noise in smart cities, reducing noise pollution and improving residents' health and well-being.

Monitoring of Soil

IoT devices are used in agriculture to keep an eye on the temperature, nutrient content, and moisture content of the soil. This aids in the best possible crop management, fertilizing, and irrigation practices for farmers. Moreover, the integration of IoT technology into the Arduino platform for monitoring soil moisture and nutrient levels in indoor plants has been proposed by [182]. Additionally, an IoT framework tailored for digital farming has proven effective in the comprehensive monitoring of soil conditions and microclimatic variables [183]. By incorporating IoT-based soil monitoring systems, there is potential for a significant boost in agricultural productivity. These systems enable real-time observation of crucial soil parameters, providing farmers with timely information for informed decision-making and the optimization of agricultural practices. Consequently, this technological advancement not only facilitates precision agriculture but also holds promise for fostering sustainable and efficient farming practices, ultimately contributing to improved crop yields [184].

Monitoring of Wildlife

IoT devices and sensors are utilized in conservation efforts to monitor the whereabouts and activities of wildlife. Researchers can better comprehend animal habitats, migration patterns, and population dynamics with the help of this data. IoT platforms can effectively support wildlife monitoring applications like location tracking, habitat observation, and behavior recognition, with potential for resource-saving mechanisms [185] .
Numerous studies have made significant contributions to this domain. Notably, The proposed opportunistic dual radio IoT network architecture proposed by [186] enables ultra-low power and sustainable wildlife monitoring applications by leveraging opportunistic mobile networks in a fixed

LPWAN IoT network infrastructure. Furthermore, [187] proposes a system that combines RFID and IoT technologies to enable real-time tracking of wild bird feeder usage in central Arkansas, offering a breakthrough in wildlife monitoring technology. In addition to the previous papers, [188] explored how LoRa technology can effectively monitor wildlife in dense forest vegetation, with a range of up to 860 meters in highly dense environments and up to 2050 meters in not-so-dense environments.

Disaster Management

In early warning systems for natural catastrophes like floods, earthquakes, and wildfires, environmental monitoring is essential. IoT devices assist in gathering information that can be utilized to forecast and address these occurrences. IoT can effectively enhance disaster management by providing environmental intelligence, analyzing information, predicting events, and improving human performance in various disaster scenarios [189]. Notably, IoT-based disaster management can be life-saving and secure smart city infrastructure, reducing risks and saving lives in various disasters [190]. Moreover, [191] proposes a low-cost, autonomous, and scalable IoT framework for disaster management systems, addressing visibility and rapid-dynamic response challenges with off-the-shelf modules and hybrid connectivity. Furthermore, IoT can enhance disaster management by predicting occurrences and damage, enhancing efficiency through AI, big data, cloud computing, and drones, and requiring expert training [192].

Ecosystem Health Monitoring

By continuously monitoring a range of environmental parameters, the overall health of an ecosystem can be evaluated. This aids in spotting modifications or disruptions that could affect ecological balance and biodiversity. IoT technology enables a prototype ecosystem monitoring system, enabling real-time, low-cost, and distributed ecosystem monitoring in remote areas [193]. IoT technology can effectively monitor urban tree ecosystem services, providing valuable data for sustainable urban development and environmental policies [194]. The domain has seen substantial input from various research endeavors. Notably, [195] presents an IoT healthcare ecosystem for smart homes that can monitor vital signs, such as heart rate, temperature, and respiration, while sleeping or engaging in indoor and outdoor activities, with secure authentication and data privacy. Furthermore, sustainable health IoT can improve human health and well-being by sensing and monitoring climate change impacts and integrating social, economic, and environmental sectors for sustainable health and community goals [196].

Remote sensing

By giving an aerial perspective of vast regions, satellites and UAVs outfitted with IoT technology aid in environmental monitoring. This is especially helpful for monitoring changes in urbanization, deforestation, and land cover. Several researchers have made valuable contributions to this field. Notably, Remote Sensing System for Smart Farming [197]. [198] proposed and IoT-based remote sensing and control of greenhouse agriculture parameters can increase yield and provide organic farming by controlling CO2, soil moisture, temperature, and light. Moreover, Remote Sensing Data Supporting Privacy Preservation with Distribution Scheme for IoT Remote Sensing Data maintains high computational efficiency and prevents tampering and forgery while maintaining privacy preservation [199].Furthermore, [200] authors contribute to the user authenticated key management protocol (UAKMP), which provides a secure, lightweight, and cost-effective three-factor remote user authentication scheme for IoT networks, offering offline sensing node registration, user anonymity, and sensing node anonymity.

1.4.3 Agricultural IoT (AgriTech)

The integration of IoT technologies into agriculture to improve production, sustainability, and efficiency is known as Agricultural IoT, or AgriTech. The following are Agriculture IoT's main features:

- **Accurate Farming:** Drones, temperature sensors, and soil moisture sensors are a few examples of IoT devices that gather data on different farm characteristics. Farmers can make precise decisions about irrigation, fertilization, and pesticide application by using data analytics tools to analyze the gathered information. The domain has been enriched by a diversity of research efforts. Notably, precision agriculture can be achieved through accurate weather forecasting, enabling farmers to make informed decisions and manage resources effectively, enhancing productivity and yield [201]. Moreover, smart farming using accurate satellite data leads to lower production costs, increased efficiency and more sustainable agriculture, benefiting both farmers and the environment [202]. Furthermore, precision farming reduces waste and environmental costs, offering potential environmental and economic benefits for farmers worldwide [203].
- **Smart Irrigation:** Sensors track soil moisture content, enabling irrigation schedule modification and avoiding overwatering. IoT-enabled irrigation systems can be remotely or automatically controlled in response to crop requirements, meteorological predictions, and real-time data. The domain has seen substantial input from various research endeavors. Notably, The smart irrigation system using Arduino-Uno automatically checks soil moisture levels and adjusts watering based on moisture levels, reducing water wastage and soil damage [204]. Moreover, [205] proposed a smart platform that effectively manages linear

irrigation systems, enabling precise water supply and real-time monitoring in tomato fields. Furthermore, smart irrigation systems proposed by [206] can optimize water usage in areas with water scarcity, reducing water usage and promoting efficient crop watering. In addition, smart irrigation systems by [207] can improve water resource management and sustainability in agriculture, but adaptation to specific agro-environmental contexts is needed.

- **Livestock Monitoring:** Animal-attached devices can track behavior, location, and health metrics to provide valuable information about cattle welfare. Tracking systems with RFID and GPS technology assist in preventing theft, managing the movement and health of animals, and improving feeding procedures.A considerable body of research has been dedicated to advancing knowledge in this particular domain. Notably, the proposed IoT-based real-time livestock monitoring system proposed by [208] uses multi-sensor boards, machine learning, and Wi-Fi/GSM technology to detect sick animals and predict cattle health, enabling early and timely medical care. Moreover, [209] proposed an IoT-based livestock monitoring and management system effectively improves farm efficiency and animal welfare by utilizing relevant sensors and a flexible technology stack.

1.4.4 Industrial IoT (IIoT)

Within the industrial landscape, IIoT transforms traditional manufacturing processes by incorporating sensors and connectivity (Figure 1.6). This enables real-time monitoring of equipment, predictive maintenance, and enhanced efficiency in production. IIoT fosters the concept of smart factories, where interconnected systems streamline operations and minimize downtime [210, 211, 212]. The literature reflects numerous research initiatives that have advanced this domain. Notably, the proposed data sharing mechanism for industrial IoT sensors and actuators using blockchain-assisted identity-based cryptography effectively improves industrial production efficiency [213]. Moreover, the adoption of IoT in manufacturing leads to the generation of industrial big data, enabling new data-driven strategies and transforming traditional systems into modern digitalized ones [214]. In addition, [215] proposes a graphical model for analyzing industrial IoT networks' vulnerability relations and a set of risk mitigation strategies to improve overall security.

1.4.5 Healthcare

IoT plays a pivotal role in revolutionizing healthcare through applications like remote patient monitoring, wearable health devices, and smart medical equipment (Figure 1.7). These technologies enable continuous monitoring of vital signs, medication adherence tracking, and efficient management of medical resources, ultimately enhancing patient care and reducing healthcare costs [216, 217, 218, 219]. The domain has been enriched by a diversity of research efforts. Notably,[220] presents a novel healthcare IoT system that combines attribute-based

Figure 1.6: Industry 4.0. [5]

encryption, cloud computing, and edge computing for efficient, flexible, and secure fine-grained access control in healthcare IoT networks without secure channels. Moreover, in the domain of security, [221] proposed a HealthIIoT-enabled monitoring framework that securely transmits patient healthcare data to the cloud for seamless access by healthcare professionals, reducing identity theft and clinical errors. However, real-time decision-making for this kind of application is highly sensitive and crucial. [222] contributes to an IoT-based system that efficiently transmits real-time health data over low-power wireless area networks (6LoWPAN), providing a cost-effective and reliable solution for remote monitoring in healthcare applications.

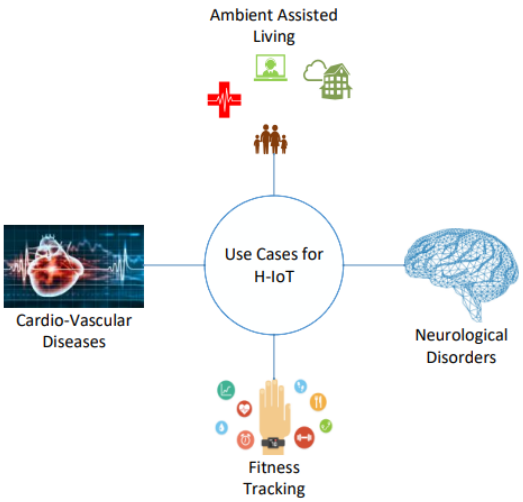

Figure 1.7: Broad Categories of H-IoT Applications [6]

Wearable devices represent a popular and tangible manifestation of IoT, seamlessly integrating technology into daily life. Smartwatches, fitness trackers, and other wearables collect and transmit data for health monitoring, fitness tracking, and personalized user experiences. The data insights derived from wearables empower individuals to make informed decisions about their well-being [223, 224, 225, 226]. Extensive literature exists on the topic of wearables. Notably, wearable sensors and IoT-based monitoring solutions show promise for supporting independent living for older adults, but they face challenges like low usability, battery issues, and a lack of interoperability [227].As noted by [228], Wearable IoT (WIoT) can revolutionize healthcare by providing personalized health and wellness information through wearable sensors, internet-connected gateways, and cloud and big data support.

1.4.6 Smart transportation

Smart transportation and traffic management involve the integration of advanced technologies to improve the efficiency, safety, and sustainability of transportation systems within urban areas (Figure 1.8). Here are key components of smart transportation and traffic management:

- **Intelligent Transportation Systems (ITS):** Traffic Surveillance and Management using data analytics, cameras, and sensors to continuously monitor traffic conditions. Congestion control and traffic signal timing optimization are achieved with the help of this data. Adaptive Traffic Scheduling giving drivers access to real-time traffic information via navigation applications so they may select the best routes given the circumstances at the time [229, 230].
- **Connected and Autonomous Vehicles:** Communication from Vehicle to Infrastructure (V2I) improves traffic flow and safety by enabling communication between automobiles and traffic infrastructure. We mention [231] presents a novel IoT platform for the era of connected cars, enabling data collection, processing, and distribution in real-time for various use cases, including CAN data collection, remote device flashing, eco-driving, and weather reports. Moreover, [232] contributes on a generic, scalable IoT solution for electric vehicles, providing real-time cloud connectivity and data collection for up to 2 CAN buses with a 63% cheaper hardware prototype. Autonomous Automobiles Introducing self-driving cars [231], which can improve transportation efficiency, minimize accidents, and optimize traffic patterns,
- **Smart Parking:** Installing sensors in parking spots to deliver information about available spaces in real time. By using smartphone apps, drivers may receive this information and spend less time looking for parking. Reducing the need for physical payment methods and streamlining transactions by integrating digital payment solutions for parking [233]. Scholars have extensively investigated smart parking solutions using dual-mode Bluetooth mesh networks that effectively localize parked vehicles in outdoor parking lots, offering

faster occupancy turnover and lower costs for future parking management applications [234].Moreover, [235] proposes a smart parking solution based on LoRaWAN and Kubernetes, enabling real-time parking space find, view, and rate with a portable and scalable architecture. Additionally, [236] aims to enhance smart parking solutions by incorporating image processing and machine learning, enhancing management processes, and integrating security solutions.

- **Smart Traffic Lights:** Using smart traffic lights that modify signal timings in response to current traffic circumstances can reduce congestion and enhance overall traffic flow. This is known as adaptive traffic signal control. A substantial body of research has addressed this domain. Notably, the smart agent algorithm-based traffic light effectively reduces traffic congestion and accidents by adaptively controlling traffic signals in congested conditions [237]. Additionally, the smart traffic light using a fuzzy-logic-based microcontroller effectively reduces traffic congestion at road junctions by adapting to vehicle dynamics and using ultrasonic, infrared, and light sensors [238]. Moreover, The smart traffic light system using Vehicular Ad hoc NeTworking (VANET) and Named Data Networking (NDN) proposed by [239] reduces traffic congestion and waiting time by using virtual traffic lights and roadside units.

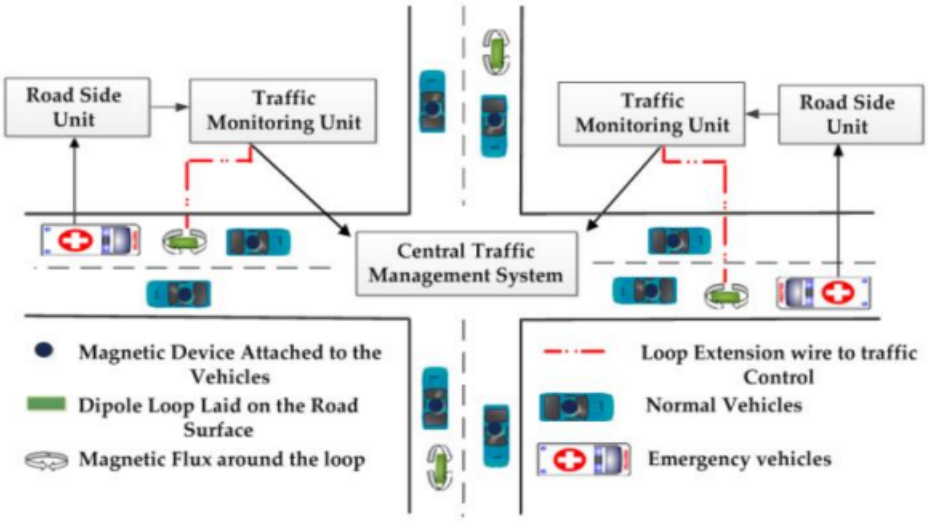

Figure 1.8: Smart traffic control management [7]

1.5 IoT Architecture

The foundational architecture of the IoT comprises three essential layers: The perception layer, the network layer, and the application layer (Figure 1.9). Despite the apparent simplicity of this multi-layer structure, the operations within the network and application layers are both diverse and intricate [240].

Within the network layer, responsibilities extend beyond basic routing and data transmission. This layer is tasked with providing comprehensive data services, including aggregation and computing functionalities. Similarly, the Application Layer, responsible for serving both customers and devices, goes beyond basic service provision. It encompasses data services such as mining and analytics [241].

To establish a versatile and adaptable multi-layer architecture for IoT, an intermediary service layer is introduced between the network layer and the application layer. This service layer is designed to facilitate data services within the IoT framework. The adoption of Service-oriented Architectures (SoA) has been a pivotal development, leading to a four-layered IoT architecture [241].

In addition to the four layers, a business layer has been incorporated to further enrich the IoT architecture. This layer is instrumental in constructing business models, flow charts, and graphs. It plays a pivotal role in the design, analysis, and implementation of various elements within the IoT system. Moreover, the business layer supports the comparison of outputs from each layer with expected outcomes, thereby enhancing the overall user experience [242].

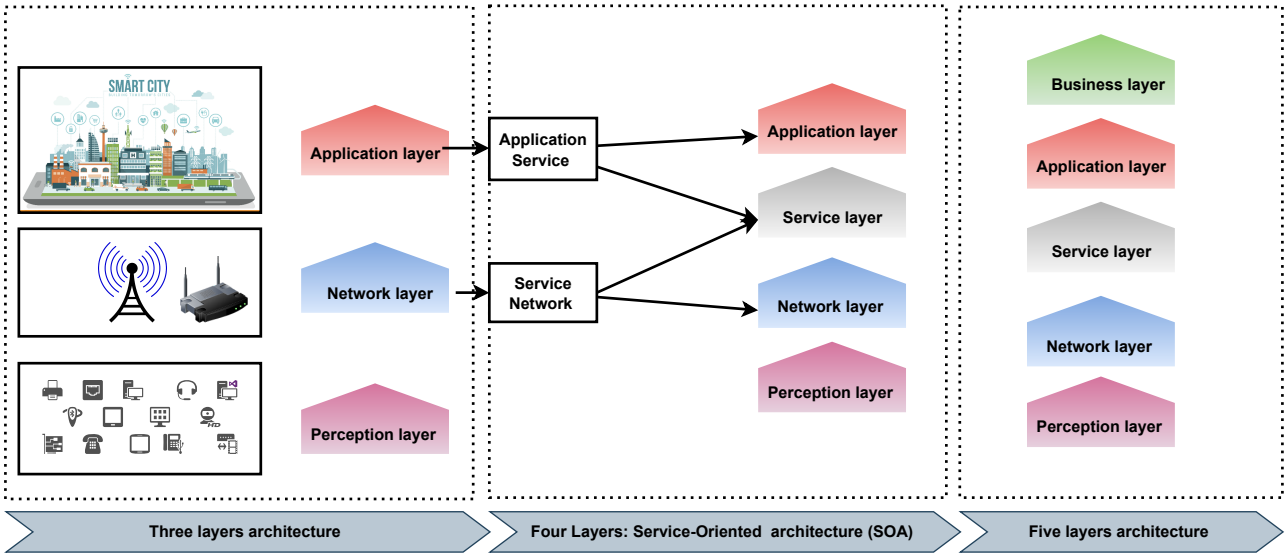

Figure 1.9: Iot architecture

1.6 IoT Data Management

Efficient data management lies at the core of successful IoT implementations, ensuring the seamless flow, storage, and analysis of vast amounts of data generated by interconnected devices. The design of data management systems focuses on the structure of these systems and the optimal methods for storing and preserving data. Processing elements are responsible for handling data access and processing within storage systems [8]. Various approaches are employed in the design

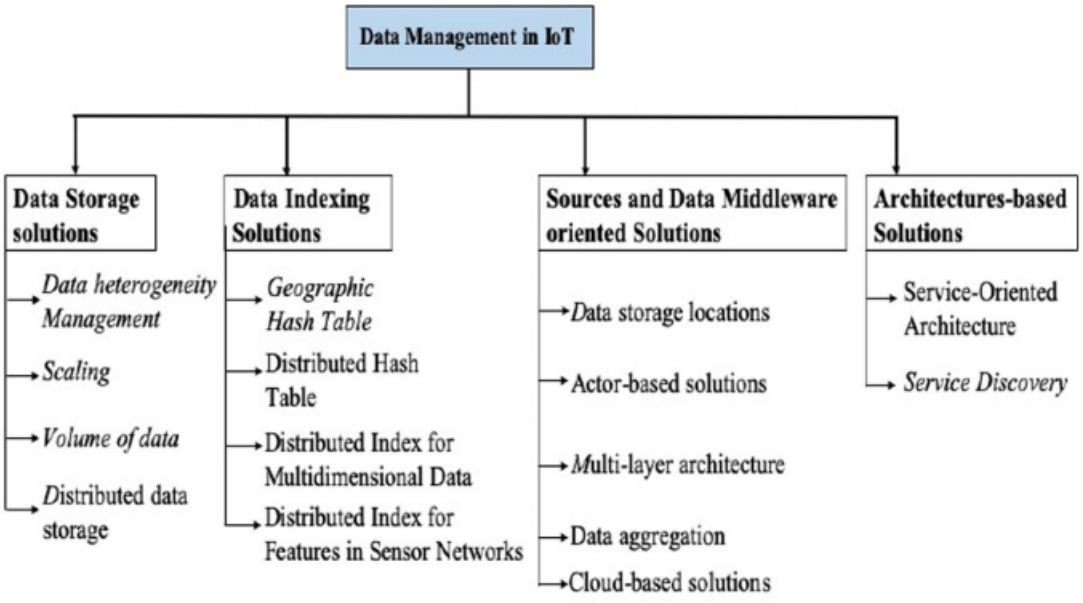

Figure 1.10: Taxonomy of Data management solutions in IoT [8]

of data management systems, as outlined in the following and depicted in the taxonomy shown in (Figure 1.10).

1.6.1 Big Data analytics in IoT

As IoT devices generate massive volumes of data, leveraging big data analytics becomes instrumental in extracting meaningful insights. This involves the use of advanced algorithms and analytics tools to analyze, interpret, and derive actionable intelligence from the vast datasets produced by interconnected devices. Big Data analytics in IoT facilitates real-time decision-making, predictive maintenance, and the identification of trends, ultimately enhancing operational efficiency and innovation [243, 244, 245, 246] .

1.6.2 Data storage and processing techniques

Effectively managing the storage and processing of IoT data is essential for optimizing system performance and ensuring seamless operations. Various techniques contribute to this aspect, including:

- **Cloud-Based Storage:** Leveraging cloud services for data storage provides scalability, flexibility, and accessibility. Cloud platforms enable the centralized storage of vast datasets and facilitate on-demand processing [247]. However, a multi-cloud or hybrid cloud storage model can effectively secure and protect IoT data while maintaining high system availability [248]. Additionally, the intelligent storage management system, combining cloud computing and IoT, offers stronger applicability and expansion functions, benefiting various intelligent

management systems [249].

- **Edge Computing:** Processing data at the edge, closer to the source of generation, reduces latency and enhances real-time decision-making [250]. Edge computing is particularly beneficial for applications where immediate insights are crucial.
- **Distributed Databases:** Utilizing distributed databases ensures resilience and reliability in handling large volumes of IoT data. This approach involves spreading data across multiple nodes or servers to enhance scalability and fault tolerance [251].
- **Compression Techniques:** Employing data compression techniques minimizes storage requirements and enhances data transmission efficiency. Compression reduces the size of datasets without compromising the integrity of the information. Big data compression techniques in IoT frameworks can reduce the complexity of big data management tasks, improving efficiency and scalability [252].Moreover, lossless compression techniques are essential for maintaining data integrity in low-bandwidth IoTs like NBIoT and LTE-M, ensuring efficient use of limited resources [253].
- **In-Memory Computing:** Storing and processing data in memory rather than on traditional disk-based storage systems improves speed and responsiveness. In-memory computing can significantly improve computing efficiency for IoT and AI tasks, eliminating data transfer time and energy consumption while performing massive parallel computations. Notably, [254] proposed a photodiode-one memristor pixel vision sensor demonstrates in-memory computing capabilities, offering a portable and energy-efficient solution for IoT applications.Additionally, ReRAM-based in-memory computing architecture for SHA-3 encryption and authentication on IoT nodes offers comparable throughput to optimized, bit-serial, lightweight CMOS implementations [255].

1.7 Challenges and Future Trends

The implementation of the Internet of Things is currently challenged by security vulnerabilities, privacy concerns, interoperability issues, scalability limitations, data management complexity, and the need for power-efficient devices (Figure 1.11). To address these challenges, emerging trends in IoT point towards the dominance of edge computing, the integration of 5G networks for enhanced connectivity, the synergy of AI and machine learning for intelligent data processing, the potential use of blockchain for heightened security, and a growing focus on sustainability. Navigating these challenges while embracing these future trends is pivotal for shaping a resilient and innovative landscape in IoT implementations, fostering advancements in connectivity, intelligence, and sustainable practices.

- **Security and Privacy:** Wireless IoT presents new privacy challenges, including a lack of theoretical foundation, trade-off optimization between privacy and data utility, and system

isomerism over-complexity and high scalability [256].

- **Interoperability and Standardization:** Ensuring seamless communication and compatibility among diverse IoT devices and platforms.However, standardized IoT platforms based on oneM2M global standards can efficiently deliver services across multiple technology domains, enabling interoperability between devices and cloud-based applications [254].
- **Scalability:** managing the scale of IoT deployments and addressing power efficiency for devices, especially in remote locations.
- **Availability:** Ensuring IoT availability involves both hardware and software. Software availability enables IoT applications to serve individuals in different locations simultaneously, while hardware availability ensures the continuous presence of devices supporting IoT functionality and protocols[257].

Figure 1.11: Iot challenges [4]

1.8 Conclusion

In conclusion, this chapter provides a comprehensive exploration of IoT, covering its definition, key technologies, applications, architecture, and data management. The discussion delves into crucial aspects such as sensor technologies, communication protocols, cloud computing, fog computing, and edge computing. Furthermore, the chapter explores diverse IoT applications, including Smart City services, environmental monitoring, Agricultural IoT, Industrial IoT, healthcare, and smart transportation. The architecture and data management sections shed light on the structural framework and handling of data in IoT systems, emphasizing big data analytics, storage, and processing techniques.

As with any rapidly evolving field, the chapter also addresses challenges and anticipates future trends in IoT. The examination of challenges serves to highlight potential obstacles, while the exploration of future trends provides insight into the direction in which the IoT is headed.

Overall, this chapter serves as a valuable resource for understanding the multifaceted landscape of the IoT and lays the groundwork for further exploration and research in this dynamic and transformative field.

Chapter 2

Unmanned Aerial Vehicles (UAVs)

2.1 Introduction

Drones have become essential tools in various sectors, including military operations, disaster response, emergency services, and surveillance. These intelligent devices have revolutionized how we approach challenges, providing unprecedented capabilities and efficiencies in navigating complex environments. The following chapter will explore the multifaceted applications of unmanned aerial vehicles and their transformative impact on diverse industries.

2.2 Definition and Overview of Drones

Drones are highly mobile and lightweight devices that operate within the constraints of limited energy, storage, and processing resources. Equipped with various sensors, these devices excel in navigating complex environments to accomplish various missions. Drones can function autonomously or be controlled remotely, and they have the ability to collaborate and establish connections with other drones and devices, forming a cohesive drone network for enhanced capabilities.
Joint Publication 1-02, the Department of Defense Dictionary, defines a UAV as follows: *"A powered, aerial vehicle that does not carry a human operator, uses aerodynamic forces to provide vehicle lift, can fly autonomously or be piloted remotly, can nonlenthal payload. Ballistic or semiballistic vehicles, cruise missiles, and aertillery projectiles are not considered unmanned aerial vehicles."* [9]
by Henri Eisenbeiss defines a UAV as follows: *"The name UAV covers all vehicles, which are flying in the air with no person onboard with capability controlling the aircraft. This term is used commonly in the computer science and artificial intelligence community, but terms like Remotely Piloted Vehicle (RPV), Remotely Operated Aircraft (ROA), Remote Controlled Helicopter (RC-Helicopter), Unmanned Vehicle Systems (UVS) and model helicopter are often used, too"* [258]

The term UAV gained widespread adoption in the early 1990s to characterize automated aircraft, supplanting the previously utilized expression RPV, which was employed during and after the Vietnam War [9]. The family tree of unmanned aerial vehicles is depicted in (Figure 2.1)

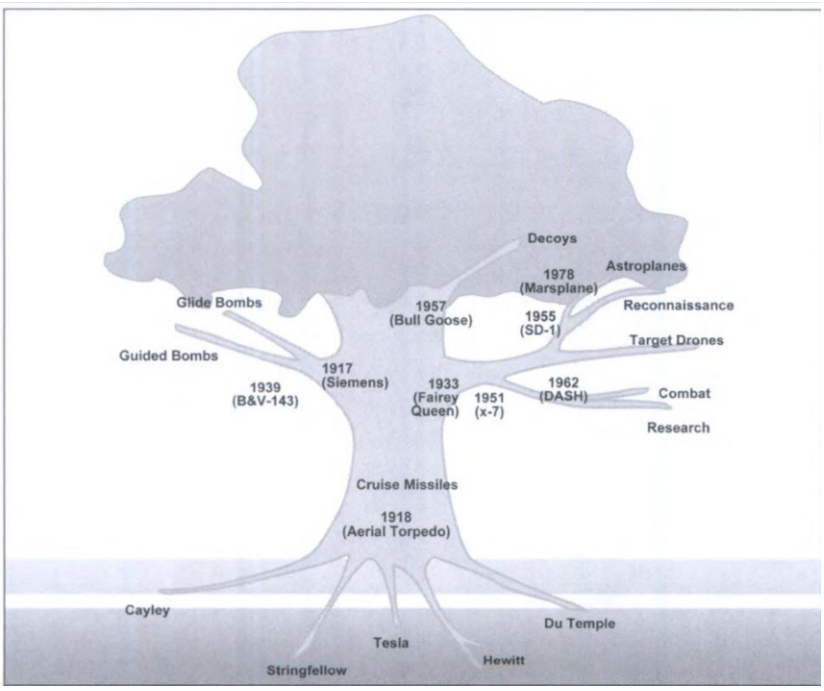

Figure 2.1: A family tree of unmanned aerial vehicles [9]

2.3 Drones by Category

Drones, or unmanned aerial vehicles, come in various types designed for specific purposes and applications. Here are some common types:

2.3.1 Classification by Performance Characteristics

Classification by Weight

UAVs cover a wide range of weights Table 2.1 2.2 2.3, from the lightweight micro UAVs that weigh just a few pounds to the substantial Global Hawk (Tier III), which exceeds 11 tonnes [13]. However, it is important to note that the majority of examined UAVs fall into the category of relatively light UAVs, with only a limited number surpassing two tonnes. This data highlights the significant impact that lightweight UAVs have in the industry [13].

Classification by Endurance and Range

To classify UAVs, one alternative method is to evaluate their endurance and range, which are typically interconnected. The duration a UAV can remain in the air is directly proportional to its operational radius [13]. Evaluating range and endurance is crucial for UAV designers. This allows them to determine the appropriate UAV type based on the distance of the mission objective from the launch site and the frequency of refueling. By considering these factors, UAV designers

Class Type	Drone Category	Weight Range
Class I(a)	Nano drones	$W \leqslant 200\,\mathrm{g}$
Class I(b)	Micro drones	$200\,\mathrm{g} < W \leqslant 2\,\mathrm{kg}$
Class I(c)	Mini drones	$2\,\mathrm{kg} < W \leqslant 20\,\mathrm{kg}$
Class I(d)	Small drones	$20\,\mathrm{kg} < W \leqslant 150\,\mathrm{kg}$
Class II	Tactical drones	$150\,\mathrm{kg} < W \leqslant 600\,\mathrm{kg}$
Class III	MALE/HALE/Strike drones	$W > 600\,\mathrm{kg}$

Table 2.1: Proposed drones' categorization by Brooke-Holland based on their weight [12]

Designation	Weight Range	Example
Super Heavy	> 2000 kg	Global Hawk
Heavy	$200 - 2000$ kg	A-160
Medium	$50 - 200$ kg	Raven
Light	$5 - 50$ kg	RPO Midget
Micro	< 5 kg	Dragon Eye

Table 2.2: Proposed drones' categorization by Arjomandi et al. based on their weight [13]

Designation	Weight Range
Micro	$W < 2\,\mathrm{lbs}$
Mini	$2\,\mathrm{lbs} \leqslant W \leqslant 30\,\mathrm{lbs}$
Tactical	$30\,\mathrm{lbs} \leqslant W \leqslant 1000\,\mathrm{lbs}$
Medium and high altitude	$1000\,\mathrm{lbs} \leqslant W \leqslant 30,000\,\mathrm{lbs}$
Heavy	$W > 30,000\,\mathrm{lbs}$

Table 2.3: Proposed drones' categorization by Weibel and Hansman based on their weight [14].

can confidently select the most suitable UAV for the mission. These factors directly impact the duration the UAV can spend on its task while airborne and on the ground [13].

Category	Endurance	Range	Example
High	> 24 hours	> 1500 km	Predator B
Medium	$5 - 24$ hours	$100 - 400$ km	Silver Fox
Low	< 5 hours	< 100 km	Pointer

Table 2.4: Range and Endurance Categories [13]

Classification by Maximum Altitude

The maximum operational altitude, often referred to as the flight ceiling, stands as another performance metric for classifying UAVs. This criterion is beneficial for designers and potential buyers in selecting a UAV that aligns with specific altitude requirements [13]. In military scenarios, certain UAVs necessitate low visibility to evade enemy detection and potential destruction, making high altitude a crucial specification. Moreover, for imaging and reconnaissance purposes, a high

operational altitude is essential to capture images of a broader expanse of terrain [13].

Category	Max Altitude	Example
Low	< 1000 m	Pointer
Medium	$1000 - 10000$ m	Finder
High	> 10000 m	Darkstar

Table 2.5: Classification by Maximum Altitude [13]

Classification by Wing Loading

An additional effective method for categorizing UAVs involves considering their wing loading capacity. To determine the wing loading of a UAV, the total weight of the UAV is divided by its wing area Table 2.6 [13].

Category	Wing Loading (kg/m^2)	Example
Low	< 50	Seeker
Medium	$50 - 100$	X-45
High	> 100	Global Hawk

Table 2.6: Classification by Wing Loading [13]

Classification by Engine Type

UAVs require diverse engines for various tasks, with electric and piston engines being the most prevalent in the considered projects. The relationship between a UAV's weight and its engine size aligns with general aeronautical principles. Lighter UAVs commonly employ electric motors, whereas heavier military-grade UAVs favor piston engines. The type of engine significantly impacts endurance and range, emphasizing the importance of selecting an appropriate engine for enhanced UAV capabilities Table 2.7 [13].

2.3.2 Classification by mission Aspects

To systematically classify UAVs based on their mission capabilities, it is advantageous to categorize them. The UAV Roadmap of 2002 outlines mission capabilities into the following classifications: Intelligence, Surveillance, Target Acquisition, and Reconnaissance (ISTAR); Combat (UCAV); Multi-Purpose; Vertical Take-Off and Landing (VTOL); Radar and Communication Relay; Aerial Delivery and Resupply [13].

UEL Rotary	**Turbofan**	Two stroke	Piston	Turboprop	Electric	Push & Pull	Prop
Outrider	Global Hawk	Pioneer	Predator B	Predato C	Dragon Eye	Hunter	LEWK
Shadow	Darkstar	RPO Midget	Neptune		FPASS		Sperwer
Shadow	600 Phoenix		Dragon Drone		Dragon Warrior		
Cypher	X-45		Finder		Pointer		
	X-50		A 160		Raven		
	Fire		Scout		GNAT Luna		
			Crecerelle		Javelin		
			Seeker				
			Brevel				
			Snow Goose				
			Silver Fox				
			Heron				

Table 2.7: UAVs and Engine Types [13]

ISTAR

The Intelligence, Surveillance, Target Acquisition, and Reconnaissance (ISTAR) system employs UAVs to systematically collect pertinent enemy intelligence, ascertain target locations, and patrol adversarial airspace, thereby mitigating the exposure of operators to life-threatening situations. Particularly in military engagements, ground combat commanders necessitate real-time insights into impending enemy forces. For instance, discerning the nature of enemy defenses beyond an upcoming topographical feature is critical. The utilization of reconnaissance UAVs significantly enhances the efficacy of acquiring such intelligence, concurrently eliminating the peril to the lives of deployed soldiers [13]. This category encompasses the largest number of UAVs, enumerated in Table 2.8 along with their salient features Table

UAV Model	**Key Features**
Brevel	Used for reconnaissance and target locating. Very low radar, acoustic, and thermal signatures.
Cypher	Fitted with video cameras, Infra-Red cameras, chemical detectors, magnometers, radio and satellite links, microphones for relaying pre-recorded announcements. Can be fitted with non-lethal payloads such as tear gas, smoke canisters, or steel spikes.

Table 2.8 – continued from previous page

UAV Model	Key Features
Dark Star	Used for overflying heavily defended areas. Has low-observable characteristics for penetration of robust air defenses. The Tier III Minus UAV.
Dragon Eye	Made of lightweight Styrofoam-like materials, weighs 5 lbs. Backpackable, modular UAV providing organic aerial reconnaissance and surveillance for the US Marine Corps.
FPASS/Desert Hawk	Designed for conducting area surveillance, patrolling base perimeters, and runway approach/departure paths, and performing convoy overwatch.
Global Hawk	Endurance of 36 hours and range over 21,720 km. Equipped with ISS, SAR/MTI, and IR/EO sensors. Used operationally in Afghanistan and Iraq. The Tier II Plus.
GNAT	Long-endurance surveillance UAV, later evolved into the Predator.
Heron	Deep-penetration, wide-area, real-time intelligence. Medium altitude and long-endurance strategic UAV System ISTAR.
Hummingbird Warrior	Provides reconnaissance, surveillance, target acquisition, communication relay, precision re-supply, sensor delivery, and eventually precision attack capabilities.
LEWK	Loitering Electronic Warfare Killer (LEWK). Affordable, recoverable UAV for radar jamming, lethal/non-lethal munitions delivery, communication relay, and imagery receipt.
LUNA	Family of advanced lightweight reconnaissance drones. Easily transported, automated flight control, designed for mobility with minimal logistics trail.
Neptune	Specially suited for operations over water. Payload includes a color camera or a thermal imaging device. Optimized for quick launch from ground and sea.
Shadow	Tactical UAV for gathering intelligence. Provides color video images in daylight and black-and-white thermal images at night.
Outrider	Tactical intelligence UAV for near-real-time reconnaissance, surveillance, and target acquisition. Range of 200 kilometers and target on-station time of four hours.

Table 2.8 – continued from previous page

UAV Model	Key Features
Phoenix	Real-time surveillance and target acquisition UAV designed to integrate with the Battlefield Artillery Target Engagement System (BATES). All-weather day and night surveillance capability.
Pioneer	Procured starting in 1985 for interim UAV capability. Provides imagery intelligence (IMINT) for tactical commanders on land and at sea.
Predator A	RQ-1 Predator is a long-endurance, medium-altitude unmanned aircraft system for surveillance and reconnaissance missions. Equipped with synthetic aperture radar, video cameras, and forward-looking infra-red (FLIR).
Raven	Search for improvised explosive devices (IED), provide reconnaissance for patrols, and fly the perimeter of camps.
Silver Fox	Designed to provide low-cost aerial surveillance imaging and carry sensor payload packages. Video images are transmitted to the ground station for quick reference.

Table 2.8: Overview of Various UAVs in the ISTAR Category [13]

UCAV

UCAV, an acronym denoting Unmanned Combat Aerial Vehicles, represents a class of aircraft characterized by high maneuverability Table2.9, enabling them to participate in air-to-air combat and deliver precision weaponry to surface targets. In contrast to other UAVs, UCAVs exhibit elevated cruise speeds but frequently have shorter endurance capabilities. Presently, all UCAVs are undergoing experimental and testing phases, guided by specific design objectives [13].

Multi-Purpose UAVs

In the realm of Multi-Purpose UAV, typically repurposed from reconnaissance counterparts, their central mission involves interdiction and armed reconnaissance against crucial, time-sensitive targets. Equipped with self-guided weapons, these UAVs are capable of delivering precision strikes with maximum impact. Multi-Purpose UAVs excel in reconnaissance, surveillance, and target acquisition, providing crucial support to the Joint Forces commander in scenarios where weaponry is unnecessary [13].

- MQ-1 Predator: A multi-functional adaptation stemming from the reconnaissance predator, equipped to carry and deploy two AGM-114 Hellfire missiles for armed reconnaissance

UCAV Characteristics	X45 UCAV Specifications
Unmanned Combat Aerial Vehicles (UCAV)	- Cruise speed of Mach 0.85 - Carries a 4,500-lb. payload - Flies at an altitude of 40,000 feet with a mission radius of 1,200 nautical miles - Transports eight 250-lb. Small Diameter Bombs - Accommodates auxiliary fuel tanks and other payloads - Capable of hitting a ground target with a 250-lb. inert near-precision-guided weapon
Design Goals for UCAVs	- Engage in deep strikes with precision weapons - Complement manned fighter and bomber forces - Highly adaptable to changing battle conditions - Provides 24/7 electronic attack capabilities - Secondary missions include high-risk reconnaissance, surveillance, and intelligence gathering - Refueled by Air-to-Air Refueling - Operates independently, integrates with manned aircraft operations, or executes multi-vehicle coordinated operations - Deployable from one location and controlled by another

Table 2.9: Overview of UCAV Characteristics and X45 Specifications [13]

tasks.

- MQ-5B Hunter: This variant of the Hunter is meticulously optimized for diverse mission roles, featuring enhancements such as an extended center-wing section, improved avionics, and Mercedes Benz heavy-fuel engines. It operates at higher altitudes (6,100m or 20,000ft) with an extended endurance of 15 hours. The MQ-5B Hunter is armed with the Viper Strike, a highly accurate laser-guided bomb suitable for urban combat.
- MQ-9 Predator B: Essentially an upsized version of the RQ/MQ-1 Predator, the MQ-9 seamlessly integrates striking and reconnaissance capabilities. It can be outfitted with AGM-114C/K Hellfire missiles and various guided munitions.

VTOL

VTOL UAVs are a distinct group of UAV that possess the unique capability to generate downward thrust, enabling them to take off within confined spaces. While they may share characteristics with other categories, their crucial ability to vertically take off and land sets them apart [13]. VTOL UAVs are a crucial component of military fleets, particularly in scenarios where traditional runway facilities are inaccessible, such as forest or bush areas, or when launching and recovering from non-carrier battleships. Their unique feature of vertical take-off and landing

capabilities makes them essential for specific missions. It is important to note that this text adheres to the characteristics of objectivity, comprehensibility, and logical structure, with clear and objective language, a formal register, and precise word choice [13].

- Hummingbird Warrior
- Fire Scout
- Killer Bee
- X50

Radar and Communication Relay

- **Tethered Aerostat Radar System** The Tethered Aerostat Radar System is fundamentally an aerodynamic balloon containing a mixture of helium and air. Operating as a low-level surveillance system, it utilizes aerostats as radar platforms with a specific mission to facilitate low-level trafficking surveillance. Additionally, the system has the capability to serve as a relay for television and radio signals, offering versatile applications beyond its primary radar function [13].
- **Near Space Maneuvering Vehicle (NSMV)/Ascender/V-Airship:**
  The NSMV, also known as Ascender or V-Airship, functions in the airspace between 100,000 and 120,000 feet, situated above fixed-wing aircraft and below low-earth orbit satellites. This specific region is virtually devoid of aircraft and surface-to-air missile threats. The primary objective of the NSMV is to complement existing systems such as the Global Hawk by offering a more specialized and responsive capability for communication, intelligence, and reconnaissance purposes [13].
- **Near Space Maneuvering Vehicle (NSMV)/Ascender/V-Airsh** Operating within the altitude range of 100,000 to 120,000 feet, the Near Space Maneuvering Vehicle (NSMV) occupies a strategic position above fixed-wing aircraft and beneath low-earth orbit satellites. This specific aerial region is notable for its scarcity of both aircraft and surface-to-air missile (SAM) threats. The primary purpose of the NSMV is to complement existing systems such as the Global Hawk, offering a heightened level of dedicated and responsive capabilities in the realms of communication, intelligence, and reconnaissance [13].

Aerial Delivery/Resupply

The UAVs falling within this category are specifically engineered for the precise delivery of small cargo items, including ammunition and food supplies, to Special Forces units. The sole representative in this category is the CQ-10 Snow Goose. Comprising a central fuselage module for payload and fuel accommodation, it is equipped with a GPS-based navigation and control system, powered by a single piston engine that propels a pusher propeller. Notably, the CQ-10

Snow Goose demonstrates flexibility in deployment, as it can be air-dropped or launched from a HMMWV [13].

2.4 Drones by Type

2.4.1 UAVs

Drones exhibit a wide range of sizes and configurations, varying in operational purpose (Figure2.2), fabrication materials, and control system complexity and cost. Their mission capabilities often categorize them into different types:

HTOL and VTOL UAVs

Horizontal Take Off and Landing drones (HTOL) come in four configurations: tailplane-aft, tailplane forward, tail-aft on booms, and tailless/flying wing. VTOL drones, especially fixed-wing ones, use a vertical propulsion system at the front of the fuselage. They can take off and land vertically without needing a runway [10].

Tilt-Rotor, Tilt-Wing, Tilt-Body, and Ducted Fan UAVs

VTOL drones are more efficient for hovering flight but have limitations in cruise speed. Hybrid drones, like tilt-rotor, tilt-wing, tilt-body, and ducted fan UAVs, combine VTOL and HTOL capabilities [10]. Tilt-rotor UAVs have rotors that tilt forward for cruise flight, while tilt-wing UAVs have engines fixed to wings that tilt with the wing. Tilt-body UAVs have a free-rotating wing in the pitch axis, and the fuselage acts as a lifting body, providing short take-off and landing (STOL) capabilities. Ducted fan UAVs enclose their thrusters within a duct, with contra-rotating elements for stability. They can take off and land vertically and hover, controlled by counter rotors and control surfaces [10].

Helicopter and Heli-Wing UAVs

Helicopter UAVs come in single rotor, coaxial rotor, tandem rotor, and quad-rotor configurations for vertical takeoff, landing, and hovering. Heli-wing UAVs use a rotating wing as their blade, allowing them to fly vertically like a helicopter and horizontally like a fixed-wing UAV [10].

Unconventional UAVs

UAVs that don't fit into the aforementioned categories are considered unconventional. Bio-inspired flying robots, such as the FESTO AirJelly inspired by jellyfish, fall into this group. The FESTO AirJelly utilizes a peristaltic drive for propulsion and glides through the air using a

helium-filled ballonet. In summary, UAVs encompass a diverse range of configurations to meet various mission requirements, from conventional fixed-wing and rotorcraft designs to hybrid and unconventional models inspired by nature [10].

Figure 2.2: Different types of UAVs,(a) HTOL, (b) VTOL, (c) tilt-rotor UAV, (d) tilt-wing UAV, (e) tilt-body UAV, (f) ducted fan UAV, (g) helicopter, (h) heli-wing , and (i) unconventional UAV [10].

2.4.2 μUAVs

Micro Unmanned Aerial Vehicles (μUAVs) represent a class of unmanned aerial vehicles that are compact and lightweight enough to be carried by an individual and launched by hand without requiring a runway [259, 260, 261]. They fall between the size of Micro Air Vehicles (MAVs) and larger UAVs that cannot be hand-launched. The configurations of μUAVs are diverse, and they can be classified into several categories:

HTOL and VTOL μUAVs: HTOL and VTOL μUAVs can be launched by hand and do not need a runway. They exhibit configurations similar to larger UAV models but are smaller and lighter [262, 263, 264, 265].

Hybrid Model μUAVs: Hybrid models include tilt-wing, tilt-rotor, tilt-body, and ducted fan μUAVs. These designs combine features of both VTOL and HTOL, providing versatility in flight modes [266, 267].

Helicopter μUAVs: Helicopter μUAVs maintain the vertical take-off and landing capability but are smaller and more portable. They can be carried by an individual and launched by hand [268, 269, 270].

Ornithopter and Ornicopter μUAVs: Ornithopter μUAVs mimic bird flight by flapping their wings. The concept of flapping wings dates back to ancient Greek legends and has been explored by inventors like Leonardo da Vinci. Ornicopters are helicopters without tail rotors, utilizing wing flapping for lift and thrust [271, 272].

Cyclocopter μUAVs: Cyclocopters or cyclogyros are μUAVs with cycloidal rotors, resembling a paddle wheel with airfoils. They generate lift and thrust by rotating around a horizontal axis, enabling vertical take-off, landing, and hovering [273, 274, 275].

2.4.3 MAVs:

Micro Air Vehicles (MAVs) are small, lightweight unmanned aerial vehicles with a length smaller than 100 cm and a weight lower than 2 kg. They are classified into nine categories based on their design and capabilities (Figure 2.3) [276, 277, 278].

Figure 2.3: Different types of MAVs, (a) fixed wing, (b) flapping wing, (c) fixed/flapping-wing, (d) rotary wing, (e) VTOL, (f) ducted fan, (g) tilt-rotor, (h) helicopter, (i) unconventional, (j) ornicopter [10].

Fixed Wing MAVs: Consist of rigid wings, fuselage, and tails, using a motor and propeller for propulsion. Suitable for various operational environments, including jungle, desert, urban, maritime, mountains, and arctic environments. Covert, low radar cross-section, and difficult to detect due to small dimensions [279, 278, 280].

Flapping Wing MAVs Designed in three classes: MAV inspired by birds, NAV inspired by insects, and PAV inspired by organisms between small birds and large insects. Flexible and lightweight wings mimic bird and insect flight for improved aerodynamic proficiency and flight stability. More complex aerodynamics compared to fixed and rotary wings [281, 282, 283, 284].

Fixed/Flapping-Wing MAVs Hybrid designs using fixed wings for lift and flapping wings for propulsion. Increased efficiency, mechanically and aerodynamically balanced platform, and reduced stall over the fixed wing [285, 286, 287].

Rotary Wing MAVs Rotary Wing MAVs have rotating blades or propeller-based systems that allow them to hover and provide maneuverability in confined spaces. They can fly horizontally, vertically and hover in a fixed position. Various configurations include mono-copters, twin-copters, tricopters, quad-copters, penta-copters, hexa-copters, octo-copters, deca-copters, and dodeca-copters [285, 288, 289].

2.4.4 NAVs

Nano Air Vehicles (NAVs) are extremely compact and lightweight drones, with a maximum wing span of 15 cm and a weight less than 50 g, as part of a program initiated by DARPA. These diminutive drones have a range of less than 1 km, operate at altitudes around 100 m, and come in various configurations including fixed wings, rotary wings, and flapping wings. The NAVs program aims to explore the capabilities of these nano-sized aerial vehicles for applications requiring small-scale, highly maneuverable platforms [290, 291, 292].

2.4.5 PAVs

The emergence of Pico Air Vehicles (PAVs) has marked a significant advancement in drone technology, with researchers focusing on insect-sized designs. Characterized by their small size and light weight, PAVs fall into two main categories: quadrotors and flapping wings. The latter has attracted particular attention due to the impressive flight capabilities observed in flapping insects. Pioneering projects such as the RoboBee initiative aim to design and manufacture these tiny drones, opening up new possibilities for micro-aerial technology. Inspired by nature, these insect-sized drones represent a unique and promising frontier in the field of unmanned aerial vehicles (Figure 2.4) [293, 294, 295].

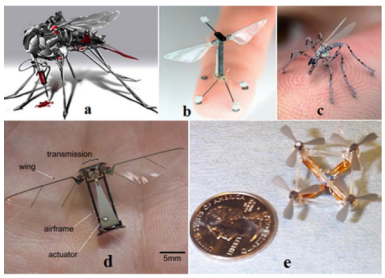

Figure 2.4: Different types of PAVs , (a, b, c, and d) flapping wing, and (e) quadrotor [10].

2.4.6 Bio-drones

In the pursuit of advanced reconnaissance and patrolling capabilities for civil and military applications, the focus has shifted to micro drones due to their smaller size and weight [296, 297]. Inspired by nature, two main approaches have emerged: taxidermy bio-drones and live bio-drones. Taxidermy bio-drones involve using the preserved bodies of animals, such as cats, rats, and birds, as structural components integrated with robotics (Figure 2.5 2.6) [298, 299]. Live bio-drones leverage advancements in radio systems, digital circuits, and neurophysiology studies to control the flight of living birds and insects [300]. Researchers have successfully implanted electronic chips in pigeons' brains for remote control, equipping them with sensors like GPS and cameras for autonomous missions. These innovative approaches offer unique alternatives for reconnaissance and patrolling tasks.

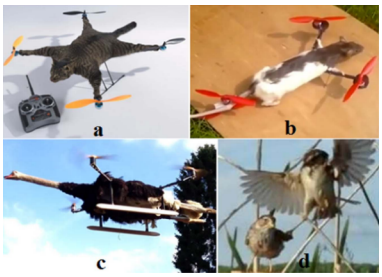

Figure 2.5: Taxidermy bio-drones (a) Orvillecopter, (b) Ratcopter, (c) OstrichCopter, and (d) Robosparrow [10].

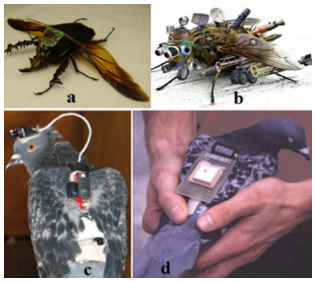

Figure 2.6: Live bio-drones (a) controlled beetle, (b) schematic of controlled insect, (c and d) controlled pigeon [10].

2.4.7 Hybrid UAVs

Hybrid UAVs are unmanned aerial Vs that use two or more energy sources to power their flight propulsion system. They can combine the advantages of different types of UAVs, such as fixed-wing, rotary-wing, and multi-rotor, to achieve longer endurance, faster speed, and greater versatility. Hybrid UAVs can be used for various applications, such as surveillance, reconnaissance, mapping, delivery, and disaster relief [301, 302].

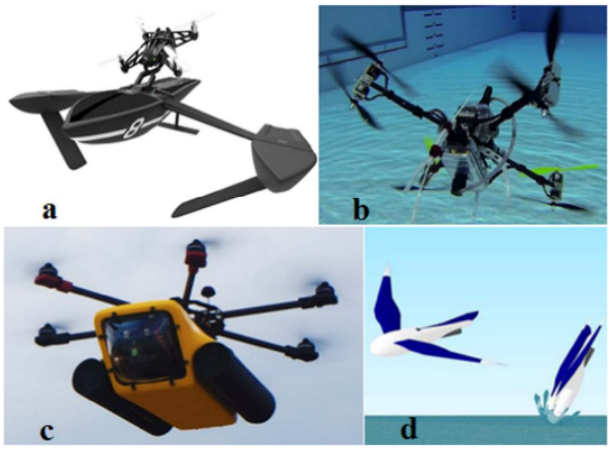

Figure 2.7: Air-water hybrid drones: (a) Parrot Hydrofoil, (b) Rutgers University drone, (c) HexH20, and (d) AquaMAV [10]

2.5 Applications of Drones

Drones find extensive applications in both civilian and military settings, operating in diverse environments such as outdoor and indoor spaces [303, 304, 305]. They are equipped with various sensors and cameras for intelligence, surveillance, and reconnaissance missions. The categorization of drone applications can be based on mission type (military/civil), flight zone (outdoor/indoor), and environment (underwater/on water/ground/air/space) [306] (Figure 2.8).

In daily life, drones have over two hundred potential applications, spanning areas like search and rescue, environmental protection, mailing and delivery, exploration of oceans or other planets, and various other uses. These drones offer a swift overview of target areas without endangering human lives [307]. Micro drones, due to their compact size, are suitable for reconnaissance inside buildings, providing insights in scenarios such as battlefield situations. Equipped with infrared cameras, drones can capture images even in darkness [308, 309]. Small drones are currently essential for inspecting buildings in military contexts, carrying specialized sensors to detect biological, nuclear, chemical, or other threats. The subsequent discussion delves into some of the civilian applications of drones [310].

2.5.1 Mining Industry

The mining industry has witnessed a significant transformation with the integration of drone technology into its operations. Drones have become increasingly essential tools for routine tasks in both surface and underground mining activities [11].
Drones are deployed in various capacities across the mining lifecycle. In surface mining operations, drones are employed for tasks such as surveying, mapping, and monitoring [311]. They provide high-resolution aerial imagery, 3D models, and topographical data, aiding in accurate surveying

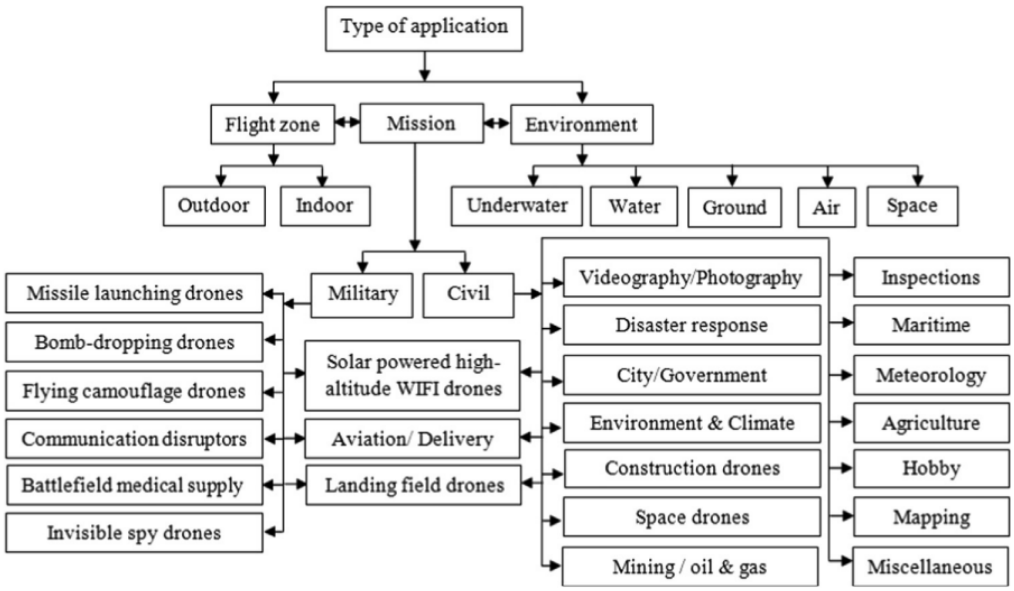

Figure 2.8: Classification of drones' applications [10].

and resource estimation. Additionally, drones assist in tracking changes in the landscape over time, enabling effective land management and environmental monitoring [11].
In underground mining, drones play a crucial role in addressing challenges associated with safety and data acquisition. They are utilized to inspect tunnels, shafts, and other subterranean structures, minimizing the need for manual inspections in hazardous environments. Drones equipped with advanced sensors and cameras facilitate the collection of real-time data, contributing to improved decision-making processes for mine operators [312].

Drone Technology Applications in the Mining Industry

Drones are valuable assets in the mining industry, providing two essesntial advantages [312]. Firstly, equipped with various sensors, drones enable swift inspections, vital for both emergency situations and hazard identification. Secondly, drones are instrumental in inspecting and unblocking box-holes and ore-passes. Their applications extend to blockage inspections, explosive handling, and package delivery within mining environments. Lee and Choi have systematically categorized drone applications in the mining industry across surface, underground, and abandoned mines, as outlined in Table 2.10 [15].

Applications of Drones in Surface Mining

Mines, often located in vast and remote mountainous regions, pose a challenge for effective monitoring due to their remote locations, requiring significant manpower [313]. Traditional methods of mine monitoring are acknowledged to be both time and cost intensive [314]. In

Surface Mine	Underground Mines	Abandoned Mines
Mine operation	Geotechnical characterization	Subsidence monitoring
3D mapping	Rock size distribution	Recultivation
Slope stability	Gas detection	Landscape mapping
Mine safety	Mine rescue mission	Gas storage detection
Construction monitoring		Acid drainage monitoring
Facility management		

Table 2.10: The applications in mining [15].

addressing these challenges, drones are emerging as valuable tools for monitoring (Figure 2.9), surveying and mapping mine environments [313]. Their application ranges from monitoring mining activities to detecting topographic changes in the mining area. This not only facilitates informed mine planning, but also enhances safety measures through the acquisition of valuable data [313]. Drones therefore offer a practical solution to the logistical difficulties associated with traditional monitoring methods in the mining industry.

Drones play a pivotal role in surface mining operations, addressing various challenges and improving operational efficiency. In the work of Raval et al. [315], drones are used to monitor socio-environmental aspects, enabling the detection of potential problems. Furthermore, in areas where direct access is impractical using conventional methods, drones serve the crucial function of measuring deformations in structures and surfaces, as highlighted by Gruchlik et al. [316]. This is particularly valuable when continuous or quasi-continuous measurement is essential.

Moreover, the applications of drones extend to the monitoring of mining activity and the production of precise cartographic products, including land cover maps with a spatial resolution of 4-10 cm and an impressive overall accuracy of 91% [317]. The use of drones in surface mining not only generates high-resolution images but also significantly reduces the time and energy expended on missions requiring such imagery by over 50%.

Furthermore, drones in mining operations provide real-time data, enabling the swift identification and mitigation of hazards, expediting data collection processes, and facilitating the dissemination of accurate maps and models to stakeholders [311]. Additionally, drone-based hyperspectral analysis, as explored by Robinson et al. [318], proves instrumental in supporting soil and water geochemical investigations at both active and historic mining sites, presenting advantages in data acquisition efficiency and extensive area coverage.

Application of drones in Underground Mine

Despite the continuous advancements in drone technology, their utilization in underground mines has been constrained (Figure 2.10), primarily due to the inherent challenges associated with this demanding environment [319]. The harsh conditions within underground mines, marked

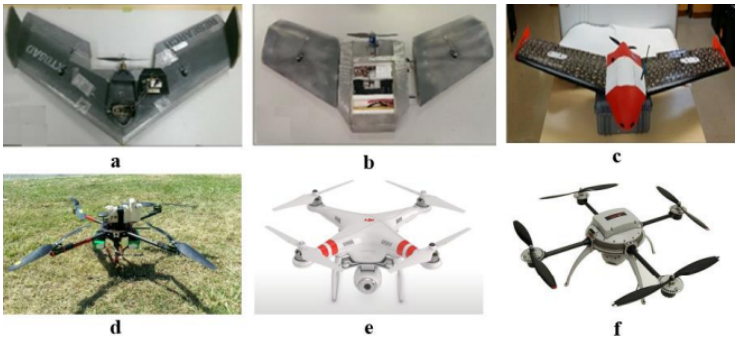

Figure 2.9: Views of the some utilized drones in surface mining (a) Teklite, (b) GoSurv, (c) Swamp Fox, (d) Quadcopter, (e) Phantom 2 Vision+, (f) Aeryon Scout [11].

by confined spaces, limited visibility, fluctuating air velocity, high dust concentration, and the absence of a reliable wireless communication system, present formidable obstacles for drone operations. Flying drones in these underground working areas becomes a complex task for operators, compounded by the impracticality of reaching inaccessible and perilous locations [319]. However, the potential applications of drones in underground mines are extensive, particularly in enhancing health and safety measures. These applications encompass surface roughness mapping, analysis of rock mass stability, ventilation modeling, detection of hazardous gases, and monitoring for potential leakages [320, 319]. Despite the current limitations, the diverse applications suggest that the integration of drone technology holds significant promise for improving safety and operational efficiency in the challenging environment of underground mines.

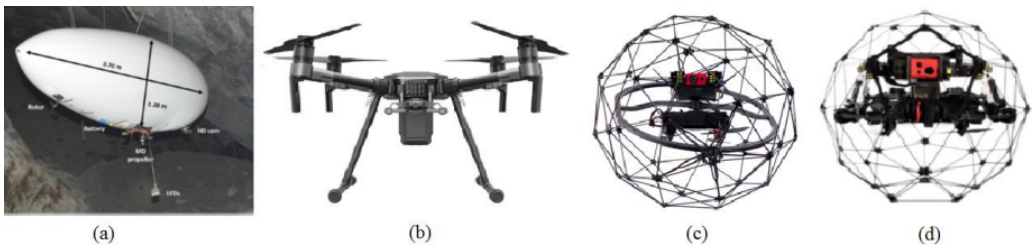

Figure 2.10: Commonly used drones in underground mines (a) Zeppelin, (b) DJI M210, (c) ELIOS 1 [68], (d) ELIOS 2 [11].

2.5.2 Agriculture and Crop Monitoring

The technical analysis of UAVs in precision agriculture reveals their diverse applications, including crop monitoring, crop height estimation, pesticide spraying, and soil and field analysis [321]. The hardware implementations of UAVs depend critically on factors such as weight, flight range, payload capacity, configuration, and cost [322]. Although initially perceived as expensive toys, drones have gained recognition in the agricultural sector for their autonomous flight capabilities, facilitated by dedicated software for flight planning and deployment with GPS [323, 324, 325]. Drones offer advantages over large aircraft such as high spatial resolution, rapid

turnaround, low operating costs and ease of use. These features are particularly beneficial in precision agriculture, where large areas need to be monitored and analyzed efficiently. The use of aerial vehicles is made possible by the miniaturization of compact cameras and other sensors, including infrared and sonar, which contribute to the effectiveness of agricultural operations [323, 324, 325].

Soil and Field Analysis

Drones play a crucial role in the initial stages of the crop cycle, generating precise 3-D maps for early soil analysis. These maps aid in planning seed planting patterns, and post-planting, drones continue to contribute by providing essential data for irrigation and managing nitrogen levels effectively [323].

Planting

Innovative startups have introduced drone planting systems that boast an impressive 75% uptake rate while reducing planting costs by a substantial 85%. These systems use pods to shoot seeds and plant nutrients into the soil, ensuring that plants receive all the nutrients they need to survive. In particular, crop protection UAVs can effectively apply cotton defoliants with a twice-spray strategy without significantly affecting seed cotton yield or fiber quality in Xinjiang [326]. The [327] method, which incorporates the Dragonfly Algorithm, effectively schedules UAV operations in agricultural plant protection, reducing human intervention and improving autonomous production systems. In addition, China's plant protection UAVs improve the accuracy and environmental friendliness of agricultural operations, providing new research opportunities for improved efficiency, environmental friendliness and accuracy [328].

Crop Spraying

Drones are adept at scanning the ground and precisely spraying liquid, adjusting their distance from the ground and spraying in real time for uniform coverage. This results in increased efficiency and a significant reduction in the amount of chemicals entering groundwater. Experts estimate that drone-based aerial spraying can be completed up to five times faster than traditional machines. [323].

Crop Monitoring

The vastness of fields and the inefficiency of crop monitoring pose significant challenges in agriculture. These challenges are exacerbated by unpredictable weather conditions, resulting in increased risk and higher field maintenance costs. [323].

Irrigation

Equipped with hyper-spectral, multispectral, or thermal sensors, drones play a pivotal role in identifying dry or problematic areas within a field. As the crop grows, drones enable the calculation of the vegetation index, describing the crop's relative density and health. Additionally, they reveal the heat signature, indicating the amount of energy or heat emitted by the crop [323].

2.5.3 Search and Rescue Operations

Search and Rescue (SAR) is a vital activity that aims to save lives in emergency situations, such as natural disasters, accidents, or conflicts. Depending on the environment and the scenario, SAR can be classified into four types: maritime, combat, urban, and wilderness [329]. Maritime SAR is one of the most challenging types, as it involves finding and rescuing people who are lost or in distress at sea, often in harsh and unpredictable conditions. UAVs can be a valuable resource for maritime SAR, as they can cover large areas, provide aerial views, and operate in remote or dangerous locations, without risking human lives or requiring expensive assets [330]. However, using UAVs for maritime SAR also poses several challenges, such as the limited fuel capacity of commercial UAVs, the uncertainty in the location and status of the survivors, and the need for autonomous control and coordination of multiple UAVs and service stations [331, 329]. Researchers have proposed different approaches to address these challenges and optimize the performance of UAVs for maritime SAR. One approach is to use Mixed-Integer Linear Programming (MILP) models to plan the optimal deployment and routing of UAVs, taking into account the fuel constraints, the survivor uncertainty, and the possibility of refueling at autonomous service stations[331, 329]. This approach can find the best solution for a given scenario, but it may require high computational power and time, and it may not be able to adapt to dynamic changes in the environment or the mission. Another approach is to use UAVs with rotary wings, which have the advantage of being able to fly vertically and horizontally, as well as hover at desired positions, for maritime SAR operations. This approach employs algorithms to systematically capture photographs of potential survivor locations, using a state-of-the-art object detection network to perform real-time rescue target detection on-board the UAV, with minimal human intervention. This approach can increase the vehicle autonomy and search range, but it may also face challenges such as the limited payload and endurance of rotary wing UAVs, the reliability and accuracy of the object detection network, and the communication and coordination with other UAVs and rescue assets.

2.5.4 Disasters

Recognizing and responding to disasters in time is very important to assess the risk and move as quickly as possible despite the region's topography and the type of the accidents and

the way to deal with them. Generally, UAVs work as a cooperative devices to identIFy risks and give a comprehensive view of the danger. In [332], the authors proposed a solution to connect drones for disaster and emergency cases with buses used as edge computing device to make a portable base station that serves as a temporary host. The solution proposed in [333], allows drones to provide accurate and fast information in the afflicted areas. In [334], the authors propose a fleet of autonomous cooperative drones capable self-organization. The works done by [335] allow to improve the effectiveness of locating the affected people by finding their actual location and number by detecting the WIFi of their mobile phone with the drone. The authors in [336] proposed an adaptive forwarding area based routing algorithm and which uses geographic information of flooding.

2.5.5 Environmental Monitoring and Conservation

Unmanned Aerial Vehicles have become invaluable tools for environmental monitoring due to their versatility, mobility, and ability to access remote or hazardous areas (Figure 2.11). Drone-enabled IoT relay systems can provide high-speed data collection for remote environmental monitoring in remote areas without public networks [337].

Figure 2.11: Application of drones' in environmental protection [10].

Advanced Sensor Technologies: Drones are equipped with increasingly sophisticated sensors, including multispectral and hyperspectral cameras, LiDAR (Light Detection and Ranging), and thermal imaging. These sensors enable detailed data collection for various environmental parameters, such as vegetation health, topography, and temperature [338, 339, 340, 341].

Machine Learning and Data Analytics: Integration with machine learning algorithms allows for the automated analysis of vast amounts of data collected by drones. This aids in the identification of patterns, species recognition, and the extraction of meaningful insights from environmental datasets [342, 343].

Autonomous Navigation and Swarming: Advances in autonomous navigation systems enable drones to operate in complex environments with minimal human intervention. Swarming technology allows multiple drones to collaborate, enhancing coverage and data collection efficiency over large areas [344, 345, 346, 347].

Real-time Monitoring and Decision Support: Drones provide real-time data, enabling quick response to environmental changes. This is particularly valuable in disaster management, anti-poaching efforts, and monitoring events such as wildfires. Decision support systems integrate drone data to aid conservation planning and interventions [348, 349, 350].

Customized Applications for Conservation: Tailored drone applications have been developed for specific conservation needs, such as tracking wildlife migration, monitoring marine environments, and assessing the health of coral reefs. These applications help address the unique challenges faced by different ecosystems [351, 352, 353].

2.5.6 Mailing and delivery

In recent times, the concept of drone delivery services has captivated the attention of various global companies. Noteworthy examples include Amazon and Google in the United States [354, 355], as well as DHL postal service in Germany [356]. Numerous other companies are also leveraging drone technology to efficiently transport packages to customers. The delivery process involves specialized drones that execute vertical take-offs and landings, equipped with the precise customer address to facilitate cargo transport. Refer to (Figure 2.12) for a visual representation of these delivery drones.
The articles collectively explore innovative strategies to enhance the efficiency and effectiveness of drone-based parcel delivery systems. Ulmer and Thomas [357] focus on the integration of drones and vehicles, demonstrating that combining these technologies, along with geographical districting, can significantly improve same-day delivery performance. Das et al. [358] propose a synchronized routing mechanism for drones and trucks in package delivery logistics, aiming to maximize customer service and minimize travel costs. Kornatowski et al. [359] introduce Dronistics, an intuitive and secure system for last-centimeter person-to-person delivery using cargo drones, particularly designed for short-distance deliveries to inexperienced users. Huang et al. [360] present an inventive approach where drones can leverage public transportation vehicles, expanding the delivery area and reducing costs. Finally, Liu et al. [361] address uncertain delivery demand scenarios by formulating a two-stage stochastic programming approach and a hybrid genetic algorithm for optimal drone fleet deployment, resulting in cost reduction. These studies collectively contribute valuable insights to the evolving field of drone-based parcel delivery logistics.

Figure 2.12: Application of drones'in mailing and delivery [10].

2.5.7 Space drones

space drones are small unmanned aerial vehicles designed for planetary exploration, data collection, and surveillance, with applications in climate science, space research, and environmental research. Space drones are designed and fabricated to perform planetary exploration, offering advantages over other approaches like telescopes and satellites [362].
Drones offer distinct advantages over other robotic systems in planetary exploration, prompting the development of specialized drones capable of flying and executing missions in extraterrestrial environments. NASA, for instance, is actively involved in constructing drones tailored for planetary exploration [363, 364]. Various types of drones have been specifically designed and manufactured to carry out missions in space and explore celestial bodies [363, 364, 365, 366]. (Figure 2.13) illustrates some examples of these space drones. It is crucial to highlight that the design and fabrication of space drones must be intricately tailored to the unique characteristics of the target environment. Notably, the gravitational conditions on Mars necessitate adjustments in the weight of drones, experiencing a reduction of 61.5% compared to their weights on Earth [367].

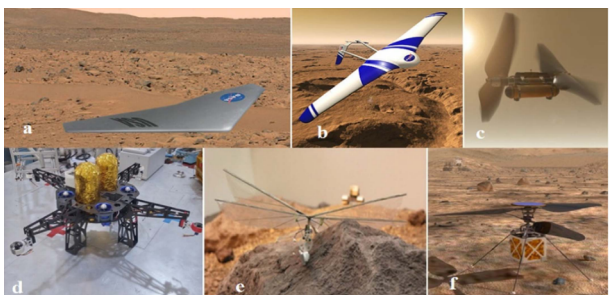

Figure 2.13: Application of drones' in space [10].

2.6 Challenges and Regulations

Challenges and regulations surrounding drones have become increasingly prominent as the use of UAVs continues to grow. These challenges span various domains and are influenced by technological, legal, and societal factors. Some notable challenges include:

Privacy Concerns Drones, especially those equipped with high-resolution cameras, have raised significant privacy concerns. Here are some key points:

- **Invasion of Personal Space:** Drones can capture images and videos from great heights, potentially invading personal spaces without consent [368].
- **Collection of Personal Information:** There are concerns about drones recording and collecting personal information without permission, which infringes on privacy rights [368].
- **Data Security:** Drones are primarily data collection devices. Many parties potentially have access to drone-captured data, raising concerns about sensitive data and images ending up in the wrong hands [369, 370].
- **Surveillance:** There are valid concerns about drones potentially being used as surveillance vehicles. Without responsible and ethical regulation, law enforcement agencies may use drones for surveillance unbeknownst to the public, potentially creating a chilling effect in public spaces and paving the way for discriminatory targeting [371].
- **Cybersecurity:** Drones are a type of connected device, collecting and sending data for analysis. This creates implications for the safety and hackability of the devices [372].

Airspace Management Integrating drones into existing airspace while ensuring safety and avoiding collisions with manned aircraft poses a significant challenge. Developing effective air traffic management systems for both recreational and commercial drone use is crucial [373].

Noise Pollution Drones can generate noise disturbances, particularly in urban areas. Managing the noise impact on the environment and communities is a concern that needs attention, especially as drone usage increases [374].

Limited Battery Life Most drones have limited battery life, restricting their flight duration. This constraint poses challenges for applications requiring extended operation times, such as surveillance, monitoring, and delivery services [375].

Traffic and Obstacle Detection Without human eyes to help, a drone needs to look out for itself. Technologies like the IntuVue RDR-84K Radar can guide the drone around other air traffic and obstacles [368].

Navigation When GPS signals are not available, drones need a different way to find position. An Inertial Measurement Unit can provide the navigation system with precise information [368].

Communications Drones need to stay in contact from the other side of a hill, or from half a world away. Small UAV SATCOM can help with this [368].

Drones Regulations

- Altitude Control: Drones are restricted from ascending beyond 120 meters (400 feet) above ground level [376].
- Safety Buffer: A minimum distance of 30 meters must be maintained between drones and other individuals [376].
- Simultaneous Flight: The simultaneous flight of more than one drone is prohibited [376].
- Visual Line-of-Sight: Drones must remain within the operator's visual line-of-sight [376].
- Airport Proximity: Proximity to airports is strictly regulated, with a minimum distance of 10 kilometers [377].
- Safe Distances: Drones are not permitted to approach closer than 50 meters to people, buildings, or roads [378].
- Nighttime Restrictions: Nighttime flights are prohibited for drones [378].
- Airspace Restrictions: Restricted airspace is off-limits for drone operations [378].
- No-fly Zones: Flying near other aircraft, especially in the vicinity of airports, is strictly prohibited [378].
- Event and Emergency Restrictions: Overflight of groups of people, stadiums, sporting events, and emergency response efforts, such as fires, is not allowed [378].
- Sobriety Requirement: Operating drones under the influence is strictly prohibited [378].

2.7 Conclusion

In conclusion, the exploration of UAVs has revealed a diverse landscape encompassing various categories and types of drones, each designed for specific purposes. The classification of drones based on performance characteristics and mission aspects has provided a comprehensive overview, ranging from UAVs and µUAVs to Bio-drones and Hybrid UAVs. Additionally, the exploration of drone applications has unveiled their versatile role across industries, including mining, agriculture, search and rescue, disaster management, environmental monitoring, and even space exploration.

However, this chapter has also delved into the significant challenges and regulations associated with the proliferation of drones. Privacy concerns, airspace management, noise pollution, limited battery life, and various technical obstacles pose hurdles that demand careful consideration. As the drone industry continues to evolve, addressing these challenges will be pivotal to ensuring the responsible and ethical integration of drones into our daily lives.

Looking forward, the chapter has highlighted emerging trends in the drone industry, including integration with smart cities, advancements in urban air mobility, the potential for AI-driven decision-making, and the continued miniaturization and increased affordability of drone technology. These trends underscore the evolving nature of UAVs and their potential to transform various aspects of our society.

In summary, while the integration of drones presents exciting possibilities for innovation and efficiency, a proactive approach to addressing challenges and adhering to regulations is imperative. The future trends indicate a continued evolution towards more sophisticated and accessible drone technology, promising a dynamic landscape that necessitates ongoing vigilance and adaptability in the realm of Unmanned Aerial Vehicles.

Part II

Propositions

Chapter 3

Drone Recovery System

3.1 Introduction

Unmanned aerial vehicles, commonly known as drones, have garnered significant attention in recent times for their potential contributions to public safety, emergency response, disaster management, as well as routine tasks such as surveillance and object tracking. Drones boast various capabilities that rival those of humans and other machinery. Their agility and swift tracking abilities enable them to navigate challenging terrain, transmit crucial information swiftly, and assess hazardous situations with precision.

However, to maintain optimal speed and efficiency, drones must be compact and lightweight. This requirement imposes constraints on the size and number of components used, necessitating constant communication with a base station for data transmission and reception due to limited storage and processing capabilities. Consequently, a reliable connection, robust protection, and real-time data transmission become imperative.

The integration of IoT applications across diverse sectors such as transportation, construction, healthcare, and public safety has significantly enhanced communication, aiding specialists in performing tasks more effectively and accessing precise information promptly. Drones are intricately linked within IoT architectures, yet continuous communication with ground stations is susceptible to disruptions caused by factors like drone movement and environmental conditions such as wind, resulting in network interruptions.

Such communication failures can incapacitate drone operations, hindering the transmission of directives from base stations and jeopardizing mission-critical data. Instances of drones suddenly losing connectivity and plummeting have been reported, highlighting the urgency of addressing these challenges. Furthermore, the hierarchical structure of IoT architectures, particularly the reliance on fog or edge nodes for device communication and security, presents obstacles to connecting drones with alternate nodes when they move beyond their designated fog areas.

This contribution aims to tackle these issues by proposing a novel protocol designed to restore drone connectivity in the event of signal loss or departure from designated areas.

Requirements	Method	Contribution
Drone network	Cellular connectivity	[379] [380] [381] [382]
	Decentralized control	[383]
	Edge computing infra structure	[333]
	SHERPA network	[384]
	Internet of drones	[385] [386]
	Service-oriented cloud	[385]
Security	ArtIFicial neural network (ANN) based solution	[380]
	Techniques of encryption WiMAX	[384]
	Linearly homomorphic authenticated encryption	[387]
	Bose-Chaudhuri-Hocquenghem encoding	[388]
	Quantum key distribution and visual cryptographic	[389]
	Encryption with AES/RSA	[390]
Communication technologies	Third Generation Partnership Project (3GPP), LTE connected drones	[379]
	Vehicular Ad Hoc Network(VANET)	[333]
	Micro Air Vehicle Link MAVLink-enabled drones	[385]
	WiMAX	[384]
	Bluetooth antennas	[391]
	Heterogeneous approach	[383]
	3G communication	[382]
	Free Space Optics	[392]
	WIFi	[393]
Information management	Predict packet transmission rate with Support Vector Machine with Quadratic Kernel(SVM-QK)	[394]
	Optimize the data collection time with Reinforcement learning-based Spatial Crowdsensing Algorithm (RSCA)	[395]
	Adaptive Computation Offloading Drone System	[396]
Energy consumption	Localized Altitude Scheduler	[397] [398] [399] [400]

Table 3.1: Taxonomy of recent researches

3.2 Related work

Nowadays, drones are being used in various military and civilian systems. However, their integration into our daily lives depends on their effectiveness and performance. In this contribution, we group the most important factors that affect the performance of any system that relies on autonomous drones into five categories: network, security, communication technologies, information management, and energy consumption. Table 3.1 summarizes the most relevant papers for each category.

3.2.1 Security

Security systems and protocols are introduced and integrated to protect information as well as devices from piracy. The protection level of the devices varies according to their field of use. When the drone works as a daily civilian device, such as in emergencies and disasters, it only collects information related to accidents, and therefore existing protection systems in communication technologies may satisfy the security requirements. But in the case of monitoring, tracking, and stalking, the focus is on the quality of information transmitted by the drone [401], and thus it is important to establish an effective and strong protection protocol against piracy [402].

3.2.2 Disaster

Recognizing and responding to disasters in time is very important to assess the risk and move as quickly as possible despite the region's topography and the type of the accidents and the way to deal with them. Generally, UAVs work as a cooperative devices to identIFy risks and give a comprehensive view of the danger. In [332], the authors proposed a solution to connect drones for disaster and emergency cases with buses used as edge computing device to make a portable base station that serves as a temporary host. The solution proposed in [333], allows drones to provide accurate and fast information in the afflicted areas. In [334], the authors propose a fleet of autonomous cooperative drones capable self-organization. The works done by [335] allow to improve the effectiveness of locating the affected people by finding their actual location and number by detecting the WIFi of their mobile phone with the drone. The authors in [336] proposed an adaptive forwarding area based routing algorithm and which uses geographic information of flooding.

3.2.3 Communication Technologies

The type of network used strongly depends on the environment and can be either centralized or decentralized. However, decentralization is widely preferred right now due to the emergence of

the Internet of Things [403] and the use of the Fog and Edge computing paradigms [404][405].

Much research has focused on the quality and distance of information transmission, as it is the most important feature of drones, ability to travel long distances and send information in real time. In this regard, numerous communication technologies have been proposed for drones, such as Long-Term Evolution(LTE), Worldwide Interoperability for Microwave Access (WiMax), Wireless Fidelity (WIFi), and ZigBee.

Drones have also been used to simplify communication in non-covered areas. In [385], the authors proposed a path planner for drones using MAVLink-enabled drones to create the Internet of Drones. Also, microaerial vehicles have been proposed as an alternative to humans in space exploration, which has created many challenges such as size and the amount of stored energy [406]. The authors in [393] address the problem of synchronization and coordination of drones and propose to use WIFi to achieve their tasks. To manage the interference in drone networks, the works done in [407] provide an appropriate allocation scheme of channel resources for drone communications with stochastic geometry analysis of interference.

The direct connection to the base station makes the UAVs space-limited and also increases the information transmission time of the entire group of cooperating UAVs. To deal with this, the authors in [408] propose a dedicated network instead of a commonly used network to solve those problems and give a more effective means of communication.

Usually, using a single drone is not enough for most missions. For this, authors in [393] suggested leading missions with one drone leader connected by an AdHoc network while the rest of the group would be self-driving and connected to the leader via Wi-Fi.
This solution uses the leader as a link point to connect the base station with the rest of the drones. Therefore, the leader is exposed to hacking and damage, giving rise to the loss of information and damage to the entire network with only a few seconds of interruption.

3.2.4 Drone network

Drones can also be used to connect remote or damaged areas after a disaster where there is no communication infrastructure[409]. In [410], the authors propose using autonomous flight wireless nodes with drones to connect remote areas. The well-known dedicated Vehicle Network (VANET) suffers from disconnections due to vehicle instability and varying distances between them [411]. To solve this issue, [412] proposes using vehicle-drone hybrid vehicular ad hoc network infrastructure to transfer information between vehicles effectively. However, the drone network uses a greedy algorithm to optimize mobile data collection time [395]. To address this, [413] proposes developing a connection infrastructure with self-driving robots controlled by multi-swarm Unmanned Aerial Vehicles (UAVs). Another solution proposed by [394] is to predict packet transmission rates within the network using machine learning methods such as Support Vector Machine with Quadratic Kernel (SVM-QK) to optimize transmission time. Despite the existing

UAV communication-related articles, the diversity between fixed and mobile devices in the IoT environment requires special treatment. Additionally, the proposed papers in the state of the art relied on specIFic platforms to control and monitor drones. However, considering a decentralized network with Fog nodes, these platforms are vulnerable to communication failures at any moment without any protocols to retrieve lost drones.

3.2.5 Drone recovery

Permanently losing contact with the drone is considered one of the most challenging problems for mobile devices, especially drones, as they are autonomous. Indeed, deviating from their designated area due to unknown reasons such as winds remains an open problem. The loss of the drone directly affects the system, which can result in the loss of important information or material value. There are solutions to avoid drone loss, such as covering the necessary areas and utilizing temporary edge devices [333]. In addition, drones have limited battery duration [396], so it relies on accelerating the drone's response time and offloading the management module via Multipath Transmission Control Protocol (MPTCP) to increase its uptime.

Previous state-of-the-art methods did not propose a recovery mode to ensure the completion of the drone's mission, and most of them act after the crash. State-of-the-art methods are based on the following three solutions:

- **GPS tracking:** Most drones are equipped with GPS technology, which allows to track the drone's location in real-time. [414, 415, 416, 417, 418, 419, 420, 421, 422]
- **RTH (Return-to-Home)feature:** Most drones have a built-in RTH feature, which allows the drone to automatically return to its takeoff location IF it loses connection with the controller or IF the battery level is low. [423, 424, 425, 426, 427, 428, 429, 430, 431]
- **Sound and light signals:** Some drones are equipped with sound and light signals, which can help locate the drone IF it is lost in a dark or remote area. [432, 433, 434]

3.3 System model

IoT is an architecture for decentralized communication that relies on the principles of Fog and Edge computing. Fog computing ensures a high quality of service (QoS) by addressing four critical aspects: connectivity, reliability, capacity, and delay. Figure 3.1 illustrates the main components of an IoT architecture that leverages Fog computing, consisting of three layers: Devices, Fogs, and Cloud. There are four distinct types of communication that occur within IoT systems.

- **Device to Devices communication:** Refers to the cooperation between a several devices to complete a task.

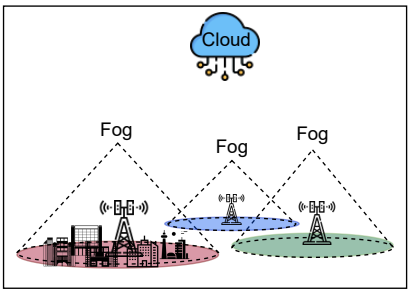

Figure 3.1: IoT architecture

- **Device to Fog communication:** Provide treatment and management of daily information and data close to the used devices.
- **Fog to Fog communication:** Is a type of communication between fog computing nodes. It enables data processing and analysis tasks to be performed closer to the data source, reducing latency and improving system performance.
- **Fog to Cloud communication:** Provide treatment and management of Fogs and big data.

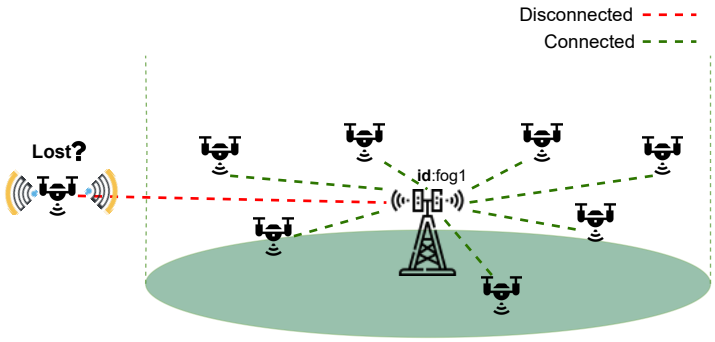

Figure 3.2: Drone disconnection issues

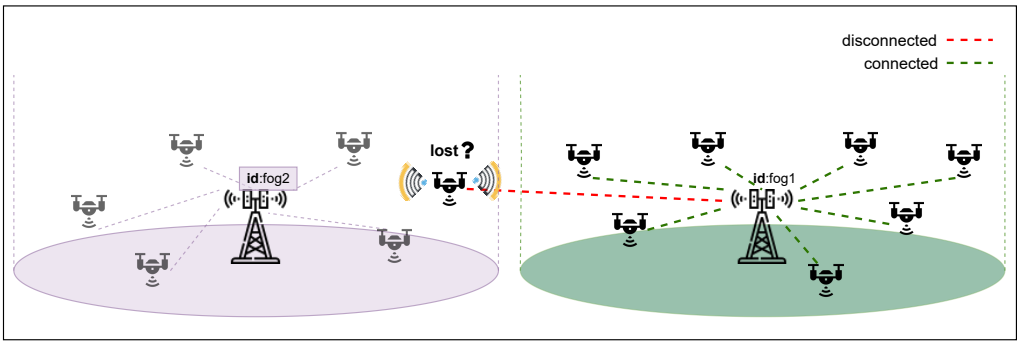

Figure 3.3: Drone connection issues

The standard IoT architecture was proposed based on a fixed device, and the communication between the device and the fog node cannot be interrupted due to the movement of the device outside the range of the fog.Drones are mobile devices that can always fall out of the parent

fog area due to an unexpected event such as the wind (figure 3.2). In that case, the drone cannot communicate outside of its fog parent, and fog nodes cannot communicate without cloud interconnection. To address these issues, we propose to add, in addition to the three communication types cited before, two other communication types, namely, mobile device communication and fog to fog communication.The role of the proposed fog-to-fog communication is to maintain the QoS of the fog computing paradigm by reducing fog-to-cloud communication when a mobile device is lost. Indeed, fog-to-fog communication can provide a big solution to maintaining the performance of IoT devices, especially when it comes to mobile devices. Figure 3.3 shows drones issues with the limitation of fog range and how to recover the lost drone in an IoT system. The Fog receiver should accept a new connection attempt from new devices.

3.4 Proposed recovery protocol

We propose a new protocol to recover lost drones in an IoT environment. It consists of three elements: one role for the drone and two roles for the fog node (Figure 3.4). The system elements work in collaboration to recover the lost drone. The use of the newly introduced **Fog to Fog communication** allows the Fog node to communicate with foreign devices while maintaining the same level of network security. Indeed, the fog filters the messages received in order to accept connection attempts from drones outside the range of their parent fog. To avoid hacking, only the drones reported as lost by the parent fog are accepted.

To recover lost drones, three algorithms were proposed. The execution of the latter starts when a communication interruption is detected. In the following, a detailed description of the proposed algorithm for each element is provided.

Drone: The recovering algorithm (Algorithm 1) is triggered when an interruption is detected by the drone. There are three ways to reestablish the connection. First, the drone tries to reestablish connection with the parent fog. After a given waiting time, if there is no response from the parent fog, the drone goes to the next way. The second way is to try to find any wireless range of neighboring fogs to make a connection, knowing that the drone has no access key. if there is no response from any other Fog, that means that the drone fell in a remote area. The last way is to activate an ad-hoc connection and wait for help.

Fog node: On the fog node side, two algorithms were proposed. The first one (Algorithm 2) is executed when the fog detects a failed connection with a drone. In this case, the fog node takes on the role of main fog; otherwise, the role of fog neighbor is activated. First, the main fog sends a general broadcast to all fog neighbors. In the event of any response from neighbors, the appropriate fog is selected to accept the communication with the lost drone. Otherwise, the Main Fog selects a drone among the others and sends it to the last known place where the

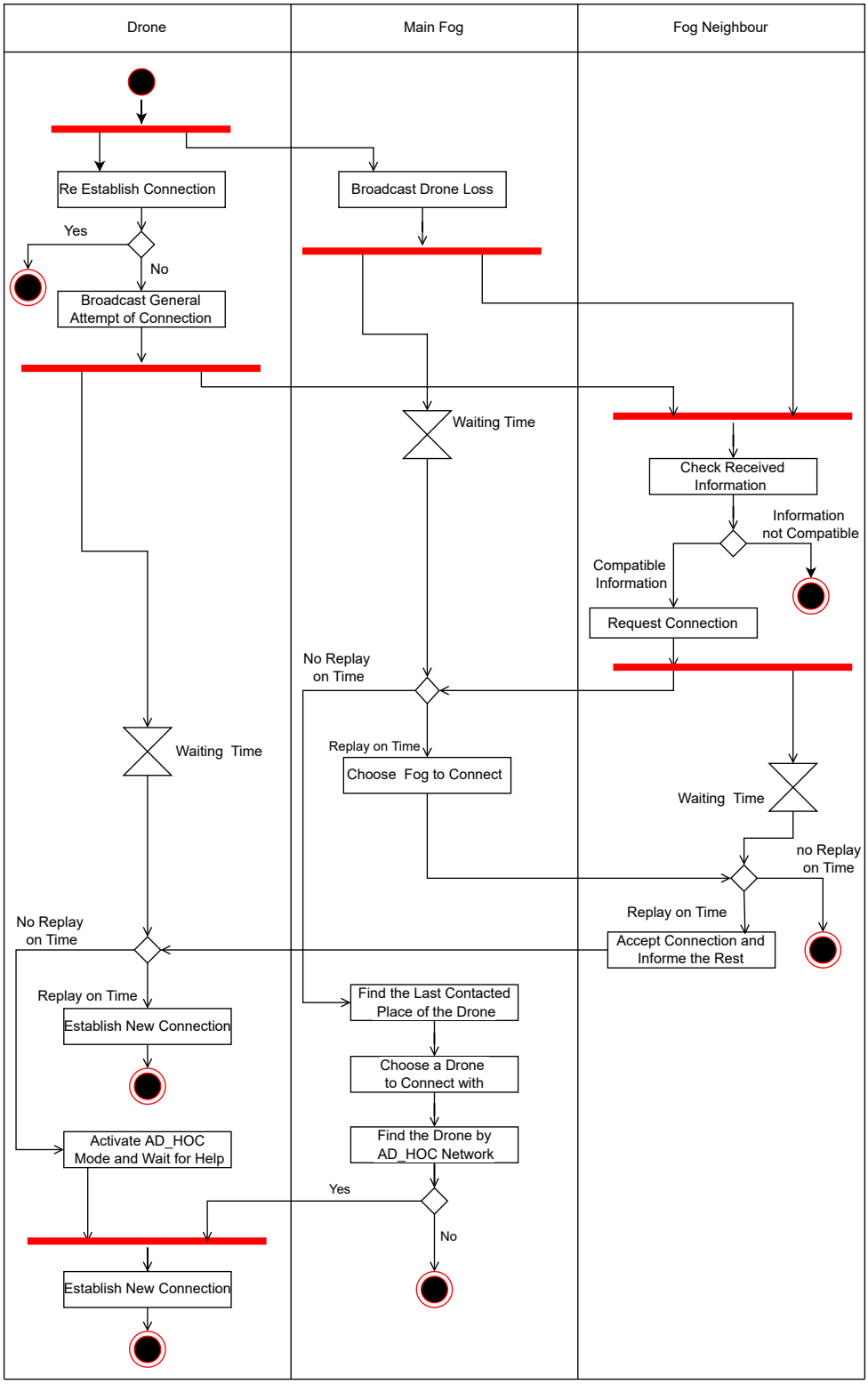

Figure 3.4: Drone recovery protocol

Algorithm 1: LostConnection

```
1: ReEstablishConnection();
2: if fogConnection = true then
3:    go to 18
4: else
5:    BroadCastGeneralAttempt();
6: end if
7: waitForResponse();
8: if acceptation = true then
9:    ReEstablishNewConnection();
10:   go to end;
11: else
12:   ActiveAdHocMode();
13: end if
14: EstablishDroneConnection();
15: if droneConnection = true then
16:   go to 18;
17: end if
18: end.
```

communication was lost. The rescue drone activates an ad-hoc mode to retrieve the lost drone. This strategy makes it possible to broaden the scope of the main fog. It should be noted that the rescue drone never leaves the range of the main fog.

The second algorithm (Algorithm 3) is devoted to the fog neighbors. Its role is to catch the broadcast messages from the main fog and wait for a connection attempt from a drone. The goal is to ensure an indirect connection with the main fog until the recovery of the drone.

Algorithm 2: Main Fog

```
1: broadCastLossDrone();
2: waitForResponse();
3: listC ← ListOfCandidates();
4: if listC = φ then
5:    go to 11;
6: else
7:    electionFog();
8: end if
9: BroadCastWinner();
10: go to 13 ;
11: loc ← lastDroneLoc();
12: electionDrone(loc);
13: end.
```

The time efficiency of the algorithms is determined by the time efficiency of the subsequent

Algorithm 3: Fog neighbor

```
1: info ← ReceivedInformation();
2: if info ∈ tableRequests then
3:    requestconnection(info);
4: else
5:    go to 11;
6: end if
7: res ← waitElectionResponse();
8: if res = myId then
9:    acceptDroneConnection();
10: end if
11: end.
```

functions such as: ReEstablishConnection(), BroadCastGeneralAttempt(), EstablishDroneConnection() and electionDrone(loc). Hence, the upper bound for the time complexity of these algorithms is O(N), where N represents the maximum possible number of steps the algorithm can execute before stopping. Nonetheless, the real time complexity can be significantly lower depending on the specifics of the functions.

3.4.1 Fog to Fog communication scheme

Every fog node in IoT has the capability to send a request or task (known as "job" J_i) to the Fog-Cloud system, which can be for processing, storage, or both. These jobs J_i will come with specific needs that are indicated by a set of two ordered values.

$$RT_i = 2Del_{i,j} \tag{3.1}$$

In cases where Fog2Fog communication is involved, a Fog node Fog_j may choose to assign the job J_i to another Fog node $FogK$ for processing. However, before sending J_i to Fog_k, Fog_j must confirm that Fog_k is available and capable of processing J_i without compromising its ability to process other jobs. Therefore, a three-way communication process between both Fog nodes is necessary to ensure that Fog_k is prepared to receive and process Fog_k from Fog_j. We denote $HS_{j,k}$, k as the time it takes for a handshake to be completed between Fog_j and Fog_k :

$$HS_{j,k} = T\_ACK + ACK \tag{3.2}$$

The time taken to transmit the 2-tuple J_{R_i} from Fog j to Fog_k is represented as T. The duration required for the acknowledgment of the tuple (which confirms the acceptance of Fog_k to process the job) to be transmitted from Fog_k to Fog_j is indicated as T_{ACK}. The time taken for the confirmation to travel from Fog_j to Fog_k is represented by ACK. The size of J_i, the size of the

Algorithm 4: Fog to fog communication

```
1: SumSizei = 0;
2: CL = null; // empty list
3: if (MaxDelAllowedJR1 > THRESHOLD) then
4:    mainFog submits J to the cloud
5: else
6:    for all available Fogi neighboring Fog do
7:       for all Jobj ∈ {J}FCi do
8:          SumSizei+ = SizeJRj;
9:       end for
10:      if (SumSizei ⩽ StorageFCi AND FRT1, i < MaxDelAllowedJR1) then
11:         addFogi to CL;
12:      end if
13:   end for
14:   if (CL is empty) then
15:      mainFog submits J to the cloud;
16:   else
17:      // start handshake
18:      for all Fogi in CL do
19:         mainFog sends JR to Fogi;
20:      end for
21:      while (!TIMEOUT) do
22:         mainFog receives T_ACK from Fogk;
23:         Fogk is added to CL2;
24:      end while
25:      for all Fogi in CL2 do
26:         if (FRT1, i < FRT1, min) then
27:            min = i;
28:         end if
29:      end for
30:      mainFog sends confirmation to the fog willing
31:      to serve J and with the minimum delay
32:      mainFog sends ACK to Fogi;
33:      MainFog submits the job to the fog with the
34:      minimum delay
35:      mainFog submits J to Fogi;
36:   end if
37: end if
```

acknowledgment packets, and the bandwidth of the link can be used to easily calculate all three components.

The roundtrip delay for a job J_i to be submitted to Fog_j, sent to another Fog_k for processing, and returned to the original node that submitted the job is represented as $FRT_{i,j}$.

$$FRT_{j,j} = 2(Del_{i,j} + Fog2FogDel_{i,j,k} + HS_{j,k} \tag{3.3}$$

We define a set $\{F\}$ that consists of all the available fogs in the system, and C represents the cloud. Each Fog_i in $\{F\}$ is assigned an ordered 3-tuple, fog capacity FC_i, to represent its capabilities

such that:

$$Fc_i = (Availability, Storage, ActiveJobs) \tag{3.4}$$

Where Availability is a Boolean value that indicates if Fog_i can handle new jobs. Storage denotes the available storage, and ActiveJobs is a dynamic set that includes all active jobs currently handled by Fog_i. As new jobs are added, they should be included in the set, and any completed jobs should be promptly removed.

In addition, we make the assumption that each fog has knowledge of the delay involved in reaching any other fog in the system, as the bandwidth of the links connecting them are considered fixed. The cloud, on the other hand, is considered to be continuously available to handle any job with any storage and processing requirements, and as a result, it is not assigned a capacity n-tuple like the fogs.

Complexity: The complexity of the proposed algorithm depends on the input size of the problem, which includes the number of fog nodes, the number of jobs, and their sizes. Assuming n is the number of fog nodes, m is the number of jobs, and k is the average size of the jobs, the time complexity of the algorithm is $O(nmk)$, assuming that the size of the input does not change. However, it should be noted that the actual running time of the algorithm can vary depending on the specific input values and the performance of the fog nodes and the cloud.

3.4.2 Drone to fog communication scheme

Every device in IoT has the capability of collecting and transmitting data (known asD_i) from the physical world to fog nodes over the internet. Could represented by a set of values.

$$D_i =< S_i, T_i, P_i, M_i > \tag{3.5}$$

The transfer of data from an IoT device to a fog node can be depicted as a message containing four key parameters: the source device ID (S_i), timestamp (T_i), physical parameter (P_i), and measurement value (M_i). The source device ID serves to uniquely identify the IoT device transmitting the data, while the timestamp indicates the precise moment when the data was captured. The physical parameter being monitored or measured by the device, such as temperature, humidity, or air quality, is denoted by P_i. Finally, the measurement value or data point obtained by the device for the corresponding physical parameter is represented by M_i. This message is transferred over the internet utilizing communication protocols like MQTT, CoAP, or HTTP, and undergoes processing by the fog node before being disseminated to other devices or cloud platforms for further analysis and processing.

The wait time for response refers to the duration for which the drone must await a response from the fog node subsequent to transmitting data. This wait time can be computed by considering

factors such as round trip time, signal propagation time, and the processing time required by the fog node to validate successful transmission and dispatch a response to the drone. It can be symbolized as WT_i.

$$WT_i = (RTT + 2TPP) + TPC \tag{3.6}$$

where RTT denotes the round trip time,TPP denotes the time taken for the signal to propagate from the drone to the fog node and back to the drone, and TPC denotes the processing time required by the fog node to confirm successful transmission and send a response back to the drone.

Complexity: $T(n) = O(max\_retries WT_i$, where $T(n)$ is the worst-case running time of the algorithm for an input of size n (in this case, n represents the parameters listed above), max_retries is the maximum number of times to retry transmitting data, and WT_i is the maximum time to wait for a response from the fog node. The worst-case running time of the algorithm is proportional to the number of retry attempts (max_retries) and the maximum time to wait for a response from the fog node (WT_i). Therefore, the overall time complexity of the algorithm is $O(max\_retries WT_i)$.

3.4.3 Establish connection scheme with WIFI

Complexity: $T(n) = O(max\_retries(N + 1))$, where T(n) is the worst-case running time of the algorithm for an input of size n (in this case, n represents the parameters listed above), max_retries is the maximum number of connection attempts, and N is the number of detected Wi-Fi networks.

The worst-case running time of the algorithm is proportional to the number of connection attempts (max_retries) and the time complexity of the steps involved in each connection attempt. The most time-consuming steps are scanning for Wi-Fi networks (scan_for_wIFi_networks) and connecting to the best available network (connect_to_best_network), which have a time complexity of O(N), where N is the number of detected Wi-Fi networks. Therefore, the overall time complexity of the algorithm is $O(max\_retries(N + 1))$.

3.4.4 Drone to drone ad hoc scheme

Establish a connection using ad hoc and peer-to-peer topology with Wi-Fi technology between drones to find the lost drone. The actual implementation of the protocol requires specific steps. The connection is based on broadcasting a hello message H.

$$H =< SA, DA, MT, PV, Payload > \tag{3.7}$$

Algorithm 5: Drone to fog connection

```
1:  maxRetries ← value //
2:  waitTime ← value // In seconds
3:  retryCount ← 0
4:  delayCounter ← 0
5:  while True do
6:    if not WIFiConnected then
7:      EstablishWIFiConnectionToFogNode()
8:    end if
9:    data ← EncodeCapturedData()
10:   if TransmitData(data, maxRetries, waitTime) then
11:     delayCounter.start()
12:     while delayCounter.elapsed() < waitTime do
13:       // Wait for response from fog node to confirm successful transmission
14:       pass
15:     end while
16:     delayCounter.reset()
17:     if ResponseSuccessful() then
18:       continue
19:     else
20:       if retryCount < maxRetries then
21:         retryCount ← retryCount + 1
22:         continue
23:       else
24:         //Max retries reached, give up
25:         break
26:       end if
27:     end if
28:   else
29:     //Failed to transmit data
30:     if retryCount < maxRetries then
31:       retryCount ← retryCount + 1
32:       continue
33:     else
34:       // Max retries reached, give up
35:       break
36:     end if
37:   end if
38: end while
```

Algorithm 6: Establish connection with WIFI

```
1: while not connected and num_retries < max_retries do
2:    // Attempt to connect to network using provided credentials
3:    connection_result ← AttemptConnection(network_credentials)
4:    if connection_result then
5:       // Connection successful, set connected flag to true
6:       connected ← true
7:    else
8:       // Connection failed,
9:       //Scan for available networks and attempt to connect to an alternate node
10:      ScanForNetworks(scan_timeout)
11:      new_node ← FindAlternateNode()
12:      connection_result ← AttemptConnection(network_credentials)
13:      if not connection_result then
14:         // Adjust drone position,
15:         //Increase transmission power, and
16:         //wait before retrying connection
17:         AdjustDronePosition()
18:         IncreaseTransmissionPower(transmission_power)
19:         num_retries ← num_retries + 1
20:         Wait(retry_wait_time)
21:      end if
22:   end if
23: end while
24: // Check if connection was successful and return appropriate message
25: if connected then
26:    return success_message
27: else
28:    return error_message
29: end if
```

The H message format consists of the Source Address (SA), Destination Address (DA), Message Type (MT), Protocol Version (PV), and a variable length $Pyload$ that the sender can include in the message.

Complexity: T(n) = O(n), where T(n) is the worst-case running time of the algorithm for an input of size n (in this case, n represents the number of drones within the max_range). The worst-case running time of the algorithm is proportional to the number of drones within the max_range. Therefore, the overall time complexity of the algorithm is O(n).

Algorithm 7: Drone-to-Drone Communication Algorithm AD-hoc

```
nearby_list ← null // list of closest neighboring drones found
RM ← null // received message from drone B
InitializeWIFi()
nearby_list ← scanNearbyDrones
for node in nearbylist do
    SendHellomessage(drone)
end for
while RM = null do
    Listen for incoming "Hello" messages from drone B
    RM ← ReceiveHelloMessage()
end while
sendHelloMessage(drone, IP)
GetIPAddress(drone)
NegotiateSecurityProtocolAndExchangeKeys(drone)
EstablishCommunicationOverWIFi(ip)
end
```

3.4.5 Election algorithm for the best fog candidate

The election algorithm for fog best candidate takes into account several parameters. The algorithm can be optimized and customized based on the specific requirements and constraints of the fog network.

The compatibility between the communication channel of the fog node F_i and device D_i denoted $CC_{i,j}$. A higher channel compatibility score indicates a better match between the communication protocols, frequencies, or bandwidths used by the fog node and the device.

$$CC_{i,j} = |CF_i \cap CD_j| / |CF_i \cup CD_j| \tag{3.8}$$

Where '|' denotes the cardinality or size of a set, and CF_i is communication channels supported by the fog node, and CD_i be the set of communication channels required by the device.

Fog Capacity FC_i refers to the amount of processing power PF_i, storage capacity SF_i, and bandwidth BF_i that a fog node can provide to connected devices. It reflects the ability of the fog node to process and store data locally and offload some tasks from the cloud or edge devices.

$$FC_i = PF_i Wp + SF_i Ws + BF_i Wb \tag{3.9}$$

Where Wp, Ws, Wb are weights assigned to each parameter, representing their relative importance in the calculation.

Fog range FR_i is a parameter that measures the maximum distance between a fog node F_i and

a device beyond which the communication link becomes weak or unstable.

$$FR_i = (maxRange - D_{i,j})/maxRange \tag{3.10}$$

Where $D_{i,j}$ is the distance between F_i and D_i.

Latency Lt, also known as network delay, is the time it takes for a data packet to travel from the source device to the destination device in a network.

$$Lt = TransmissionDelay + PropagationDelay + ProcessingDelay + QueuingDelay \tag{3.11}$$

We define a set F that consists of all the available fogs for the election. Each Fog_i in F is assigned an ordered set of values to find the best candidate , to represent its capabilities such that:

$$< CC_{ij}, FC_i, FR_i, MD_i, Lt_i, EEi, S_i, GD_i > \tag{3.12}$$

Each candidate fog node broadcasts its score SC_i to the central fog node, which subsequently utilizes these scores to determine the most appropriate candidate for task processing. Through the transmission of their scores, candidate fog nodes furnish the central fog node with insights into their capabilities across multiple domains, including capacity, latency, energy efficiency, security, and availability. Armed with this information, the central fog node can assess and select the candidate that aligns most closely with the task requirements and exhibits the highest overall suitability. The value of SC_i, representing the score of a specific fog node, is derived by amalgamating the computed values of various attributes and assigning corresponding weights. Each attribute is assessed based on its significance in the decision-making process, and a weight is assigned accordingly.

$$\begin{aligned} SC_i = {} & CC_{ij}CCw + FC_iFCw + FR_iFRw + MD_iMDw \\ & + LtLtw + EE_iEEw + S_iSw + GD_iGDw \end{aligned} \tag{3.13}$$

Where $CCw, FCw, FPw, MDw, Ltw, EEw, Sw, GDw$ are weights assigned to each parameter, MD_i represents the maximum number of devices that can be handled by a specific fog node, while EE_i reflects the level of energy efficiency provided by that node. The attribute S_i ndicates the security score of the fog node, while GD_i represents the geographic distance of the node from the requested device.

Complexity: The overall time complexity of the algorithm is therefore O(n), where n is the number of fog nodes in the list of nearby fog nodes.

Algorithm 8: Election algorithm for the best fog condidate

```
nearby_fog_nodes ← GetNearbyFogNodes()
if nearby_fog_nodes.empty() then
  HandleError("No nearby fog nodes available.")
else
  scores ← {}
  for fog_node in nearby_fog_nodes do
    score ← CalculateScore(fog_node)
    scores[fog_node] ← score
  end for
  sorted_scores ← sorted(scores.items(), key=lambda x: x[1], reverse=True)
  best_fog_node ← sorted_scores[0][0]
  response ← SendResponse(best_fog_node)
  if response.error then
    HandleError(response.error_message)
  else
    HandleSuccess(response.message)
  end if
end if
```

3.5 Experiments

3.5.1 System requirements

A fleet of cooperative drones operating in a fog computing system will communicate via short-range connections, taking into account the capacity of the fog nodes. In this case, the drones will use WIFI technology to connect with the fog nodes. These tasks require the selection or calculation of minimum characteristics Table 3.2,Table 3.3 and capacity parameters as follows:

- **Channel Width (in MHz):** $ChannelWidth = n20MHz$, where (n) is the number of channels used. For example, a channel width of 40 MHz means that two adjacent channels are used.
- **Frequency Band (in GHz):** $FrequenceBand = c/(2wavelength)$, where (c) is the speed of light (299,792,458 m/s) and wavelength is the length of the wave.
- **Signal Strength (in dBm):** $SignalStrength = 10log10(P1/P2)$, where (P1) is the received power and (P2) is the reference power (usually 1 mW or 1 milliwatt).
- **Latency (in seconds):** $Latency = (2distance)/(speedoflight)$, where $(distance)$ is the distance between the device and the fog computing system.

Video Processing Capability	Supports real-time video encoding and decoding, and video analytics
Bandwidth	High bandwidth capacity, such as 10 Gbps
Latency	Low latency, less than 100 ms
GPU	High-end GPU for video processing
Storage	High-capacity storage, such as 10 TB
Power Backup	Backup power supply, such as battery or generator, for uninterrupted operation
Location	Near the drone fleet, with multiple nodes distributed to cover a large area
Cloud Connectivity	Connects to cloud services for backup storage and data sharing
Data Management	Efficient data management system for data ingestion, processing, and storage
Security	Advanced security features, such as intrusion detection, threat intelligence, and security monitoring

Table 3.2: Fog node Requirements

Drone devices Characteristic	**Typical Value**
Flight Time	20-30 minutes
Maximum Altitude	300-500 meters
Maximum Speed	50-70 km/h
Camera Resolution	1080p-4K
Field of View	90-120 degrees
Payload Capacity	1-2 kg
Transmission Range	2-5 km
Gimbal Stabilization	2-3 axis

Table 3.3: Drone requirements

3.5.2 Simulation Environment

Since there is no IoT network that is publicly available to evaluate the proposed solutions, we developed our own simulator to test the proposed algorithms. In addition, all existing simulators did not allow for addressing the lost drone issue. The proposed simulator is designed to take into account all possible scenarios of losing drones. To stay as faithful as possible to the IoT architecture, the simulator was developed by taking into account two main actors, namely, the fog layer and the device layer (Figure 3.1).

Drones represent the device layer and appear as a circle with a radius expressing its connection field. Each drone has two states: normal and emergency, and it communicates through three different modes: communication with the main fog, communication with neighboring fogs, and no communication. Each drone has information about the fog it belongs to as well as information about other drones owned by the same fog node. The fog node is also represented as a circle; the radius represents the area that can be covered by the fog; the difference between the fog and the drone is the coverage area. Each fog has its own list of devices as well as a list of neighboring

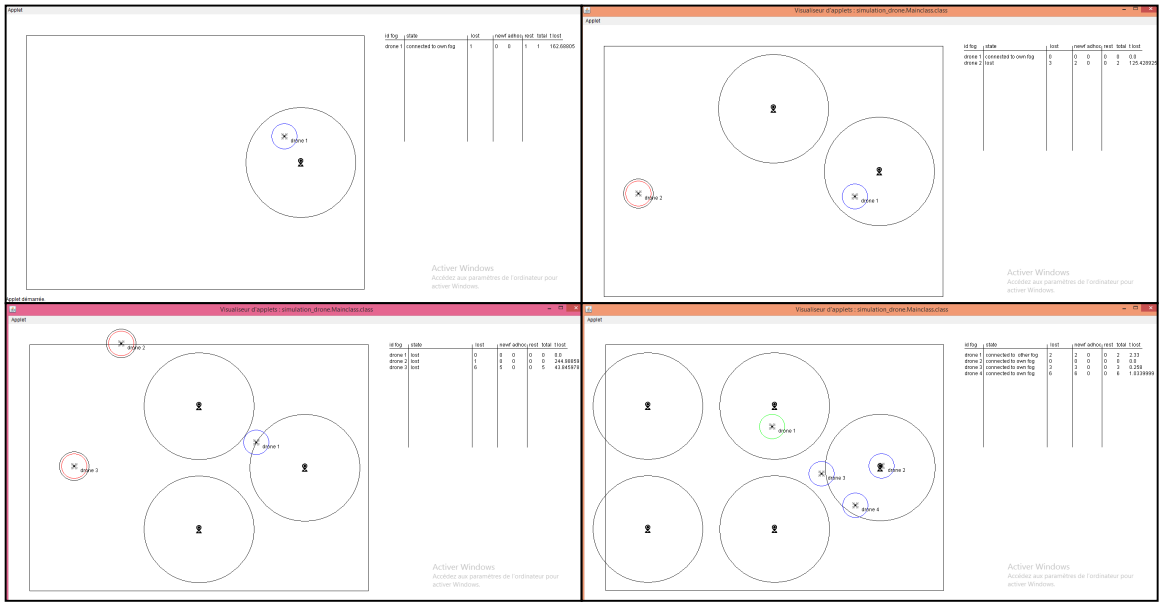

Figure 3.5: Simulation Screenshots

fogs. The fog nodes are distributed randomly in order to avoid perfect drone situations.

It should be noted that the simulation interface depicts the behavior of the system and not the system itself. This is because the experiment was conducted on a real physical network that connects multiple computers wirelessly. We used laptops to simulate the drones and desktop computers to simulate the Fog nodes. All proposed algorithms were implemented on these computers according to their respective roles. The event of the drone leaving the range of the Fog is simulated by moving the laptops out of the Fog's range. This experiment was conducted at the Department of Computer Science at the University of Guelma.

3.5.3 Simulation Results

In this section, we present numerical results in order to evaluate the performance of the proposed algorithms to restore lost drones. The simulation is performed on each actor in the system (drones, fog neighbors, and the main fog). The simulation was run 1,000 times for each drone to ensure all possible scenarios. We placed the centers of the fog nodes in a random way to obtain more credible and realistic results, knowing that the distribution of centers is very important for covering larger areas and thus avoiding losing connection.

The drone loss event is performed by randomly distancing the drone outside the fog range. This is done by adding a random value to the actual coordinates of the drone. The number of losses for each drone is also a random value.

Remember that the objective of the simulation is to ensure that the proposed algorithms work and can bring back the lost drones, despite the time needed for that.

We proposed various scenarios with different numbers of drones and fog nodes. Each scenario

Settings		Losses	Recovered	Recovery type			RecoveryTime (S)
#of drones	Fognodes			Main Fog	Fogneighbours	Ad-Hoc	
One	1	1	1	1	0	0	162,688
	2	3	2	0	2	0	210,464
	3	2	2	0	2	0	163,332
	4	7	7	1	6	0	52,110
	5	10	10	0	10	0	12,052
Two	1	2	1	1	0	0	194,568
	2	3	2	0	2	0	124,428
	3	6	6	1	5	0	119,956
	4	6	6	0	6	0	50,449
	5	8	8	0	8	0	0,750
Three	1	3	1	1	0	0	417,720
	2	4	2	0	2	0	318,611
	3	7	5	0	5	0	288,833
	4	7	7	1	6	0	42,894
	5	11	11	0	9	2	37,949
Four	1	8	5	3	0	2	470,670
	2	9	8	2	5	1	207,425
	3	6	5	0	5	0	356,504
	4	10	9	0	9	0	281,999
	5	11	11	0	11	0	3,621

Table 3.4: Simulation Results

was tested four times to get different behaviors.
We tested the system with four scenarios. The first contains a single drone, the second contains two drones, and the last contains four drones. Each scenario is tested, respectively, with 1, 2, 3, and 4 fog nodes. Table 3.4 summarizes the results obtained for each scenario.

Based on the obtained results, we notice that the system succeeded in recovering the lost drones in most cases, with a recovery rate of 86.13%. However, the recovery time is inversely proportional to the number of fog nodes. Indeed, when the number of fog nodes is high, there is a good chance that the drone will get lost in the range of another fog node. This speeds up the recovery operation and reduces the number of total losses. We also note that the activation of the ad-hoc network made it possible to recover 5 cases among 101 losses, which means that the complementary recovery strategy allows for an addition of 4%.

3.6 Conclusion

The use of drones has become an essential means of solving problems with difficult access. In general, drone-based missions operate on the directives of a base station, which gives the instructions to be followed by the drones to accomplish their missions. Recently, it has been noticed that several drones disappear during a mission or during repatriation, causing losses in money and information. This worrying situation had as its main cause the loss of connection

between the drone and the base station. To resolve this problem, we have proposed in this contribution a new communication protocol that allows to recover the drones in case of loss through two strategies.
The first is to ask other fog nodes for help; then, allow them to communicate with the lost drone. The repatriation is done by following the instructions through the neighboring fogs until arriving at the range of the main fog. The second strategy is activated when no neighboring fog reports a connection attempt from an unknown drone. In this case, the main fog sends a backup drone to the last known position of the lost drone. The latter activates an ad-hoc network to try to recover the drone. The proposed strategies have been implemented and tested in several scenarios. The results obtained show that the lost drones were recovered in most cases.

Chapter 4

Fog Node Overload: Dynamic Solution for Enhanced IoT Efficiency

4.1 Introduction

Cities are becoming more interconnected due to the growing use of technology and the Internet [435]. The huge number of connected devices is expected to reach 19.08 billion by 2025 [436], representing the significant transition to IoT. This evolution aims to bridge the gap between the physical and virtual worlds, using the internet as a means of communication and information sharing. As a result, IoT has become the main driver for a wide range of applications, including industry, smart cities, smart homes, smart energy, smart cars, smart agriculture, smart campuses and buildings, healthcare and logistics [437]. This explosion in applications poses a major challenges : managing many objects, gateways and network devices, which increases complexity due to the high scalability involved [438]. Notably, the development from the traditional cloud computing to a Cloud of Things caused by the IoT has introduced latency issues due to bandwidth limitations[439], despite the promise of unlimited high-speed processing and storage by cloud. Cisco, responded to such challenges by creating the fog computing as a technological platform by 2013 [440]. The fog computing brings computing resources close to IoT devices and users [439, 441, 442]. In addition, fog nodes can help in reducing high computational, communication (service), and network latency's and bandwidth[439]. However, it's important to note that the limited resources (storage and processing capacity) at fog nodes may result in overload during high traffic volumes[443, 444]. This overload impact the capacity and quality of service[443, 444], potentially affecting the efficiency and responsiveness of the whole IoT system [445, 446]. On the other hand, there is a multitude of sensors communicating unidirectional with IoT high layers, transmitting collected data without the capability to verify connectivity or handle data loss, especially with small-capacity sensors. In such scenarios, sensitive IoT applications requiring real-time decision-making are affected directly by the limitations facing the fog computing [447, 448]. While the concept and theoretical foundations of fog computing have been extensively studied, there exists a gap in effectively addressing real-time overloading issues without compromising data integrity or overall system performance. Numerous studies have sought to solve this problem by designing approaches focused on fog nodes collaboration and overload prediction. Among these approaches, load balancing is the most widely used resource allocation method for allocating available resources strategically between tasks [449, 450, 451, 452, 453, 454]. However, this

solution comes up against two major problems. Firstly, the heterogeneity between tasks and the specialized nature of fog nodes require an intermediate platform for task standardization. Secondly, it exacerbates communication latency in the presence of a load manager in the system. The latter is responsible for managing tasks between groups of fog nodes [455, 456].

In light of the above cited challenges, a new managing approach is needed for the fog node in real-time overload situation. We are developing a DFC-based mechanism that allows the fog node to control its state according to available resources without the intervention of another part. The main objectives of this solution are freeing the fog node from any selection, task or processing, granting it only an intermediate data transfer object, which offers a real view of the resources available in the system and also allows the fog node to complete its processing until reactivation. This solution aims to preserve data and provide stable response times in a fog-based IoT environment.

4.2 Related work

In recent years, numerous studies have proposed strategies to improve the effectiveness of fog computing systems from diverse viewpoints[457, 458, 459]. These investigations have delved into various approaches to harnessing the benefits of fog computing technology while mitigating its limitations and associated challenges[457, 458, 459]. For instance, some studies have focused on the overloading challenge in fog nodes[460, 461]. In this context, [449] proposed a load-sharing mechanism based on random walk. This mechanism aims to offload jobs to neighboring nodes, presenting a lightweight, randomized, on-line distributed load balancing algorithm. It is characterized by independent providers, heterogeneous load conditions, and includes a variant based on a self-tuning mechanism. Building on this, M. A. Jasim et al. [450] presented a strategy for managing loads that addresses saturated fog nodes in periods of high traffic. The goal is to improve network utilization rates with fewer migration iterations and less downtime. More precisely, the approach involves a pre-overload migration scheme that transfers mapped Virtualized Network Functions (VNFs) from a host node to target nodes prior to a saturation event. This proactive method minimizes service downtime during the migration process, albeit with an associated increase in resource usage. Moreover, Fan et al. [451] introduced a workload balancing scheme in a fog network to minimize latency in both communication and data processing. Their approach involves formulating the problem of minimizing overall latency by associating IoT devices with different Base Stations (BSs) or fog nodes. To address the load balancing challenge in the fog network, they devised a distributed IoT device association scheme (LAB). This scheme assigns IoT devices to appropriate BSs or fog nodes, effectively reducing the latency of all data flows. In a similar vein, Xin Gao et al. [462] directed their attention towards forecasting instances of fog overload and strategically offloading data to neighboring nodes through

the implementation of a resource allocation mechanism. Pushpa Singh et al.[452] suggested a concept to compute the probabilistic overloading state of a fog node and identify the fog node for load sharing. Taking a different approach, Mohammed Al-Khafajiy et al. [453] introduced a fog computing architecture and framework incorporating an offloading and collaboration strategy among fog nodes. They proposed a fog resources management framework based on a request offloading method. The primary objective of this framework is to improve the performance of fog computing by addressing load imbalances. In their approach, latency reduction is achieved through the implementation of a fog-to-fog collaboration model, enabling the distribution of loads among nodes in the fog layer. Moreover, the proposed collaboration model can differentiate between heavy requests from the IoT layer and lighter requests from the things layer. The studies conducted by [454] and [462] employed prediction methods as a viable solution for identifying and addressing overload situations. On a related note, [463] introduced a task provisioning approach in dynamic fog computing with the aim of optimizing the number of served end-users. In a related context, Al-Khafajiy et al. [464] proposed improvements for enhancing fog computing performance through Fog-2-Fog collaboration. Lastly, the research conducted by [465] centers on the load balancing aspect of fog networks, with the goal of mitigating situations in which specific fog nodes experience either insufficient or excessive loads.

Although the aforementioned studies resolve some challenges in the context of avoid the overload are based on two main points: firstly, the creation of an intermediate manager or platform under the fog node layer to manage the tasks received from the devices by distributing them to the available fog nodes. These studies enable high collaboration and resource utilization for the fog layer, but require tasks to be standardized, resulting in high computation and network latency. These solutions have two drawbacks: the sharing mechanism that works with each task is not triggered by the state of the fog node, and the decision is made by another party and not by the fog itself, which means there is no real-time decision for implementation and only predictions. In this contribution, a DFC-based mechanism is applied inside the fog node to control and manage its mode according to its available capacity. It has the advantage of freeing the fog node from its function when it has no capacity. This solution reduces network and computation latency and provides real-time decision-making.

4.3 System Model And Problem Formulation

4.3.1 Fog Computing infrastructure

This architecture composed of three principals physical elements iot device, fog device and gateway device. These elements in FC architecture have the requirements of infrastructure, platform, and applications (Figure 4.1). Follow the principle of proximity to the device, the FC layer have two link of communication the first is for the cloud and the second is for devices.

[466][467][?] [468].

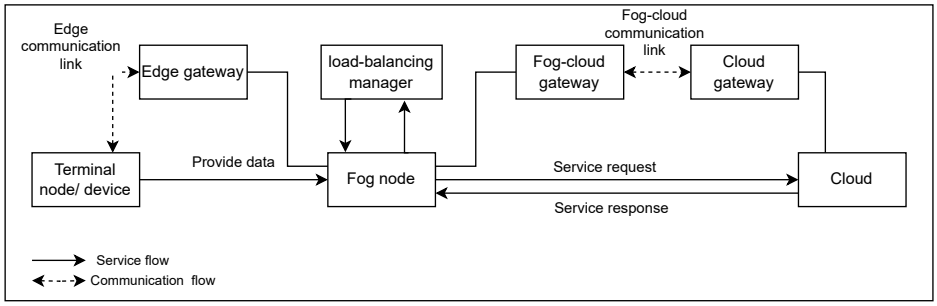

Figure 4.1: Fog Computing Infrastructure

Terminal node device any device has the capacity of sensing and generating data with no processing or treatment only transmission links to higher level layer.

Fog processing node Any device has the capacity of storage and processing at the edge of iot network is able to be a fog device. controller, switch, router, server, surveillance camera, The most of these devices have a maximum performance of 266-400 MHz MPC8272 processor,16 KB Cache, 64 MB random access memory and 20 MB processor board flash memory.A huge number of equipped sensors generate data to perform a real time tasks.

Edge communication devices Terminal device to fog networks based on Wireless Local Aria Networks(WLAN), this type of connection support ZigBee, Bluetooth, Wi-Fi (802.11a/ac), Wi-Fi 802.11ah, LoRa and Zwave technologies For a short distance connection. This type is characterised by low cost as well as low energy consumption.

Fog-cloud communication devices the communication between the fog node and cloud needs connection of type WAN(Wide area networks) which support WIMAX and 4G technologies. this type provide powerfull extension of communication.

4.3.2 Scenario description

The FC paradigm anddresses the bandwidth constraints of cloud computing brought on by the large number of connected devices by providing a distributed network for IoT contexts in smart cities. However, it becomes clear from examining the FC's drawbacks and problems that the processing and storage limitations present the biggest obstacle (Figure 4.3). Fog nodes are also not designed for high costs, making them prone to failure while handling real-time tasks and degrading the performance of sensitive IoT applications. Low latency and data loss arise from the fog node's inability to accept data during a breakdown until it has recharged.Here are some

important factors to keep in consideration when it comes to fog computing (Figure 4.2) and how it impacts capacity, cost, latency, and bandwidth:

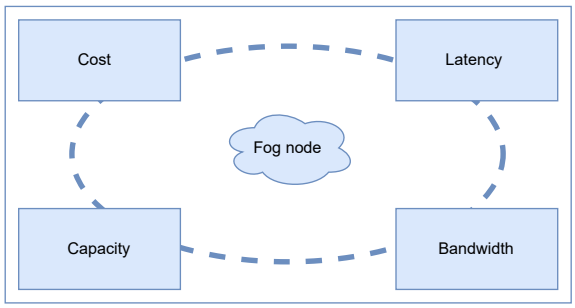

Figure 4.2: Fog computing challenges

- Capacity and Latency: Fog nodes with higher capacities have lower latency because they can process and analyse data more quickly at the edge, near the edge devices.
- Capacity and Cost: Increasing the capacity of fog nodes typically results in increased expenses because more hardware and infrastructure are required.
- Cost and Latency: Investing in network upgrades and the deployment of advanced fog nodes may be necessary to reduce latency in fog computing, which will raise expenses.
- Bandwidth and Capacity: Fog nodes with higher capacities may produce or process bigger volumes of data, necessitating a correspondingly higher bandwidth for effective data delivery.
- Latency and Bandwidth: By facilitating quicker data transfer between edge devices, fog nodes, and the cloud, higher bandwidth availability reduces latency in fog computing.
- Cost and Bandwidth: Increasing bandwidth for fog computing may call for network infrastructure expenditures, which could raise costs.

4.3.3 System Model

The proposed model allow to devices sending data to the fog node without any conditions or limitations. Then, the fog node in the default mode stores and process data until getting a warning of exceed the maximum capacity. We develop the fog node to change its mode from fog node to be another devices which transfer data directly to the cloud without any treatment And this is in case it is unable to perform well. The figure 4.4 shows the stages of realising a dynamism for the fog node to loosen up the overload. In the virtual cluster every device transmit data cyclically to the main fog node for storage and processing .the new parameter added to the node fog is the mode, This variable refers to two cases. The first case is the default state where the fog node is capable to manage received data and there is no changes. the second case where the fog node had a surcharge of treatment, Our model aims to Put the fog node into a stagnant state and transfer received data from devices to the cloud passing over the fog node. Moreover, the fog node work as a middle devices of transmission with two kinds of communication links,

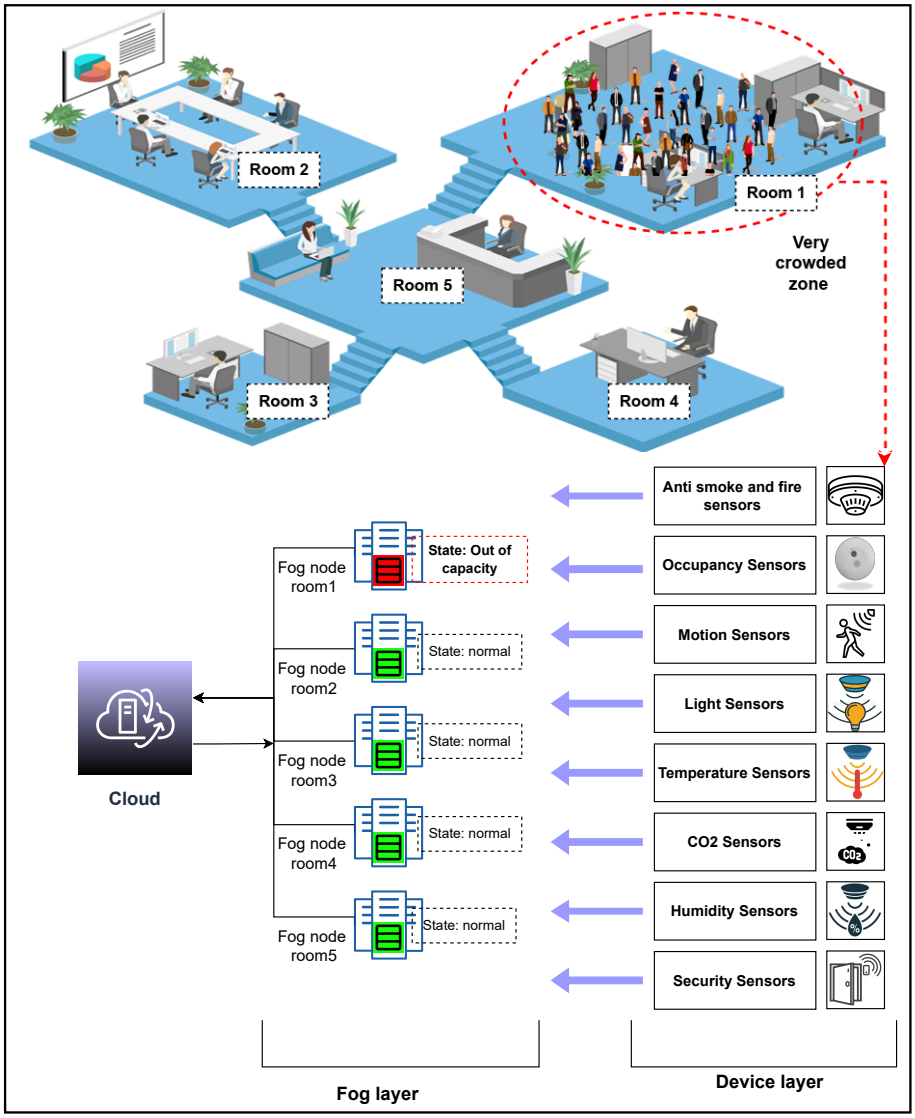

Figure 4.3: Fog computing limitations

short communication link and long communication link. The use of fog node mode Adheres to several steps:

Fog mode: The most important step is checking capacity of the fog node. If the transmitted data makes the fog node full the mode returned to device mode, And Send received data to the cloud.

Device mode: This mode means that the fog was full and incapable to treat data, So the next step is depend on checking the capacity until losing the half charge of the fog node.

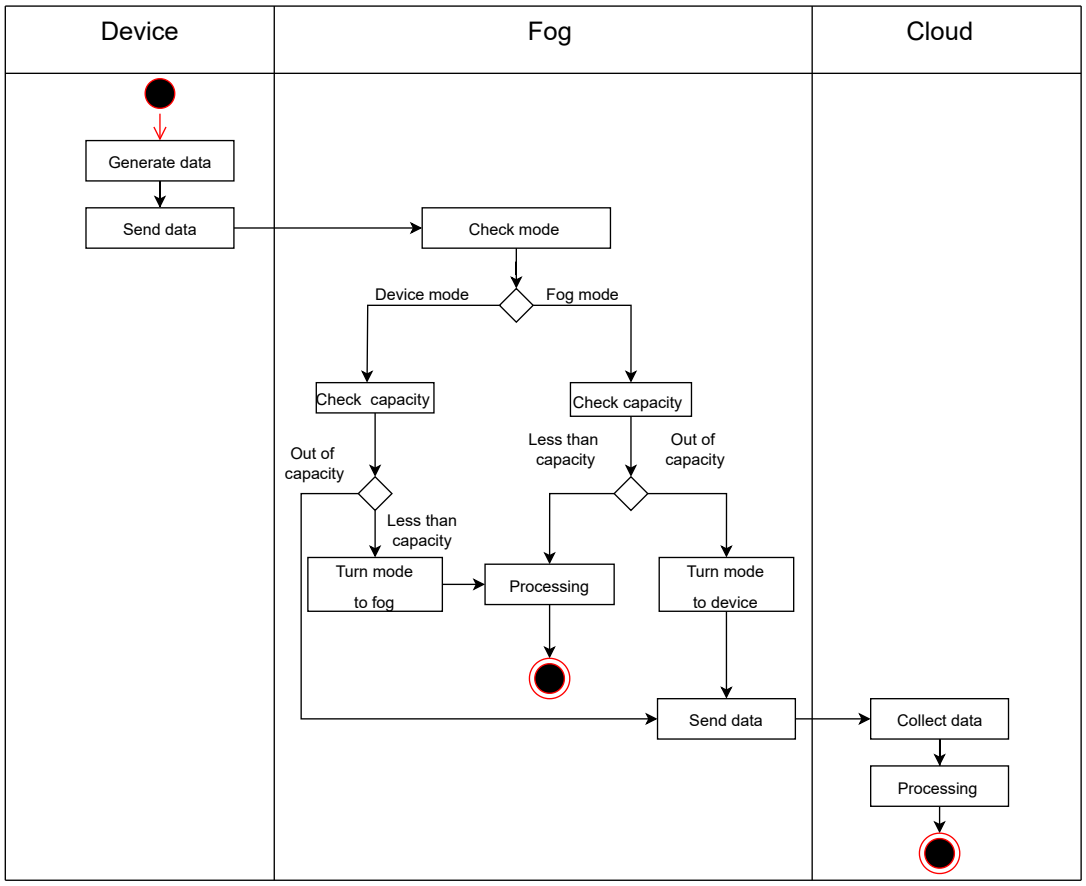

Figure 4.4: Dynamic fog computing model

4.3.4 Proposed dynamic fog mechanism

The success of an IoT system largely depends on the efficiency and reliability of its device-to-fog and fog-to-cloud communication network. Designing and implementing such a network is a challenging task due to the large volume of data transmitted by multiple IoT devices, low latency requirements, and energy constraints. To address these challenges, it is essential to study and analyse the various parameters that affect the performance of the network, including data rate, latency, range, reliability, energy efficiency, security, and protocol. By understanding the impact of these parameters and developing efficient algorithms and protocols, we can optimise the network's performance and ensure a high quality of service.

- Fog node storage utilisation: This can be calculated by dividing the number of existing data points in the linked list by the maximum capacity of the fog node.

$$FogStorageUtilization = \frac{N}{C} \tag{4.1}$$

where N is the number of existing data points and C is the maximum capacity of the fog node.

- Data transmission rate to the cloud: This can be calculated by dividing the number of data points $X_{i,Cl}$ that are resent to the cloud by the total number of data pointsX_i.

$$DataTransmissionRatetoCloud = \frac{\sum X_{i,Cl}}{\sum X_i} \tag{4.2}$$

Algorithm 9: Dynamic-Fog Mode Management

Require: x: new data point, l_x: linked list of existing data points, m: binary flag indicating current mode (0 for fog, 1 for device), C: maximum capacity of fog, cl: object representing the cloud, f: object representing the fog.
Ensure: l_x: updated linked list of data points, m: updated binary flag indicating current mode.

Set f to "this fog" object.
Set N to 0.
Set i to 0.
while i is not equal to the size of the linked list **do**
    Add the value of the current data point in the linked list to N.
    Move to the next data point in the linked list.
    Increment i by 1.
end while
if m is 1 and the capacity of the fog (C) is greater than N **then**
    Add the new data point x to the linked list l_x.
else if m is 1 and C is less than N **then**
    Set m to 0.
    Resend the new data point x to the cloud object cl using f.resendToCloud(cl, x).
else if m is 0 and the capacity of the fog divided by 2 ($C/2$) is greater than or equal to N **then**
    Set m to 1.
    Add the new data point x to the linked list l_x. **else**
    end
    Resend the new data point x to the cloud object cl using f.resendToCloud(cl, x).
end if
Return the updated linked list l_x and binary flag m.

Data transmission schemes

All of fog node F , IoT device Dev_i and Cloud c require a communication protocol as well as network connectivity in order to communicate with one another. While network connectivity allows the device,the fog node exchange data across a physical or wireless media.

- Sending message M_t with a single data value d from a sensor/device to a fog node using the MQTT protocol might be:

$$M_t = MQTT(TOPIC, DEV_{ID}, d, size) \tag{4.3}$$

Where $TOPIC$ is the MQTT topic to publish the message to, DEV_ID is the unique

identifier of the sensor/device, and d is the data value collected at time t.

- The latency L of transmission between device D_i and the fog node F might be:

$$L = T_{ack} - T_{start} \tag{4.4}$$

where T_{ack} is the time at which the acknowledgment message is received by the sensor/device, and T_{start} is the time at which the data is collected by the sensor/device.

- The Message Loss Rate (MLR) measures the percentage of messages sent by a sensor or device that are lost or not acknowledged by the fog node.

$$MLR = \frac{N_{sent} - N_{ack}}{N_{sent}} 100 \tag{4.5}$$

where N_{sent} is the total number of messages sent by the sensor/device, and N_{ack} is the number of acknowledgement messages received by the sensor/device.

- Message to Cloud rate (MCR) present the percentage of messages sent by fog to Cloud.

$$MCR = \frac{Ncl}{Nsent} 100 \tag{4.6}$$

where Ncl is the total number of messages transmitted by fog to Cloud without processing.

- waiting time in fog node (MWT) is the time required to process the incoming msg from device to fog node.
  if data processed in default state inside fog node

$$MWT = \frac{D_{size} + D_{stored}}{F_r} \tag{4.7}$$

if data processed in relay mode

$$MWT = C \tag{4.8}$$

Where D_{size} id the size of data sent by device, D_{stored} represent data already wait in the fog node, C is constant provided by Cloud for processing delay.

4.4 Experimentation And Results

4.4.1 Environment

We developed a network communication system using Java agents for devices to achieve the transfer of files sized between 0 and 10 kilobytes in a cyclical manner. Additionally, we implemented a fog node agent that checks and processes data. Moreover, if the data exceeds a certain limits, it sends the overloaded data to the Cloud.

Algorithm 10: Device-Fog communication

Require: sensor/device identifier, fog node URL, message format, reliable transport protocol
Ensure: none

```
Initialize sensor/device with unique identifier and establish connection to fog node
while true do
    Collect data from sensor/device and package it into compatible message format for fog node
    Check network connection for stability and reliability
    Send message to fog node using reliable transport protocol with sensor/device identifier
end while
```

Algorithm 11: Fog-Cloud communication

```
Input: Message data, destination cloud server IP address, transport protocol
Output: Acknowledgment message from cloud server

Package the message data into a format compatible with the destination cloud server.
Check the network connection to ensure it is stable and reliable.
Send the message to the cloud server using the specified transport protocol and
    including any necessary authentication information.
Wait for an acknowledgment message from the cloud server to confirm receipt of
    the data.
if the acknowledgment is not received within a specified time then
    Re-send the message to the cloud server.
end if
if the acknowledgment is received then
    Verify the integrity of the data sent by comparing it with the data received by the
    cloud server.
    if the data is correct then
        Continue to send messages to the cloud server.
    else
        Take corrective action or alert the appropriate personnel.
    end if
end if
```

This experimentation was conducted in the workstation room of the Computer Science department at the University of Guelma. In this environment, we are able to test and evaluate the effectiveness of our network communication system in a controlled environment.
It is important to note that although this experimentation was conducted using real-world computers as devices, to replicate real-world network conditions, such as network congestion, latency, and packet loss.
In the current system setup, all devices generate and transmit data without receiving any acknowledgement or response from fog nodes. This lack of feedback means that if data is lost during transmission, the device has no way of knowing about it or resending the information. As a result, this situation can make the overall process significantly more challenging and less reliable. The consequences of lost data can be severe, leading to inaccuracies, disruptions, or inefficiencies in various applications and systems. Fog storage refers to the amount of storage capacity available in the fog nodes, which typically refers to a size of 100 kilobytes (KB). This storage space allows fog nodes to temporarily store data that is generated by devices before it is processed or forwarded to the Cloud. Processing frequency in the context of fog nodes refers to the rate at which data can be processed by these nodes. In this case, the processing frequency is stated as 10 kilobytes per second (KB/s), indicating the speed at which fog nodes can handle and analyze the incoming data. The data generation rates were determined based on the frequency of the size of data generated within a given time period. By estimating transmission times and comparing them with data generation rates, the potential data loss was quantified. We successfully implemented a fog computing solution under challenging circumstances, involving the processing of data between 5 to 15 devices with varying capacities. Our objective was to determine the potential data loss without utilising the Fog relay mode.

cloud	
capacity	unlimited
storage	unlimited
Fog	
storage	100 Ko
processing frequency	10Ko/s

Table 4.1: environment settings

4.4.2 Results and discussion

The table 4.3 presents the results of our simulation for the network communication system using Java agents for device-to-device file transfer. We evaluated the system's performance in terms of the number of connected devices, total size of data, total message number, waiting time in the fog, message loss rate, transferred data to the Cloud, message to Cloud rate, and the number of switches. These results were obtained in a controlled environment within the

# device	size of generated data(ko)	cycle(s)
1	50	7
2	2	2
3	3	5
4	4	5
5	5	2
6	6	5
7	7	5
8	4	3
9	3	3
10	5	10
11	2	5
12	2	10
13	2	9
14	2	7
15	2	8

Table 4.2: devices settings

workstation room of the Computer Science department at the University of Guelma. From the table, we can observe the following trends:

- As the number of connected devices increased from 5 to 15, the total size of data, total message number, and transferred data to the Cloud also increased. This is expected as more devices contribute to the data generation process.
- The waiting time in the fog remained relatively stable, ranging from 4.11 to 5.27 seconds, regardless of the number of devices. This indicates that the fog nodes were able to process the incoming data within a consistent timeframe.
- The task loss rate was consistently zero across all the scenarios, indicating that no data was lost during the transmission process. This is a positive outcome as it ensures the accuracy and reliability of the system.
- The amount of data transferred to the Cloud increased as the number of devices and total size of data increased. This suggests that the fog node agent effectively identified overloaded data and offloaded it to the cloud node for further processing.
- The task to cloud rate ranged from 4.4% to 31.87%, showing the proportion of data that was forwarded from the fog nodes to the Cloud. As more devices and data were involved, a higher percentage of data was sent to the Cloud for distributed processing.
- The number of switches, indicating the number of times data was transferred from one node to another, varied between 7 and 48. This suggests that the system dynamically adapted its routing based on the workload and data load on each node.

Overall, the simulation results demonstrate the successful implementation of the fog computing solution for Dynamic computation. The system effectively processed data from multiple

number connected devices	total size data (Mo)	total tasks number	waiting time in fog (s) (Response time)	tasks loss Rate	transferred data to cloud (Mo)	Msg to cloud	nb switch
5	6.25	500	4.70 (s)	0	0.39	04.40 %	07
6	6.83	600	4.41 (s)	0	0.72	08.33 %	14
7	7.51	700	5.27 (s)	0	1.40	17.71 %	23
8	7.91	800	4.72 (s)	0	1.88	31.87 %	35
9	8.20	900	4.51 (s)	0	2.23	28.77 %	40
10	8.69	1000	4.49 (s)	0	2.39	28.30 %	38
11	8.88	1100	4.35 (s)	0	2.64	28.81 %	44
12	9.02	1200	4.11 (s)	0	2.66	31.75 %	42
13	9.27	1300	4.16 (s)	0	2.89	26.61 %	47
14	9.47	1400	4.12 (s)	0	2.92	27.71 %	48
15	9.66	1500	4.28 (s)	0	3.11	21.66 %	48

Table 4.3: Experimentation results

devices, identified overloaded data, and forwarded it to the cloud for further processing. The absence of message loss indicates the reliability of the system in transmitting data without significant disruptions. However, the evaluation and testing in real-world network conditions to validate the system's performance and scalability in practical scenarios give us a very satisfied results.

4.5 Conclusion

This chapter highlights the challenges faced by the fog computing architecture in meeting the quality of service and latency requirements for enabling sensitive applications on the internet of things. The proposed dynamic fog computing architecture offers a solution to the problem of fog capacity saturation by allowing the fog to switch to an intermediate connected device. This chapter shows that DFC improves performance while meeting the QoS and cost requirements. Simulations demonstrate that DFC reduce latency and save data, enabling real-time and sensitive decision-making. In the case of prioritizing data preservation over bandwidth efficiency, we observed a stable latency and maximized utilization of fog node capacity. The results indicate that the proposed Distributed Fog Computing (DFC) solution offers a primitive yet effective approach for enhancing performance in IoT systems.

Chapter 5

Minimizing Data Transmission Overhead in IoT-Enabled Drone Networks through Fog Area Partitioning

5.1 Introduction

Drones, have evolved into indispensable tools for surveillance across various domains, owing to their versatility and agility in accessing remote or hazardous locations. In recent years, the integration of drones within the IoT ecosystem has further expanded their capabilities, enabling seamless connectivity and real-time data exchange with other IoT devices and systems.

Collaborative drone surveillance, where multiple drones work in concert to monitor a designated area, represents a paradigm shift in surveillance methodologies, offering unprecedented levels of situational awareness and response capabilities. However, the effective coordination of data transmission among collaborating drones remains a pressing challenge, necessitating innovative approaches to optimize resource utilization and mission performance.

This research endeavors to address the challenge of reducing data transmission overheads in collaborative drone surveillance missions. Our objective is to propose a novel approach that harnesses fog computing techniques to streamline data processing and transmission within the drone network. By partitioning the fog computing area into smaller zones and facilitating cooperative strategies among drones, we aim to enhance mission efficiency, responsiveness, and scalability.

5.2 Related work

Many strategies aim to reduce data, frequently with the aid of engines that are event- or rule-based. Nevertheless, these techniques frequently depend on domain-specific guidelines instead of taking advantage of time-series data's unique properties. A method for aggregating data in machine-to-machine systems, for instance, was presented by Shen and associates [469]. A number of research publications suggest methods for extending sensor network lifetimes through data transmission reduction. These tactics include of data collection, scheduling, routing, clustering, data compression, predictive monitoring, battery optimization, and radio efficiency enhancement [470]. In sensor networks and the Internet of Things, aggregation techniques including count, total, average, minimum, and average are frequently used to combine data from many sources.

However, because of the extra overhead and ongoing connections needed between components, centralized techniques are not feasible for sensor networks [471, 472, 473, 474].

Data redundancy poses challenges in large data environments. The integration of nodes, dataset growth, and data replication contribute to increased redundancy [475]. Fleet management in autonomous moving objects involves configuring groups of aerial objects and addressing collision and merging scenarios. Fleet management techniques can be centralized or decentralized, each offering different levels of automation [476]. Data pre-processing techniques play a crucial role in extracting meta-data for further processing. Various fundamental approaches for data pre-processing have been explored . Spatiotemporal [477], gZIP [478], AST [479], RED encoding, DQC [480], and TNs [481]. These techniques offer valuable tools for enhancing data processing and compression, with ongoing research focusing on further advancements [482] [483][484].

5.3 Method

The issues of redundant data transmission in IoT-based networks are addressed creatively in this chapter by employing drones. We propose a method that divides the fog area and distributes the data load across drones in order to minimize redundancy and maximize effectiveness. The figure **??**.

The following are the inventive features of our suggested remedy:

- We provide an algorithm that partitions the fog region into smaller segments according to factors including data load distribution, coverage needs, and proximity. Drones operating within each zone can concentrate on particular areas of interest thanks to the divide that produces limited coverage zones. As a result of our clever fog area division, we minimize redundancy and encourage drone collaboration and data sharing.
- Data Distribution Factor: The percentage of data that every drone should broadcast inside a fog area is represented by the data distribution factor (D_i), which we define. Based on the quantity of drones in a fog region, the data distribution factor is computed. This element optimizes bandwidth consumption and lowers redundancy by ensuring a fair distribution of the data load across the drones.
- We offer a step-by-step technique for the partitioning of fog areas and the distribution of data loads among drones. In order to continuously improve the fog area division and guarantee effective data transmission, this algorithm takes into account coverage requirements, proximity, and dynamic changes.
- Workload Sharing: To enable coordinated drone surveillance operations, we suggest the "shot-by-shot capture method". With this approach, redundancy is removed and coverage is maximized when numerous drones are present in the same region and the burden is distributed equitably.

Our suggested strategy is more successful overall because of the combination of job sharing, data distribution factor, and fog area partition. Our novel method increases data transmission efficiency in drone-based IoT networks by tackling the issues of redundant data transmission, bandwidth constraints, network congestion, and higher expenses. Figure 5.1.

We utilize a set of drones, $D = D_1, D_2, ..., D_n$, to characterize the task. Due to overlapping coverage regions or duplicate data, redundant data transmission occurs when each drone collects and sends data to the base station. This redundancy is measured in R. Factor that distributes data: Within a fog area, the percentage of data that each drone should broadcast is represented by the data distribution factor (D_i). It is calculable as:

$$D_i = \frac{1}{n_i}$$

where n_i is the number of drones in the fog area.

The fog region is divided into smaller portions, denoted by $F = F_1 1, F_2, ..., F_m$, in order to reduce repetition. Every fog patch relates to a particular area. The percentage of data that each drone should broadcast inside a fog area is represented by the data distribution factor Di, which we introduce. Di is computed as $\frac{1}{n_i}$, where n_i is the total number of drones in an area covered by fog.

We divide the fog region according to proximity, coverage needs, and data load distribution using an algorithm. This method generates zones of limited coverage so that drones in each zone can concentrate on certain areas of interest. As drones with comparable information cooperate and share discoveries, this division reduces redundancy. These are the steps that the fog area division algorithm involves:

- Ascertain the size and arrangement of the fog area.
- Determine what coverage is needed and draw interest areas.
- Determine the drones' proximity to one another and group them according to interest
- areas and proximity.
- Drones should be sent to designated areas of fog based on their proximity and coverage requirements.
- Respond to dynamic changes by continuously adjusting the fog area division.

The fog zone division method promotes collaboration and data exchange inside each fog zone, which increases the effectiveness of data transmission.

The purpose of the shot-by-shot acquisition technique is to make it easier for nearby surveillance drones to operate in unison. A single drone operating in the assigned region is able to continuously take five pictures per second, each of which takes up five kilobytes (5 KB). But when two drones are present in the same region at the same time, the technique makes sure that the drones share the photos they acquire fairly.

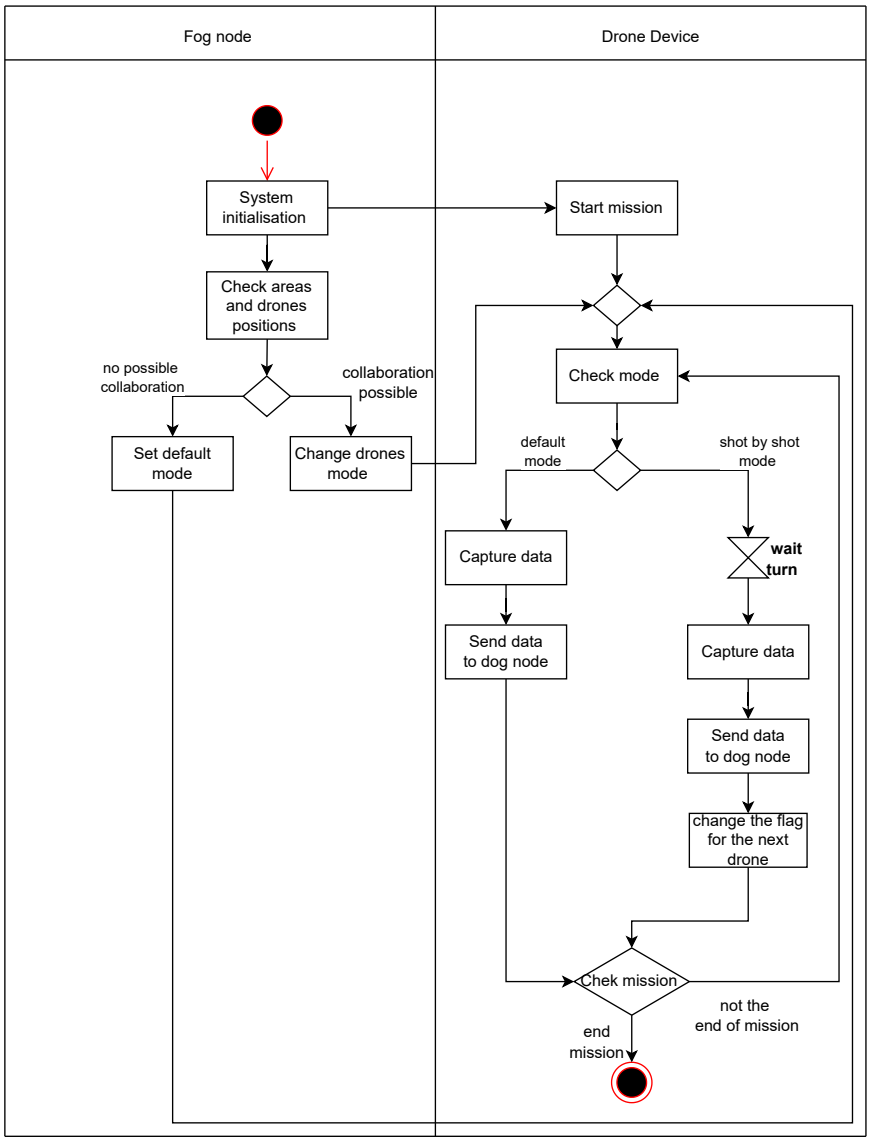

Figure 5.1: Proposed approach

When both drones are in operation, one of them is set up to take a 5 KB picture while the other drone concurrently captures another picture of the same size. Hence, both drones will take ten photographs in total within ten seconds, five shots from each drone separately. By distributing the task equally among the drones, this technique maximizes coverage and removes the possibility of data loss or redundancy.

5.3.1 System Implementation

The following essential elements are part of our suggested method for maximizing data transfer in an Internet of Things drone network: drones, cameras, sensors, GPS receivers, and base stations. Drones come with GPS receivers, cameras, and sensors installed. Sensors collect

Algorithm 12: Fog Area Division and Data Load Distribution Algorithm

Require:

Define the fog area boundaries
Specify the number of available surveillance drones

Ensure:

Optimized fog area division and data load distribution among drones
Procedure DivideFogArea()
Calculate the coverage requirements based on the significance and potential threats
    in each region
Group drones based on proximity and coverage requirements
Calculate the data distribution factor D_i for each fog area as $1/n_i$, where n_i is the number
    of drones in the fog area
Assign drones to fog areas based on proximity and coverage requirements
Monitor dynamic changes and adjust drone assignments as needed
Enable data sharing and collaboration among drones within each fog area
EndProcedure

additional data, GPS receivers provide exact location information, and cameras capture visual information (Figure 6.1). Since the base station is the main location for data processing, analysis, and collecting, it needs enough memory and storage.

- Start of itemize
- Bandwidth Savings (%): The percentage of bandwidth saved while using the data reduction method as opposed to sending data by default is shown in this column. The formula $(1 - (\text{Reduced Data Size}/\text{Default Data Size}))100$ can be used to calculate it.
- Cost Reduction (%): This column shows the portion of cost savings obtained by reducing the amount of data. It represents the possible savings on infrastructure that come with handling massive amounts of data. The computation might change based on the particular cost variables at play.

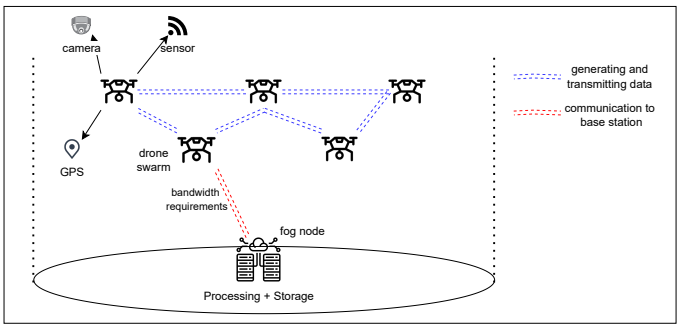

Figure 5.2: System implementation requirements

5.3.2 Communication Framework and Protocols

Strong protocols and communication frameworks are needed for the drones and base station to communicate data seamlessly. Real-time data flow between the drones and base station requires a dependable, low-latency connection. Depending on the technological stack and network architecture being used, different communication protocols may be employed. Common protocols include cellular networks, Wi-Fi, and specific protocols for drone communication like MAVLink. You may get a thorough explanation of this system component in Chapter 3.

5.3.3 Hardware and Software Requirements

The right hardware and software are required for the drones to be deployed successfully. Enough memory, processing power, and storage space are included in this. Cameras and sensors require compatibility as well as suitable data formats.

The control, data management, and transmission protocols of drones all require software. In order to receive, process, analyze, and visualize data, the base station requires software. Additionally, the system might use advanced algorithms for data processing and decision-making, compression methods, and data management software.

Table 5.1: Data Size Reduction in Drone-Based Systems

Number of Drones	**Default Data Size (KB)**	**Reduced Data Size (KB)**	**Splitting Count**	**Bandwidth Savings (%)**
5	25	20.96	663	16.16
6	30	25.42	684	15.26
7	35	28.27	1021	19.35
8	40	31.60	1192	21.00
9	45	32.18	1862	28.49
10	50	36.46	2049	27.08
11	55	37.81	2307	31.27
12	60	39.14	2496	34.76
13	65	41.02	2755	36.28
14	70	42.35	2981	39.50
15	75	43.69	3162	41.74

5.4 Results and discussion

Table 5.1 presents the findings from the studies carried out in the simulated setting. The number of drones employed in the simulation and the associated data volumes are displayed in the table both before and after the suggested data transmission reduction technique was applied.

The number of times the data was split during transmission is shown in the "number of splits" column.

The findings indicate that the default data size without reduction increases together with the number of drones. This is to be expected as more data is generated and transmitted by drones. However, the data size is much smaller than the default data when the suggested data transmission reduction option is used. This decrease in data size shows how well the suggested method works to maximize bandwidth use.

The outcomes demonstrate that the suggested approach effectively maximizes bandwidth use while minimizing data size, increasing the efficacy of data transmission. The suggested method divides data among several drones to efficiently share the burden and lower the possibility of network bottlenecks. Cost savings can be achieved by using this method, as it lessens the requirement for extra infrastructure to manage massive volumes of data.

5.5 Conclusion

By segmenting the fog area and effectively distributing data among drones, we presented a novel method in this chapter to optimize data transmission in IoT-based drone networks. We introduced the shot-by-shot acquisition strategy to reduce redundant data and presented an algorithm for fog area segmentation. Our test findings show that, in terms of cost savings, bandwidth optimization, and data transmission efficiency, our suggested method is both practical and successful. Our method has the potential to significantly increase UAV network performance, and we think it can also help improve other businesses that depend on drone technology.

Chapter 6

Improving multi-target tracking and monitoring system for collaborating drones within the Internet of Things

6.1 Introduction

The difficulties faced by surveillance drones have grown along with their capabilities. A critical problem occurs when a single drone recognizes more than one suspect at once inside its field of vision. This phenomenon poses a challenge, as the drone's capacity to track several objects at once is intrinsically restricted by elements like tracking precision, computing power, and the ability to physically observe multiple points of interest. As a result, a drone might not be able to track every recognized suspect in real-time, which could jeopardize the surveillance operation's overall efficacy.

In this chapter, we presented a novel method of separating the fog region and effectively distributing data among drones to enhance data transmission in Internet of Things-based drone networks. In order to minimize redundant data, we established the shot-by-shot acquisition approach and presented an algorithm for fog area segmentation. In terms of data transmission efficiency, bandwidth optimization, and cost reduction, our trial results show the viability and usefulness of our suggested approach. Our method, we think, has a great deal of promise to boost UAV network performance and can help progress a number of businesses that depend on drone technology.

6.2 Related work

As noted by Loayza et al. in their study [485], there are two possible approaches to designing the communication architecture between drones and a base station. This strategy has benefits for improving security and privacy. Conversely, a decentralized connection can enable drones to cover more ground more effectively, as demonstrated by the research conducted by Dawaliby et al. [486] and Azam et al. [487]. In order to maintain smooth communication, the decentralized solution also tackles the issue of restricted bandwidth between the drones and base station.

As noted in the review by Islam et al. [488], the intrinsic mobility of these devices makes the choice of connection technology critical and can result in varying connection stability. Because of the connection link's dynamic nature, a reliable and flexible communication system is required

to maintain communication even when the drones move and position themselves differently.

Innovative techniques have effectively handled the interference challenge, as demonstrated in the works of Xiang et al. [489] and Shen et al. [490]. They use a dynamic collaborative technique where UAVs are divided into sub-swarms, each of which is assigned a specific set of targets. Target switching times, tracking steps, and average total interference are all considerably decreased by using this method. This method maximizes UAV coordination to reduce interference and improve overall performance.

The usage of Jamming-Sensitive and single Case Tolerance (JSSCT) with Artificial Potential Field (APF) is suggested in path planning to overcome problems with jamming sensitivity and single cases. According to Wu et al.'s research [491], this method uses an iterative algorithm that combines Dinkelbach's algorithm with the Successive Convex Approximation (SCA) methodology. This integrated strategy optimizes energy consumption while managing the jamming issue effectively.

When combined, these cutting-edge techniques aid in the resolution of complex problems pertaining to jamming, interference, and best-path planning when it comes to unmanned aerial vehicle operations.

According to Cui et al.'s study [492], using deep reinforcement learning to path planning is a promising field. This method makes use of cutting-edge approaches to improve UAV decision-making in challenging circumstances.

Addressing the significant challenge of achieving efficient area coverage due to the high mobility of these devices, several authors have contributed noteworthy insights. Wu et al. [493] have developed a "Multi-constrained Cooperative Path Planning" algorithm, which focuses on optimizing area coverage while considering various constraints. Tang and Prabhakar's "R-DFS" algorithm employs Region Optimal Decomposition (ROD) and enhanced Depth-First-Search (DFS) techniques to generate coverage paths with minimized complexity [494]. The "SP2E" framework, introduced by Li et al., tackles coverage path planning in unknown environments, emphasizing minimal coverage and computation time while avoiding local extremums [495].

Cabreira et al. [496] have investigated ways to minimize energy consumption in the context of energy-efficient coverage path planning, taking into account variables like distance, speed, and ideal maneuvers. To illustrate the importance of visual information collecting, consider the pursuit of near-optimal visual coverage trajectories for quadrotor UAVs in 3D terrain [497].

Fevgas et al. provide a thorough analysis of cooperative strategies for energy-efficient coverage route planning algorithms, highlighting both advancements and potential future research areas [498]. Vasquez and colleagues [499] provide the basic ideas of coverage path planning, stressing its significance and examining several algorithmic techniques.

To handle the complexity of urban scenarios, Muñoz et al. [500] provide algorithms that prioritize formation maintenance and collision-free pathways in the context of path planning for

multi-UAV coverage in urban environments [501].

These joint efforts highlight the expanding corpus of literature focused on tackling the complex problems of maximizing UAV area coverage and path planning in both diversified and urban situations.

6.3 Problem Formulation

Drones with sophisticated sensors, cameras, and GPS modules may find and follow possible suspects in pre-marked regions. However, identifying and tracking many suspects within a drone's operational area at the same time has become increasingly difficult due to the surveillance drones' expanding capabilities.

6.3.1 Simultaneous Multi-Target Tracking Challenge

Imagine that a high-traffic area needs to be patrolled and monitored by a surveillance drone. This drone's sophisticated sensors and cameras are meant to detect and follow any suspicious activity inside its assigned area. A complicated issue arises when several suspects appear within the drone's area of vision. In many cases, the drone cannot effectively monitor every suspect that is spotted in real time due to a variety of physical limits, limited computational capacity, limited battery life, and other issues.

6.3.2 Constraints and Implications

Tracking many targets at once is made more difficult by the inherent limitations of individual drone capabilities. Despite the fact that contemporary drones are outfitted with sophisticated image processing and tracking algorithms, there is a limit to how many targets they can track at once. Due to this, a drone that encounters this difficulty may either monitor suspects incorrectly, give priority to some targets over others, or lose track of some suspects completely. These restrictions may make the surveillance operation less effective and make it more difficult to react quickly to new threats.

6.3.3 Collaborative Approach for Enhanced Tracking

A coordinated strategy is necessary to overcome the limitations of individual drones and enhance the effectiveness of multi-target tracking. Using the combined power of several drones, the objective is to efficiently track every suspect that has been identified in real time. The utilisation of a collaborative approach not only enhances the efficiency and efficacy of the surveillance operation overall, but also guarantees a thorough reaction to scenarios involving several targets.

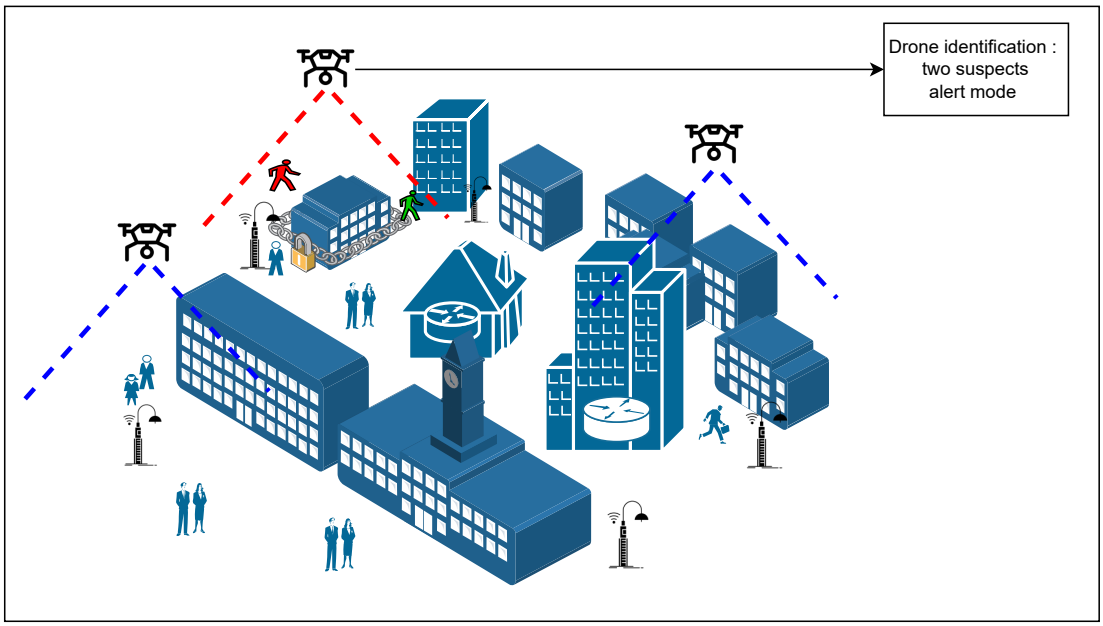

Figure 6.1: Multi-target surveillance challenge

6.4 Proposed Algorithm

This section introduces a new algorithm designed to enhance multi-target tracking and surveillance in Internet of Things scenarios. The algorithm makes use of the drones' cooperative efforts within the surveillance system to address the problem of tracking numerous suspects at once.

When a single drone's tracking capability is reached, the suggested algorithm uses a cooperative approach in which drones cooperate to track numerous suspects. It involves a number of actions, including as identifying potential suspects, allocating fresh tracking missions, and supporting drones. By dynamically dividing the tracking load across available drones, the objective is to increase tracking accuracy and optimize resource consumption. Figure 6.2 depicts how the collaborative system operates.

Suspect Detection and Information Sharing

When a drone finds more than one suspect inside its operational area, it collects relevant data about each one, such as position, photos, and other contextual information. The base station receives this data after which it is analyzed and decisions are made.

Assisting Drone Selection

Once a detection drone has provided information about several suspects, the base station evaluates the workload and capabilities of the drones that are accessible. It chooses suitable

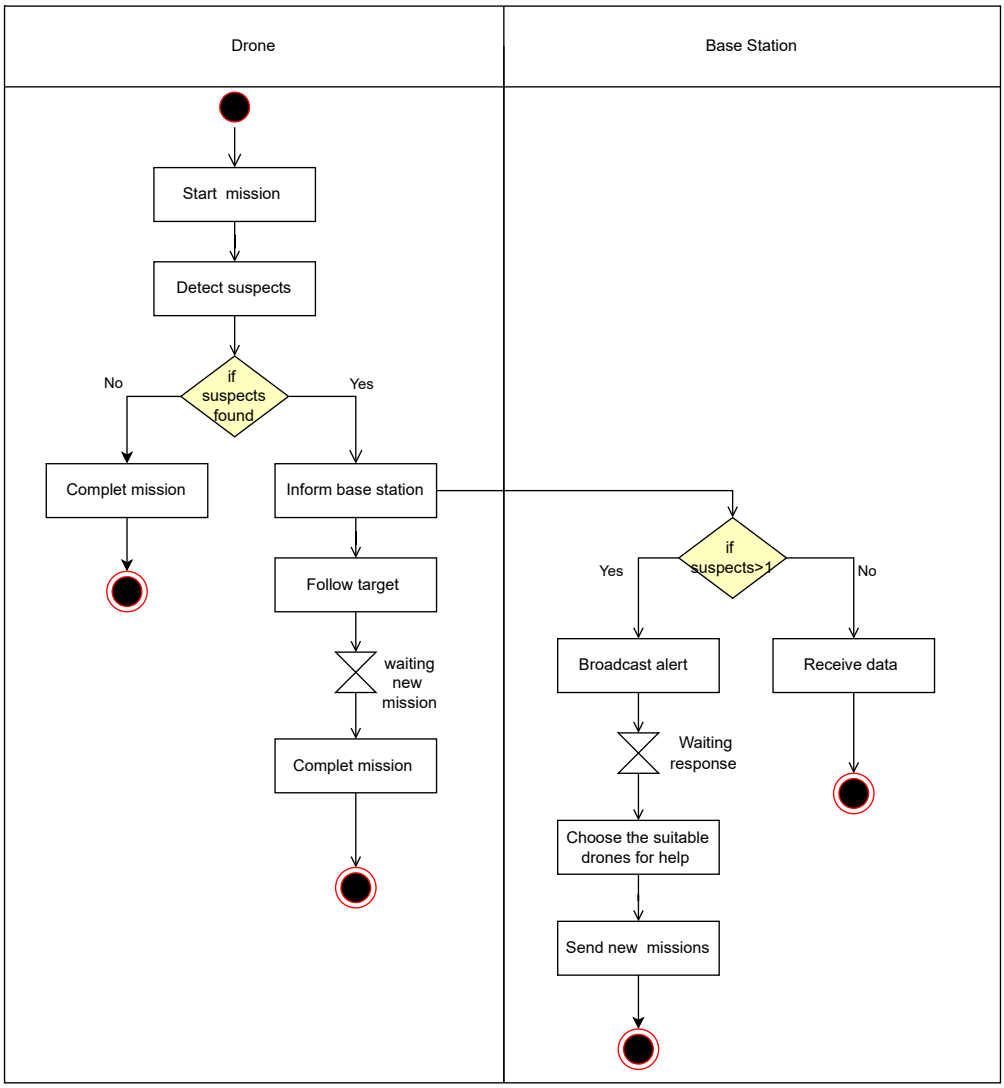

Figure 6.2: multi-target surveillance and tracking Algorithm

support drones according on their tracking capability, present tasks, and how close they are to the discovered suspects.

Mission Assignment and Collaboration

Selecting aiding drones, the base station gives them new tracking assignments. These missions require you to seek down the other suspects and stay in visual touch with them. The base station provides tracking objectives, suspect information, and mission data to the assisting drones.

Real-Time Collaboration and Data Fusion

The aiding drones collaborate to follow the extra suspect(s) while the detecting drone keeps tracking the original suspect(s). To enable coordinated tracking activities, they exchange real-time

position data, images, and tracking updates with the base station and one another.

Algorithm 13: Collaborative Multi-Target Tracking (Drone, Base Station)

Require: List of drones: `droneList`
Require: Base station: `baseStation`
Require: Detected suspects information: `detectedSuspects`
Ensure: Collaborative tracking assignments to drones

```
Procedure CollaborativeMultiTargetTracking(droneList, baseStation,
    detectedSuspects):
    // Step 1: Transmit suspect information from drones to base station
for all drone in droneList do
    if drone has detected multiple suspects then
        TransmitSuspectInfoToBaseStation(drone, detectedSuspects)
    end if
end for
    // Step 2: Base station assigns assisting drones to track additional suspects
for all drone in droneList do
    if drone has assisting drone assignment then
        assistingDrones = SelectAssistingDrones(baseStation, drone)
        AssignTrackingMissions(assistingDrones, detectedSuspects)
    end if
end for
    // Step 3: Assisting drones collaborate and track suspects
while surveillance ongoing do
    for all drone in droneList do
        if drone has active tracking mission then
            UpdateTrackingMission(drone)
            ShareTrackingInfoWithBaseStation(drone)
            ShareTrackingInfoWithOtherDrones(drone)
        end if
    end for
    // Other surveillance and tracking operations continue
end while
end procedure
```

6.5 System Architecture

The prior sections introduced the collaborative multi-target tracking algorithm, which functions inside a well-defined system architecture that includes drones, a base station, and their interactions. In the context of multi-target surveillance, this section describes the architectural elements, data flows, and communication protocols that facilitate smooth drone-base station collaboration (see Figure 6.3).

6.5.1 Drone Nodes

Every drone in the system is outfitted with a variety of sensors, such as GPS units, cameras, and other pertinent detectors. The drones can find, recognize, and follow suspects inside their operating areas thanks to these sensors. The collaborative algorithm receives the gathered data as inputs, which include photos and positional data. In order to provide real-time data interchange and coordination, drones can also wirelessly communicate with the base station and each other.

6.5.2 Base Station

The base station serves as the central control hub of the surveillance system. It receives suspect information from the drones, analyzes the data, and makes decisions based on the collaborative algorithm's directives. The base station manages the workload distribution among drones, assigns assisting drones to track additional suspects, and monitors the overall tracking operation's progress. Additionally, the base station facilitates communication between drones, ensuring that tracking data is shared effectively.

6.5.3 Data Exchange and Communication

Communication between the drones and the base station is critical to the cooperative multi-target tracking system's functionality. The drones provide relevant data to the base station, including tracking updates and information about potential suspects. From the base station, the drones in turn get tracking assignments, mission updates, and coordinating instructions. The entire surveillance operation remains coordinated and flexible in response to changing circumstances thanks to this two-way dialogue.

6.5.4 Communication Protocols

The system's communication protocols are developed to enable trustworthy and efficient data sharing. Drones, for instance, send data to the base station via wireless communication standards like Wi-Fi or cellular networks. Drones can communicate with each other in real time by using an effective and safe peer-to-peer protocol that allows tracking data to be sent instantly. Low latency interactions with the drones and data integrity are guaranteed by the base station connection protocol.

6.5.5 Scalability and Flexibility

The system architecture is designed to accommodate scalability and flexibility. As the number of drones and surveillance areas increases, the architecture can be extended to support a larger network of drones. Additionally, the system architecture is adaptable to different types of drones

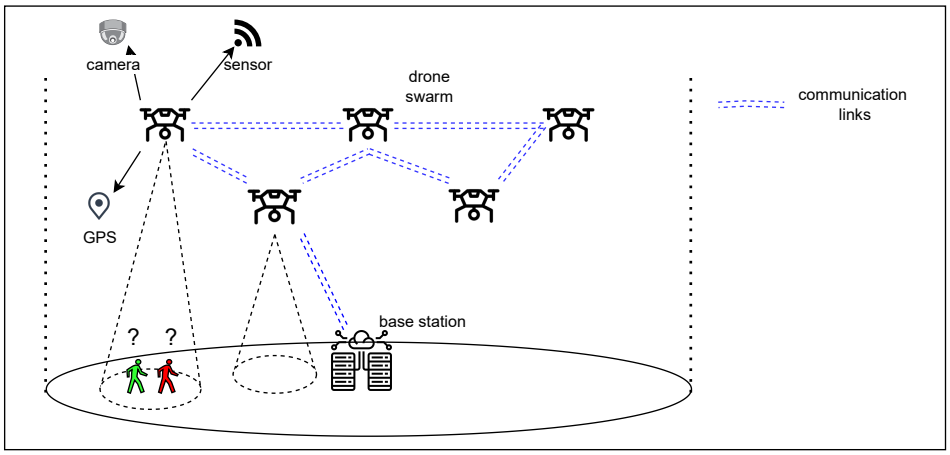

Figure 6.3: System architecture

with varying capabilities, ensuring that the collaborative algorithm can be applied to a diverse range of surveillance scenarios.

6.5.6 Visualization and User Interface

A visualization component of the system architecture shows real-time tracking data, suspect positions, and mission status to give operators situational awareness. This interface assists operators in making decisions, keeping an eye on the surveillance operation, and adjusting parameters as necessary.

6.6 System implementation

An extensive summary of the collaborative multi-target tracking algorithm's technical implementation in a practical setting is given in this section. Java's integration with the JADE framework makes it possible for drones and the base station to communicate seamlessly, allowing for efficient multi-target monitoring.

- **Software Architecture:** Java and the JADE (Java Agent Development Framework) are the foundation of the implementation, which aims to give the drones and base station a dynamic and interactive environment. Because the base station and every drone are modeled after JADE agents, they can communicate and work together effectively.
- **Agent Terminologies:** Modeled as individual JADE agents with unique functions and behaviors are suspects, the base station, and drones. The behaviors for detecting suspects, carrying out missions, and interacting with the base station are defined by the DroneAgent class.
- **Drone Representation and Suspect:** In a Cartesian coordinate system, a suspect is represented as a point with (x, y) coordinates. Similar to this, drones are shown as points

with a circular coverage zone that has a radius and a center (x, y).

- **Exchange with JADE:** The JADE architecture facilitates communication between agents. Agent Communication Language (ACL) is used by agents to communicate with one another. Messages containing suspected suspicions are periodically sent by the DroneAgent to the base station for examination.
- **Cooperative Multi-Target Monitoring System:** The collaborative multi-target tracking algorithm is the main implementation component. Every now and again, drones find suspects inside their coverage areas. The drone notifies the base station with suspect details if it detects more than one suspect.
- **Decision-Making on Base:** Drones send communications to the base station, which is used as a JADE agent, containing information that is questionable. The base station evaluates the situation, deploys support drones, and creates tracking missions in response to these messages.
- **Intelligent Tracking Cooperation:** Helping drones actively cooperate to follow suspects in real-time according on the mission assignments they get from the base station. They use JADE's messaging methods to share tracking data with the base station and each other.
- **Simulation Environment and Hardware:** Through controlled environment simulations, the implementation is verified. Using Java's capabilities, a realistic simulation of suspects, a base station, and drones is produced. Drones are programmed to carry out missions using algorithms, and suspects are generated at random.
- **Difficulties and Efficiency:** Issues with message handling and communication synchronization were resolved during deployment. To increase tracking accuracy and reduce transmission latency, optimization techniques were used.
- **Verification and Examination:** Using simulated scenarios, the implementation is put through a rigorous testing and validation process. The algorithm's performance in managing many suspects, real-time tracking collaboration, and base station decision-making is assessed through a variety of test cases.
- **Practicality and Scalability:** The application shows how the algorithm may be scaled to handle a growing number of mission assignments, suspects, and drones. The Java-JADE architecture demonstrates how the cooperative multi-target tracking system can be used in practical surveillance scenarios.

6.7 Experimental Setup

The cooperative multi-target tracking algorithm was tested using a carefully planned experimental configuration that combined JADE, Java, and simulated environments.

6.7.1 Simulation Environment and Agent Configuration

A Java-based simulation platform was designed and seamlessly linked with JADE to produce an authentic evaluation environment. The following was how the agents representing the base station, suspects, and drones were set up:

- **UAVs:** The effective area of observation of each drone was determined by its coverage radius, R_{drone}. The distance at which a drone could communicate with the base station was known as the communication range, or R_{comm}.
- **Base Station** The base station covered the whole simulation area because it was positioned in the middle of it.
- **Suspects:** Within the designated area, suspects were positioned at random coordinates (x, y).

6.7.2 Scenario Design and Communication

A number of scenarios were developed in order to assess how flexible the algorithm was in various circumstances. Through the manipulation of the number of drones N_{drones} and suspects $N_{suspects}$, the system's performance in various multi-target scenarios was examined. Through message exchanges, the JADE architecture enabled agents to communicate with one another. The ratio of successfully delivered messages to the total number of messages sent was used to compute the communication success rate, or CR.

6.7.3 Performance Metrics and Execution

The following performance measures were essential for calculating the algorithm's efficacy:

- **Detection Rate** DR**:** This metric represented the percentage of correctly detected suspects and was computed as:

$$DR = \frac{N_{correctlydetectedsuspects}}{N_{suspects}} 100\% \tag{6.1}$$

- **Tracking Precision** TP**:** Calculated as the average Euclidean distance between the actual suspect positions and their estimated positions, denoted by (x_{actual}, y_{actual}) and $(x_{estimated}, y_{estimated})$ respectively:

$$TP = \frac{1}{N_{suspects}} \sum_{i=1}^{N_{suspects}} \sqrt{(x_{actual} - x_{estimated})^2 + (y_{actual} - y_{estimated})^2} \tag{6.2}$$

- **Mission Duration** MD**:** The average time taken to complete tracking missions:

$$MD = \frac{1}{N_{missions}} \sum_{i=1}^{N_{missions}} MissionTime_i \tag{6.3}$$

In order to obtain statistically significant results and guarantee the robustness and reproducibility of the observations, the experiments were conducted several times.

6.8 Results and Analysis

This section contains the empirical findings from the collaborative multi-target tracking algorithm's experimental evaluation. We examine how well the algorithm performs in a range of situations, with a particular emphasis on multi-target surveillance scenarios.

6.8.1 Scenario-Based Performance

We carried out a number of tests with different scenarios to thoroughly assess the resilience and flexibility of the algorithm. The number of suspects and drones varied across the scenarios, reflecting a range of complexity levels found in real-world situations.

Detection Rate and Tracking Precision

A summary of the tracking accuracy (TP) and detection rate (DR) attained in various settings is provided in Table 6.1. The outcomes show how consistently the system finds suspects and determines their locations with accuracy.

Table 6.1: Detection Rate (DR) and Tracking Precision (TP) across scenarios.

Scenario	Suspects	Drones	DR (%)	TP
1	3	2	89.2	1.42
2	4	2	85.6	1.61
3	5	3	91.8	1.33
4	6	3	87.9	1.56
5	7	4	94.3	1.20
6	8	4	89.6	1.47
7	9	5	95.1	1.14
8	10	5	90.2	1.39
9	12	6	93.7	1.26
10	15	7	96.5	1.08

Mission Duration, Communication Success, and Message Load

The average mission time (MD), communication success rate (CR), and message load (ML) recorded in various circumstances are detailed in Table 6.2. The method reliably and efficiently completed missions while preserving a controlled message load.

Table 6.2: Average Mission Duration (MD), Communication Success Rate (CR), and Message Load (ML) across scenarios.

Scenario	MD (s)	CR (%)	ML
1	28.9	93	28
2	33.7	90	36
3	30.2	92	31
4	35.1	89	39
5	29.8	94	33
6	34.3	91	37
7	30.7	93	32
8	35.8	88	40
9	31.6	93	34
10	36.5	97	42

6.8.2 Discussion and Interpretation

The results presented in the tables demonstrate the effectiveness of the cooperative multi-target tracking method in a range of settings. Its reliable performance demonstrates how applicable it is in practical settings. Its efficient mission execution, controllable message load, and strong communication architecture are important components that make it effective.

The algorithm has the potential to improve multi-target tracking in IoT-driven surveillance settings, according to a quantitative examination of the data. Because of its adaptability, it presents itself as a viable option for implementation in real-world situations.

6.9 Conclusion

This chapter introduces a collaborative multi-target tracking algorithm tailored for IoT-driven surveillance environments. Through experimentation across 10 scenarios, the algorithm demonstrates proficiency in suspect detection, accurate tracking, and mission management. Performance metrics, encompassing detection rate, tracking precision, mission duration, communication success, and message load, collectively highlight its transformative potential in multi-target tracking operations.

As technology evolves, the algorithm holds promise for bolstering surveillance and security applications. Future research directions may involve algorithm refinement, real-world implementations, and evaluation under more complex conditions.

The collaborative multi-target tracking algorithm, with its versatility and performance, represents a significant advancement in IoT-based surveillance systems.

Conclusion And Perspectives

Summary and Implications

This thesis has explored the significant potential of drones in various applications, including public safety, emergency response, disaster management, and surveillance. The agility and rapid tracking capabilities of drones enable them to navigate challenging areas and relay precise information on critical situations. However, the compact size and lightweight design necessary for optimal speed and operational efficiency impose limitations on the drone's components, necessitating continuous communication with a base station for information transmission and directive reception.

The integration of Internet of Things applications across diverse sectors has significantly enhanced communication, facilitating efficient task execution and rapid acquisition of precise information. Despite the crucial role of drones in the IoT framework, their continuous communication with ground stations faces numerous challenges, including network disruptions due to the inherent movement of drones and external factors like wind. These disruptions critically hamper drone operations, inhibit the transmission of position data, and prevent the reception of guidelines from the base station, leading to potential disorientation and loss of valuable mission-collected information.

Fog nodes play a vital role in mitigating high computational, communication, and network latency, as well as bandwidth in IoT systems. However, the constrained resources at fog nodes can lead to overload issues during periods of high traffic, directly impacting the capacity and quality of service and potentially compromising the efficiency and responsiveness of the entire IoT system.

The thesis focuses on enhancing the integrity of drones operating within the IoT environment. The challenge of drone loss in fog computing systems is addressed by proposing a drone recovery system. This system aims to prevent drone crashes by intervening before potential incidents occur. Simulations demonstrate promising results regarding the effectiveness of this protocol.

Additionally, a dynamic fog computing system is proposed to tackle high-traffic situations in fog nodes. This system aims to safeguard data from loss and protect fog nodes from overload scenarios. Experimentation within the university validates the efficacy of these protocols in real-world scenarios.

Furthermore, two additional protocols are introduced aimed at minimizing data redundancy and enhancing collaboration among drones. These protocols are designed to improve drone

efficiency, reduce errors, and mitigate losses during collaborative missions.

In summary, the research contributes to strengthening drone integrity within IoT environments by addressing issues such as drone loss, high-traffic situations, data protection, and collaborative missions. The findings offer practical solutions to enhance the overall effectiveness and reliability of drones in IoT applications.

Future Directions

Despite extensive research on the conceptual and theoretical foundations of fog computing, there remains a gap in effectively managing the partitioning of fog nodes without compromising data integrity or overall system performance. Future research should focus on developing innovative solutions to this problem, such as implementing 'Fog as a Service' partitions. Additionally, enhancing the robustness and reliability of drone communication with ground stations is crucial. This will not only improve the performance of drones but also expand their potential applications within the IoT framework.

Bibliography

[1] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Internet of things (iot) communication protocols," in 2017 8th International conference on information technology (ICIT), pp. 685–690, IEEE, 2017.

[2] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," Journal of internet services and applications, vol. 1, pp. 7–18, 2010.

[3] P. Hu, S. Dhelim, H. Ning, and T. Qiu, "Survey on fog computing: architecture, key technologies, applications and open issues," Journal of network and computer applications, vol. 98, pp. 27–42, 2017.

[4] L. Farhan, S. T. Shukur, A. E. Alissa, M. Alrweg, U. Raza, and R. Kharel, "A survey on the challenges and opportunities of the internet of things (iot)," in 2017 Eleventh International Conference on Sensing Technology (ICST), pp. 1–5, IEEE, 2017.

[5] D. G. Pivoto, L. F. de Almeida, R. da Rosa Righi, J. J. Rodrigues, A. B. Lugli, and A. M. Alberti, "Cyber-physical systems architectures for industrial internet of things applications in industry 4.0: A literature review," Journal of manufacturing systems, vol. 58, pp. 176–192, 2021.

[6] Y. A. Qadri, A. Nauman, Y. B. Zikria, A. V. Vasilakos, and S. W. Kim, "The future of healthcare internet of things: a survey of emerging technologies," IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1121–1167, 2020.

[7] H. F. Azgomi and M. Jamshidi, "A brief survey on smart community and smart transportation," in 2018 IEEE 30th international conference on tools with artificial intelligence (ICTAI), pp. 932–939, IEEE, 2018.

[8] B. Diène, J. J. Rodrigues, O. Diallo, E. H. M. Ndoye, and V. V. Korotaev, "Data management techniques for internet of things," Mechanical Systems and Signal Processing, vol. 138, p. 106564, 2020.

[9] K. P. Valavanis, "Advances in unmanned aerial vehicles: state of the art and the road to autonomy," 2008.

[10] M. Hassanalian and A. Abdelkefi, "Classifications, applications, and design challenges of drones: A review," Progress in Aerospace Sciences, vol. 91, pp. 99–131, 2017.

[11] J. Shahmoradi, E. Talebi, P. Roghanchi, and M. Hassanalian, "A comprehensive review of applications of drone technology in the mining industry," Drones, vol. 4, no. 3, p. 34, 2020.

[12] L. Brooke-Holland, "Unmanned aerial vehicles (drones): an introduction," House of Commons Library: London, UK, 2012.

[13] M. Arjomandi, S. Agostino, M. Mammone, M. Nelson, and T. Zhou, "Classification of unmanned aerial vehicles," Report for Mechanical Engineering class, University of Adelaide, Adelaide, Australia, pp. 1–48, 2006.

[14] R. Weibel and R. J. Hansman, "Safety considerations for operation of different classes of uavs in the nas," in Aiaa 4th aviation technology, integration and operations (atio) forum, p. 6244, 2004.

[15] S. Lee and Y. Choi, "Reviews of unmanned aerial vehicle (drone) technology trends and its applications in the mining industry," Geosystem Engineering, vol. 19, no. 4, pp. 197–204, 2016.

[16] P. Wang, R. Valerdi, S. Zhou, and L. Li, "Introduction: Advances in iot research and applications," Information Systems Frontiers, vol. 17, pp. 239–241, 2015.

[17] J. Wang, M. K. Lim, C. Wang, and M.-L. Tseng, "The evolution of the internet of things (iot) over the past 20 years," Computers & Industrial Engineering, vol. 155, p. 107174, 2021.

[18] E. Bertino, K.-K. R. Choo, D. Georgakopolous, and S. Nepal, "Internet of things (iot) smart and secure service delivery," 2016.

[19] A. S. Abdul-Qawy, P. Pramod, E. Magesh, and T. Srinivasulu, "The internet of things (iot): An overview," International Journal of Engineering Research and Applications, vol. 5, no. 12, pp. 71–82, 2015.

[20] S. Kuyoro, F. Osisanwo, and O. Akinsowon, "Internet of things (iot): an overview," in Proc. of the 3th International Conference on Advances in Engineering Sciences and Applied Mathematics (ICAESAM), pp. 23–24, 2015.

[21] H. N. Saha, N. Saha, R. Ghosh, and S. Roychoudhury, "Recent trends in implementation of internet of things—a review," in 2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), pp. 1–6, IEEE, 2016.

[22] K. A. M. Zeinab and S. A. A. Elmustafa, "Internet of things applications, challenges and related future technologies," World Scientific News, vol. 67, no. 2, pp. 126–148, 2017.

[23] Y. Perwej, M. A. AbouGhaly, B. Kerim, and H. A. M. Harb, "An extended review on internet of things (iot) and its promising applications," Communications on Applied Electronics (CAE), ISSN, pp. 2394–4714, 2019.

[24] P. Sethi, S. R. Sarangi, et al., "Internet of things: architectures, protocols, and applications," Journal of electrical and computer engineering, vol. 2017, 2017.

[25] I. Initiative, R. Minerva, A. Biru, and D. Rotondi, "Towards a definition of the internet of things (iot)," Revision-1, on-line: http://iot. ieee. org/images/files/pdf/IEEE IoT Towards Definition Internet of Things Revision1 27MAY15. pdf. Accessed, vol. 27, no. 2017, pp. 479–501, 2015.

[26] M. Bunz and G. Meikle, The internet of things. John Wiley & Sons, 2017.

[27] X.-Y. Chen and Z.-G. Jin, "Research on key technology and applications for internet of things," Physics Procedia, vol. 33, pp. 561–566, 2012.

[28] H. Liu, "Research on key technology for internet of things," Computer Era, vol. 7, 2010.

[29] Z. Yang, Y. Yue, Y. Yang, Y. Peng, X. Wang, and W. Liu, "Study and application on the architecture and key technologies for iot," in 2011 International Conference on Multimedia Technology, pp. 747–751, IEEE, 2011.

[30] S. K. Goudos, P. I. Dallas, S. Chatziefthymiou, and S. Kyriazakos, "A survey of iot key enabling and future technologies: 5g, mobile iot, sematic web and applications," Wireless Personal Communications, vol. 97, pp. 1645–1675, 2017.

[31] K. Iniewski, "Smart sensors for industrial applications," 2017.

[32] M. J. McGrath, C. N. Scanaill, M. J. McGrath, and C. N. Scanaill, "Sensing and sensor fundamentals," Sensor technologies: Healthcare, wellness, and environmental applications, pp. 15–50, 2013.

[33] C.-M. Kyung, H. Yasuura, Y. Liu, and Y.-L. Lin, "Smart sensors and systems," Cham, Switzerland: Springer, 2017.

[34] M. Tabib-Azar and G. Beheim, "Optical temperature sensors," Integrated Optics, Microstructures, and Sensors, pp. 285–313, 1995.

[35] D. Prasad and V. Nath, "An overview of temperature sensors," in Proceeding of the Second International Conference on Microelectronics, Computing & Communication Systems (MCCS 2017), pp. 777–784, Springer, 2019.

[36] M. Szczerska, "Temperature sensors based on polymer fiber optic interferometer. chemosensors 2022, 10, 228," 2022.

[37] A. A. Zaher, "Smart temperature sensors: History, current practices, and future trends," in Process Analysis, Design, and Intensification in Microfluidics and Chemical Engineering, pp. 223–250, IGI Global, 2019.

[38] J. A. Chiou, "Pressure sensors in automotive applications and future challenges," in ASME International Mechanical Engineering Congress and Exposition, vol. 16387, pp. 525–530, American Society of Mechanical Engineers, 1999.

[39] C. Cavalloni and J. von Berg, "Overview: Principles and technologies for pressure sensors for automotive applications," Advanced Microsystems for Automotive Applications Yearbook 2002, pp. 232–242, 2002.

[40] S. Büttgenbach, I. Constantinou, A. Dietzel, M. Leester-Schädel, S. Büttgenbach, I. Constantinou, A. Dietzel, and M. Leester-Schädel, "Piezoresistive pressure sensors," Case Studies in Micromechatronics: From Systems to Processes, pp. 21–85, 2020.

[41] D. Tyler, "Application of pressure sensors in monitoring pressure," Materials and technology for sportswear and performance apparel, pp. 289–309, 2015.

[42] N. K. Aziz, J. Champion, and I. I. Hamarash, "Evaluation of smartphone's embedded sensors through applications: A case study of gyroscope and accelerometer," UKH Journal of Science and Engineering, vol. 5, no. 2, pp. 10–17, 2021.

[43] D. K. Shaeffer, "Mems inertial sensors: A tutorial overview," IEEE Communications Magazine, vol. 51, no. 4, pp. 100–109, 2013.

[44] M. Shoaib, S. Bosch, O. D. Incel, H. Scholten, and P. J. Havinga, "Fusion of smartphone motion sensors for physical activity recognition," Sensors, vol. 14, no. 6, pp. 10146–10176, 2014.

[45] A. Das, N. Borisov, and M. Caesar, "Tracking mobile web users through motion sensors: Attacks and defenses.," in NDSS, 2016.

[46] H.-K. Lee, S.-I. Chang, and E. Yoon, "Acapacitive proximity sensor in dual implementation with tactile imaging capability on a single flexible platform for robot assistant applications,"

[47] H.-K. Lee, S.-I. Chang, and E. Yoon, "Dual-mode capacitive proximity sensor for robot application: Implementation of tactile and proximity sensing capability on a single polymer platform using shared electrodes," IEEE sensors journal, vol. 9, no. 12, pp. 1748–1755, 2009.

[48] B. Bury, "Proximity sensing for robots," in IEE Colloquium on Robot Sensors, pp. 3–1, IET, 1991.

[49] D. Göger, H. Alagi, and H. Wörn, "Tactile proximity sensors for robotic applications," in 2013 IEEE International Conference on Industrial Technology (ICIT), pp. 978–983, IEEE, 2013.

[50] A. Polzer, W. Gaberl, and H. Zimmermann, "Filter-less vertical integrated rgb color sensor for light monitoring," in 2011 Proceedings of the 34th International Convention MIPRO, pp. 55–59, IEEE, 2011.

[51] A. Pandharipande and S. Li, "Light-harvesting wireless sensors for indoor lighting control," IEEE Sensors journal, vol. 13, no. 12, pp. 4599–4606, 2013.

[52] G. R. Newsham and C. Arsenault, "A camera as a sensor for lighting and shading control," Lighting Research & Technology, vol. 41, no. 2, pp. 143–163, 2009.

[53] V. M. Ionescu, "Exploiting the ambient light sensor to track user environment information," in 2016 15th RoEduNet Conference: Networking in Education and Research, pp. 1–6, IEEE, 2016.

[54] G. Jimenez-Cadena, J. Riu, and F. X. Rius, "Gas sensors based on nanostructured materials," Analyst, vol. 132, no. 11, pp. 1083–1099, 2007.

[55] D.-D. Lee and D.-S. Lee, "Environmental gas sensors," IEEE sensors journal, vol. 1, no. 3, pp. 214–224, 2001.

[56] R. A. Potyrailo, "Multivariable sensors for ubiquitous monitoring of gases in the era of internet of things and industrial internet," Chemical reviews, vol. 116, no. 19, pp. 11877–11923, 2016.

[57] C. Schueler and L. Woody, "Digital electro-optical imaging sensors," International Journal of Imaging Systems and Technology, vol. 4, no. 3, pp. 170–200, 1992.

[58] S. Ozawa, "Image sensors in traffic and vehicle control," in Proceedings of VNIS'94-1994 Vehicle Navigation and Information Systems Conference, pp. PLEN27–PLEN34, IEEE, 1994.

[59] J.-R. Riba, "Application of image sensors to detect and locate electrical discharges: a review," Sensors, vol. 22, no. 15, p. 5886, 2022.

[60] M. De Bakker, P. Verbeek, E. Nieuwkoop, and G. Steenvoorden, "A smart range image sensor," in Proceedings of the 24th European Solid-State Circuits Conference, pp. 208–211, IEEE, 1998.

[61] V. Conti, C. Militello, F. Sorbello, and S. Vitabile, "Biometric sensors rapid prototyping on field-programmable gate arrays," The Knowledge Engineering Review, vol. 30, no. 2, pp. 201–219, 2015.

[62] T. Sabhanayagam, V. P. Venkatesan, and K. Senthamaraikannan, "A comprehensive survey on various biometric systems," International Journal of Applied Engineering Research, vol. 13, no. 5, pp. 2276–2297, 2018.

[63] B. Miller, "Vital signs of identity [biometrics]," IEEE spectrum, vol. 31, no. 2, pp. 22–30, 1994.

[64] Z. Zhang, Z. Liu, M. Sinclair, A. Acero, L. Deng, J. Droppo, X. Huang, and Y. Zheng, "Multi-sensory microphones for robust speech detection, enhancement and recognition," in 2004 IEEE International Conference on Acoustics, Speech, and Signal Processing, vol. 3, pp. iii–781, IEEE, 2004.

[65] J. Parry, "Microphone arrays for desktop computers and speech recognition," in International Conference on Acoustics, Speech, and Signal Processing, pp. 1149–1151, IEEE, 1990.

[66] K. Kiyohara, Y. Kaneda, S. Takahashi, H. Nomura, and J. Kijima, "A microphone array system for speech recognition," in 1997 IEEE International Conference on Acoustics, Speech, and Signal Processing, vol. 1, pp. 215–218, IEEE, 1997.

[67] M. S. Brandstein and H. F. Silverman, "A practical methodology for speech source localization with microphone arrays," Computer Speech & Language, vol. 11, no. 2, pp. 91–126, 1997.

[68] J. Dimmock, "Infrared detectors and applications," Journal of Electronic materials, vol. 1, pp. 255–309, 1972.

[69] R. Lenggenhager and H. Baltes, CMOS thermoelectric infrared sensors. ETH Zurich, 1994.

[70] R. Usamentiaga, P. Venegas, J. Guerediaga, L. Vega, J. Molleda, and F. G. Bulnes, "Infrared thermography for temperature measurement and non-destructive testing," Sensors, vol. 14, no. 7, pp. 12305–12348, 2014.

[71] J.-J. Yon, E. Mottin, L. Biancardini, L. Letellier, and J. Tissot, "Infrared microbolometer sensors and their application in automotive safety," in Advanced Microsystems for Automotive Applications 2003, pp. 137–157, Springer, 2003.

[72] J. Lee, "Apply force/torque sensors to robotic applications," Robotics, vol. 3, no. 2, pp. 189–194, 1987.

[73] W. A. Lorenz, M. A. Peshkin, and J. E. Colgate, Force sensors for human/robot interaction. PhD thesis, Northwestern University, 1999.

[74] D. J. Beebe, A. S. Hsieh, D. D. Denton, and R. G. Radwin, "A silicon force sensor for robotics and medicine," Sensors and Actuators A: Physical, vol. 50, no. 1-2, pp. 55–65, 1995.

[75] A. Sadun, J. Jalani, and J. Sukor, "Force sensing resistor (fsr): a brief overview and the low-cost sensor for active compliance control," in First international workshop on pattern recognition, vol. 10011, pp. 222–226, SPIE, 2016.

[76] M. J. Caruso and L. S. Withanawasam, "Vehicle detection and compass applications using amr magnetic sensors," in Sensors Expo Proceedings, vol. 477, p. 39, 1999.

[77] J. P. Heremans, "Magnetic field sensors for magnetic position sensing in automotive applications," MRS Online Proceedings Library (OPL), vol. 475, p. 63, 1997.

[78] M. J. Caruso, "Applications of magnetoresistive sensors in navigation systems," tech. rep., SAE Technical Paper, 1997.

[79] M. F. Kuhn, G. P. Breier, A. R. Dias, and T. G. Clarke, "A novel rfid-based strain sensor for wireless structural health monitoring," Journal of Nondestructive Evaluation, vol. 37, pp. 1–10, 2018.

[80] M. Nie, Y.-h. Xia, and H.-s. Yang, "A flexible and highly sensitive graphene-based strain sensor for structural health monitoring," Cluster Computing, vol. 22, pp. 8217–8224, 2019.

[81] C. Liu, J. Teng, N. Wu, et al., "A wireless strain sensor network for structural health monitoring," Shock and Vibration, vol. 2015, 2015.

[82] M. Jamuna and A. V. Prakash, "A study of communication protocols for internet of things (iot) devices," in 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021), pp. 262–268, Atlantis Press, 2021.

[83] Y. Cheng, H. Zhang, and Y. Huang, "Overview of communication protocols in internet of things: architecture, development and future trends," in 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI), pp. 627–630, IEEE, 2018.

[84] R. Roges, "Communication protocols for smart sensors in iot applications," International Journal of Intelligent Communication, Computing, and Networks, vol. 1, no. 2.

[85] G. Kumar and P. Tomar, "A survey of ipv6 addressing schemes for internet of things," International Journal of Hyperconnectivity and the Internet of Things (IJHIoT), vol. 2, no. 2, pp. 43–57, 2018.

[86] B. Feldner and P. Herber, "A qualitative evaluation of ipv6 for the industrial internet of things," Procedia Computer Science, vol. 134, pp. 377–384, 2018.

[87] J.-P. Vasseur and A. Dunkels, Interconnecting smart objects with ip: The next internet. Morgan Kaufmann, 2010.

[88] S. Ziegler, A. Skarmeta, P. Kirstein, and L. Ladid, "Evaluation and recommendations on ipv6 for the internet of things," in 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), pp. 548–552, IEEE, 2015.

[89] S. N. Han, Q. H. Cao, B. Alinia, and N. Crespi, "Design, implementation, and evaluation of 6lowpan for home and building automation in the internet of things," in 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA), pp. 1–8, IEEE, 2015.

[90] B. Pediredla, I. Kevin, K. Wang, Z. Salcic, and A. Ivoghlian, "A 6lowpan implementation for memory constrained and power efficient wireless sensor nodes," in IECON 2013-39th Annual Conference of the IEEE Industrial Electronics Society, pp. 4432–4437, IEEE, 2013.

[91] L. F. Schrickte, C. B. Montez, R. S. D. Oliveira, and A. S. R. Pinto, "Design and implementation of a 6lowpan gateway for wireless sensor networks integration with the internet of things," International Journal of Embedded Systems, vol. 8, no. 5-6, pp. 380–390, 2016.

[92] C. L. Devasena, "Ipv6 low power wireless personal area network (6lowpan) for networking internet of things (iot)–analyzing its suitability for iot," Indian Journal of Science and Technology, vol. 9, no. 30, pp. 1–6, 2016.

[93] J. Chen and X. Zhou, "Zigbee wireless communication technology in industrial controls," Radio Engineering of China, vol. 36, no. 6, pp. 61–64, 2006.

[94] A. Kanwar and A. Khazanchi, "Zigbee: The new bluetooth technology," International Journal Of Engineering And Computer Science, vol. 1, no. 2, pp. p67–74, 2012.

[95] J.-S. Lee, C.-C. Chuang, and C.-C. Shen, "Applications of short-range wireless technologies to industrial automation: A zigbee approach," in 2009 Fifth Advanced International Conference on Telecommunications, pp. 15–20, IEEE, 2009.

[96] N. A. Somani and Y. Patel, "Zigbee: A low power wireless technology for industrial applications," International Journal of Control Theory and Computer Modelling (IJCTCM), vol. 2, no. 3, pp. 27–33, 2012.

[97] C. Gomez, J. Oller, and J. Paradells, "Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology," sensors, vol. 12, no. 9, pp. 11734–11753, 2012.

[98] S. Ashok and R. Krishnaiah, "Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology," International Journal, vol. 3, no. 9, pp. 11734–11753, 2013.

[99] A. Nikoukar, M. Abboud, B. Samadi, M. Güneş, and B. Dezfouli, "Empirical analysis and modeling of bluetooth low-energy (ble) advertisement channels," in 2018 17th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net), pp. 1–6, IEEE, 2018.

[100] M. B. Yassein, W. Mardini, and A. Khalil, "Smart homes automation using z-wave protocol," in 2016 International Conference on Engineering & MIS (ICEMIS), pp. 1–6, IEEE, 2016.

[101] C. Paetz, Z-wave basics: remote control in smart homes. CreateSpace Independent Publishing Platform, 2013.

[102] B. Fouladi and S. Ghanoun, "Security evaluation of the z-wave wireless protocol," Black hat USA, vol. 24, pp. 1–2, 2013.

[103] B. Bilginer and P.-L. Ljunggren, "Near field communication," 2011.

[104] S. Burkard, "Near field communication in smartphones," Dep. of Telecommunication Systems, Service-centric Networking, Berlin Institute of Technology, Germany, 2012.

[105] S. Ortiz, "Is near-field communication close to success?," computer, vol. 39, no. 3, pp. 18–20, 2006.

[106] G. Jain and S. Dahiya, "Nfc?: Advantages, limits and future scope," vol, vol. 4, pp. 1–12, 2015.

[107] M. Carandell Widmer, D. Toma, J. d. Río Fernandez, K. Ganchev, and J. Peudennier, "Evaluation of sigfox lpwan technology for autonomous sensors in coastal applications," Instrumentation Viewpoint, no. 20, pp. 36–37, 2018.

[108] J. C. Zuniga and B. Ponsard, "Sigfox system description," LPWAN@ IETF97, Nov. 14th, vol. 25, p. 14, 2016.

[109] N. I. M. Osman and E. B. Abbas, "Performance evaluation of lora and sigfox lpwan technologies for iot," Acad. J. Res. Sci. Publ, vol. 4, 2022.

[110] Y.-P. E. Wang, X. Lin, A. Adhikary, A. Grovlen, Y. Sui, Y. Blankenship, J. Bergman, and H. S. Razaghi, "A primer on 3gpp narrowband internet of things," IEEE communications magazine, vol. 55, no. 3, pp. 117–123, 2017.

[111] N. Mangalvedhe, R. Ratasuk, and A. Ghosh, "Nb-iot deployment study for low power wide area cellular iot," in 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pp. 1–6, IEEE, 2016.

[112] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "Overview of cellular lpwan technologies for iot deployment: Sigfox, lorawan, and nb-iot," in 2018 ieee international conference on pervasive computing and communications workshops (percom workshops), pp. 197–202, IEEE, 2018.

[113] H. Kashif, M. N. Khan, and Q. Awais, "Selection of network protocols for internet of things applications: A review," in 2020 IEEE 14th international conference on semantic computing (ICSC), pp. 359–362, IEEE, 2020.

[114] M. Bawa and D. Cagáňová, "Selecting network protocols for internet of things based upon innovation and knowledge management," J. Telecommun. Syst. Manag, vol. 7, no. 2, pp. 1–4, 2018.

[115] W. Ejaz, A. Anpalagan, W. Ejaz, and A. Anpalagan, "Communication technologies and protocols for internet of things," Internet of Things for Smart Cities: Technologies, Big Data and Security, pp. 17–30, 2019.

[116] L. Qian, Z. Luo, Y. Du, and L. Guo, "Cloud computing: An overview," in Cloud Computing: First International Conference, CloudCom 2009, Beijing, China, December 1-4, 2009. Proceedings 1, pp. 626–631, Springer, 2009.

[117] Q. Chen and Q. Deng, "Cloud computing and its key techniques: Cloud computing and its key techniques," Journal of Computer Applications, vol. 29, pp. 2562–2567, 2009.

[118] P. Mell and T. Grance, "The nist definition of cloud computing," vol. 23, pp. 50–50, 2011.

[119] D. W. Sun, M. Fu, L. Zhu, G. Li, and Q. Lu, "Non-intrusive anomaly detection with streaming performance metrics and logs for devops in public clouds: A case study in aws," IEEE Transactions on Emerging Topics in Computing, vol. 4, pp. 278–289, 2016.

[120] L. Sheng-w, "Research on security framework of enterprise private cloud computing platform," Modern Electronics Technique, 2014.

[121] L. Bi, "Enterprise network storage architecture based private cloud networks," Computer Knowledge and Technology, 2014.

[122] L. Bittencourt, E. Madeira, and N. Fonseca, "Impact of communication uncertainties on workflow scheduling in hybrid clouds," 2012 IEEE Global Communications Conference (GLOBECOM), pp. 1623–1628, 2012.

[123] Y. Dong, W. Liu, L. Zhao, H. Zhang, and K. Wang, "Research and implementing of software defined border protection in hybrid cloud," DEStech Transactions on Engineering and Technology Research, 2017.

[124] M. Imazaki, S. Kaneko, N. Komoda, and T. Ohkawa, "Evaluation of data optimal storage system in hybrid cloud," Proceedings of the International Conferences on Applied Computing 2022 and WWW/Internet 2022, 2022.

[125] F. Hao, G. Min, J. Chen, F. Wang, M. Lin, C. Luo, and L. Yang, "An optimized computational model for multi-community-cloud social collaboration," IEEE Transactions on Services Computing, vol. 7, pp. 346–358, 2014.

[126] J. Jimenez, R. Baig, P. Garcia, A. M. Khan, F. Freitag, L. Navarro-Moldes, E. Pietrosemoli, M. Zennaro, A. H. Payberah, and V. Vlassov, "Supporting cloud deployment in the guifi.net community network," Global Information Infrastructure Symposium - GIIS 2013, pp. 1–3, 2013.

[127] J. Gibson, R. Rondeau, D. Eveleigh, and Q. Tan, "Benefits and challenges of three cloud computing service models," 2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN), pp. 198–205, 2012.

[128] M. Tanque, "Cloud-based platforms and infrastructures," Cloud Security, 2019.

[129] L. Wang, L. F. Pires, A. Wombacher, M. J. van Sinderen, and C. Chi, "Stakeholder interactions to support service creation in cloud computing," in 2010 14th IEEE International Enterprise Distributed Object Computing Conference Workshops, pp. 173–176, IEEE, 2010.

[130] B. Joshi, M. Shrivastava, and B. Joshi, "Security threats and their mitigation in infrastructure as a service," Perspectives on Science, vol. 8, pp. 462–464, 2016.

[131] R. Dukaric and M. B. Juric, "Towards a unified taxonomy and architecture of cloud frameworks," Future Gener. Comput. Syst., vol. 29, pp. 1196–1210, 2013.

[132] C. Ardagna, E. Damiani, F. Frati, D. Rebeccani, and M. Ughetti, "Scalability patterns for platform-as-a-service," 2012 IEEE Fifth International Conference on Cloud Computing, pp. 718–725, 2012.

[133] N. Ganesh and G. Mamatha, "Enabling platform-as-a-service through a consolidated resource manager," IOSR Journal of Computer Engineering, vol. 16, pp. 24–28, 2014.

[134] L. zhen Cui, J. Tian, H. Wang, and Q. Li, "Service cooperation in paas platform based on planning method," Proceedings of the 2011 15th International Conference on Computer Supported Cooperative Work in Design (CSCWD), pp. 367–374, 2011.

[135] H. Katzan and W. Dowling, "Software-as-a-service economics," vol. 14, 2010.

[136] Y. Liu, Y. Sun, J. Ryoo, S. Rizvi, and A. Vasilakos, "A survey of security and privacy challenges in cloud computing: Solutions and future directions," J. Comput. Sci. Eng., vol. 9, 2015.

[137] Z. Tari, X. Yi, U. Premarathne, P. Bertók, and I. Khalil, "Security and privacy in cloud computing: Vision, trends, and challenges," IEEE Cloud Computing, vol. 2, pp. 30–38, 2015.

[138] A. N. Khan, M. M. Kiah, S. Khan, S. Madani, and A. R. Khan, "A study of incremental cryptography for security schemes in mobile cloud computing environments," 2013 IEEE Symposium on Wireless Technology & Applications (ISWTA), pp. 62–67, 2013.

[139] M. Kolhar, M. MujthabaG., and A. Alameen, "Cloud servers and fog or edge computing with their limitations & challenges," 2018.

[140] M. Aazam, I. Khan, A. A. Alsaffar, and E.-N. Huh, "Cloud of things: Integrating internet of things and cloud computing and the issues involved," in Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 14th-18th January, 2014, pp. 414–419, IEEE, 2014.

[141] C. C. Byers, "Architectural imperatives for fog computing: Use cases, requirements, and architectural techniques for fog-enabled iot networks," IEEE Communications Magazine, vol. 55, no. 8, pp. 14–20, 2017.

[142] M. Chiang and T. Zhang, "Fog and iot: An overview of research opportunities," IEEE Internet of Things Journal, vol. 3, pp. 854–864, 2016.

[143] F. Kraemer, A. E. Braten, N. Tamkittikhun, and D. Palma, "Fog computing in healthcare–a review and discussion," IEEE Access, vol. 5, pp. 9206–9222, 2017.

[144] M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. Ferrag, N. Choudhury, and V. Kumar, "Security and privacy in fog computing: Challenges," IEEE Access, vol. 5, pp. 19293–19304, 2017.

[145] P. Zhang, M. Zhou, and G. Fortino, "Security and trust issues in fog computing: A survey," Future Gener. Comput. Syst., vol. 88, pp. 16–27, 2018.

[146] S. Yi, Z. Qin, and Q. Li, "Security and privacy issues of fog computing: A survey," in Wireless Algorithms, Systems, and Applications: 10th International Conference, WASA 2015, Qufu, China, August 10-12, 2015, Proceedings 10, pp. 685–695, Springer, 2015.

[147] P. Kumar, N. Zaidi, and T. Choudhury, "Fog computing: Common security issues and proposed countermeasures," 2016 International Conference System Modeling & Advancement in Research Trends (SMART), pp. 311–315, 2016.

[148] E. Melnik, A. Klimenko, and D. Ivanov, "The model of device community forming problem for the geographically-distributed information and control systems using fog-computing concept," 2017.

[149] T. Dang and D. Hoang, "A data protection model for fog computing," 2017 Second International Conference on Fog and Mobile Edge Computing (FMEC), pp. 32–38, 2017.

[150] I. Stojmenovic, "Fog computing: A cloud to the ground support for smart things and machine-to-machine networks," 2014 Australasian Telecommunication Networks and Applications Conference (ATNAC), pp. 117–122, 2014.

[151]

[152] D. Lan, A. Taherkordi, F. Eliassen, and G. Horn, "A survey on fog programming: Concepts, state-of-the-art, and research challenges," pp. 1–6, 2019.

[153] S. Yi, Z. Hao, Z. Qin, and Q. A. Li, "Fog computing: Platform and applications," 2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb), pp. 73–78, 2015.

[154] I. Fatima, M. Ilahi, S. Javaid, R. Bukhsh, and N. Javaid, "Efficient resource allocation for consumers' power requests in cloud-fog-based system," International Journal of Web and Grid Services, 2019.

[155] D. E. al., "Fog computing resource optimization: A review on current scenarios and resource management," Baghdad Science Journal, 2019.

[156] K. Gai, X. Qin, and L. Zhu, "An energy-aware high performance task allocation strategy in heterogeneous fog computing environments," IEEE Transactions on Computers, vol. 70, pp. 626–639, 2021.

[157] K. Cao, Y. Liu, G. Meng, and Q. Sun, "An overview on edge computing research," IEEE access, vol. 8, pp. 85714–85728, 2020.

[158] H. Arasteh, V. Hosseinnezhad, V. Loia, A. Tommasetti, O. Troisi, M. Shafie-khah, and P. Siano, "Iot-based smart cities: A survey," in 2016 IEEE 16th international conference on environment and electrical engineering (EEEIC), pp. 1–6, IEEE, 2016.

[159] A. S. Syed, D. Sierra-Sosa, A. Kumar, and A. Elmaghraby, "Iot in smart cities: A survey of technologies, practices and challenges," Smart Cities, vol. 4, no. 2, pp. 429–475, 2021.

[160] L. R. Suzuki, "Smart cities iot: Enablers and technology road map," Smart City Networks: Through the Internet of Things, pp. 167–190, 2017.

[161] X. Xu, Q. Huang, X. Yin, M. Abbasi, M. Khosravi, and L. Qi, "Intelligent offloading for collaborative smart city services in edge computing," IEEE Internet of Things Journal, vol. 7, pp. 7919–7927, 2020.

[162] F. Li, M. Vögler, S. Sehic, S. Qanbari, S. Nastic, H. L. Truong, and S. Dustdar, "Web-scale service delivery for smart cities," IEEE Internet Computing, vol. 17, pp. 78–83, 2013.

[163] P. P. T and S. K. L, "Smart city services - challenges and approach," 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), pp. 553–558, 2019.

[164] G. Piro, I. Cianci, L. Grieco, G. Boggia, and P. Camarda, "Information centric services in smart cities," J. Syst. Softw., vol. 88, pp. 169–188, 2014.

[165] P. Sadhukhan, "An iot based framework for smart city services," 2018 International Conference on Communication, Computing and Internet of Things (IC3IoT), pp. 376–379, 2018.

[166] G. D'aniello, M. Gaeta, F. Orciuoli, G. Sansonetti, and F. Sorgente, "Knowledge-based smart city service system," Electronics, vol. 9, pp. 1–22, 2020.

[167] S. R. Laha, B. K. Pattanayak, and S. Pattnaik, "Advancement of environmental monitoring system using iot and sensor: A comprehensive analysis," AIMS Environmental Science, vol. 9, no. 6, pp. 771–800, 2022.

[168] A. Rani, "A proposal for architectural framework using internet of things with fog computing for an air quality monitoring system," Journal of Informatics Electrical and Electronics Engineering (JIEEE), 2021.

[169] S. I. Conea and G. Crişan, "Green air quality monitoring system based on arduino," 2022 14th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), pp. 1–4, 2022.

[170] G. Marques, N. Miranda, A. K. Bhoi, B. Garcia-Zapirain, S. Hamrioui, and I. D. L. T. Díez, "Internet of things and enhanced living environments: Measuring and mapping air quality using cyber-physical systems and mobile computing technologies," Sensors (Basel, Switzerland), vol. 20, 2020.

[171] A. S. Rao, S. Marshall, J. Gubbi, M. Palaniswami, R. Sinnott, and V. Pettigrovet, "Design of low-cost autonomous water quality monitoring system," 2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 14–19, 2013.

[172] P. Meghwani, "Real time water quality monitoring and control system," International Journal for Research in Applied Science and Engineering Technology, pp. 1–3, 2017.

[173] P. Whitfield, "Goals and data collection designs for water quality monitoring," Journal of The American Water Resources Association, vol. 24, pp. 775–780, 1988.

[174] J. Mabrouki, M. Azrour, D. Dhiba, Y. Farhaoui, and S. Hajjaji, "Iot-based data logger for weather monitoring using arduino-based wireless sensor networks with remote graphical application and alerts," Big Data Min. Anal., vol. 4, pp. 25–32, 2021.

[175] B. S, H. V. U. S, and R. B, "Solar powered efficient weather forecasting using iot technology," 2022 1st International Conference on Computational Science and Technology (ICCST), pp. 682–685, 2022.

[176] L. Vos, A. Droste, M. Zander, A. Overeem, H. Leijnse, B. Heusinkveld, G. Steeneveld, and R. Uijlenhoet, "Hydrometeorological monitoring using opportunistic sensing networks in the amsterdam metropolitan area," Bulletin of the American Meteorological Society, 2020.

[177] M. M. H. Anik, M. Haque, F. R. Sajid, and M. M. Khan, "Design of iot based weather monitoring system," 2022 6th International Conference on Computing Methodologies and Communication (ICCMC), pp. 1–7, 2022.

[178] C. Wang, G. Chen, R. Dong, and H. Wang, "Traffic noise monitoring and simulation research in xiamen city based on the environmental internet of things," International Journal of Sustainable Development & World Ecology, vol. 20, pp. 248 – 253, 2013.

[179] S. K. Shah, Z. Tariq, and Y. Lee, "Iot based urban noise monitoring in deep learning using historical reports," 2019 IEEE International Conference on Big Data (Big Data), pp. 4179–4184, 2019.

[180] M. B, "An iot based air and sound pollution monitoring system," International Journal for Research in Applied Science and Engineering Technology, 2022.

[181] A. H. Kazmi, E. Tragos, and M. Serrano, "Underpinning iot for road traffic noise management in smart cities," 2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp. 765–769, 2018.

[182] J. Sun, A. M. Abdulghani, M. Imran, and Q. Abbasi, "Iot enabled smart fertilization and irrigation aid for agricultural purposes," Proceedings of the 2020 International Conference on Computing, Networks and Internet of Things, 2020.

[183] S. Sarangi, S. B. Choudhury, P. Jain, P. V. Bhatt, S. Ramanath, R. Sharma, and P. Srinivasu, "Development and deployment of a scalable iot framework for digital farming applications," 2018 IEEE Global Humanitarian Technology Conference (GHTC), pp. 1–2, 2018.

[184] C. Bepery, M. S. S. Sozol, M. M. Rahman, M. Alam, and M. N. Rahman, "Framework for internet of things in remote soil monitoring," 2020 23rd International Conference on Computer and Information Technology (ICCIT), pp. 1–6, 2020.

[185] X. Liu, T. Yang, and B. Yan, "Internet of things for wildlife monitoring," 2015 IEEE/CIC International Conference on Communications in China - Workshops (CIC/ICCC), pp. 62–66, 2015.

[186] E. Ayele, N. Meratnia, and P. Havinga, "Towards a new opportunistic iot network architecture for wildlife monitoring system," 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), pp. 1–5, 2018.

[187] M. Khan, D. G. Barron, R. Patil, M. Nannemann, and M. Courson, "Internet of things based remote sensing for ornithological monitoring," 2020 IEEE Green Technologies Conference(GreenTech), pp. 71–73, 2020.

[188] M. Ojo, D. Adami, and S. Giordano, "Experimental evaluation of a lora wildlife monitoring network in a forest vegetation area," Future Internet, vol. 13, p. 115, 2021.

[189] P. Ghasemi and N. Karimian, "A qualitative study of various aspects of the application of iot in disaster management," 2020 6th International Conference on Web Research (ICWR), pp. 77–83, 2020.

[190] K. Sharma, D. Anand, M. Sabharwal, P. Tiwari, O. Cheikhrouhou, and T. Frikha, "A disaster management framework using internet of things-based interconnected devices," Mathematical Problems in Engineering, vol. 2021, pp. 1–21, 2021.

[191] K. K. Yadavalli and L. Gudino, "An autonomous, scalable and low-cost iot based framework for disaster management system," 2022 13th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP), pp. 619–624, 2022.

[192] G. Sharma and J. E. Lee, "Using iot in natural hazard management and future directions," Crisis and Emergency Management: Theory and Praxis, 2022.

[193] X. Li, N. Zhao, R. Jin, S. Liu, X. Sun, X. Wen, D. Wu, Y. Zhou, J. Guo, S. Chen, Z. Xu, M. Ma, T. Wang, Y. Qu, X. Wang, F. Wu, and Y. Zhou, "Internet of things to network smart devices for ecosystem monitoring.," Science bulletin, vol. 64 17, pp. 1234–1245, 2019.

[194] V. Matasov, L. B. Marchesini, A. Yaroslavtsev, G. Sala, O. S. Fareeva, I. Seregin, S. Castaldi, V. Vasenev, and R. Valentini, "Iot monitoring of urban tree ecosystem services: Possibilities and challenges," Forests, 2020.

[195] M. Mendonça, T. Jerónimo, M. Julião, J. Santos, N. Pombo, and B. M. C. Silva, "An iot-based healthcare ecosystem for home intelligent assistant services in smart homes," pp. 142–155, 2019.

[196] A. Salam, "Internet of things for sustainable human health," pp. 217–242, 2019.

[197] M. U. R. Patil and P. D. V. M. Patil, "Design and development of iot based remote sensing system for smart farming," International Journal for Research in Applied Science and Engineering Technology, 2022.

[198] S. Pallavi, J. Mallapur, and K. Y. Bendigeri, "Remote sensing and controlling of greenhouse agriculture parameters based on iot," 2017 International Conference on Big Data, IoT and Data Science (BID), pp. 44–48, 2017.

[199] X. Zhang, G. quan Zhang, X. Huang, and S. Poslad, "Granular content distribution for iot remote sensing data supporting privacy preservation," Remote. Sens., vol. 14, p. 5574, 2022.

[200] M. Wazid, A. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, "Design of secure user authenticated key management protocol for generic iot networks," IEEE Internet of Things Journal, vol. 5, pp. 269–282, 2018.

[201] A. Bramantoro, W. Suhaili, and N. Z. Siau, "Precision agriculture through weather forecasting," 2022 International Conference on Digital Transformation and Intelligence (ICDI), pp. 203–208, 2022.

[202] H. Bach and W. Mauser, "Sustainable agriculture and smart farming," vol. 15, pp. 261–269, 2018.

[203] R. Finger, S. Swinton, N. E. Benni, and A. Walter, "Precision farming at the nexus of agricultural production and the environment," Annual Review of Resource Economics, 2019.

[204] K. Monisha, D. Aishwarya, and K. Krupaleni, "Smart irrigation system using arduino uno," International Journal of Advance Research, Ideas and Innovations in Technology, vol. 4, pp. 678–679, 2018.

[205] J. Aleotti, M. Amoretti, A. Nicoli, and S. Caselli, "A smart precision-agriculture platform for linear irrigation systems," 2018 26th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), pp. 1–6, 2018.

[206] O. K. Ogidan, A. Onile, and O. Adegboro, "Smart irrigation system: A water management procedure," Agricultural Sciences, 2019.

[207] D. Masseroni, G. Arbat, and I. D. de Lima, "Editorial—managing and planning water resources for irrigation: Smart-irrigation systems for providing sustainable agriculture and maintaining ecosystem services," Water, vol. 12, p. 263, 2020.

[208] A. A. Chaudhry, R. Mumtaz, S. M. H. Zaidi, M. Tahir, and S. H. M. School, "Internet of things (iot) and machine learning (ml) enabled livestock monitoring," 2020 IEEE 17th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET), pp. 151–155, 2020.

[209] J. O. Isaac, "Iot - livestock monitoring and management system," vol. 5, 2021.

[210] I. Butun, M. Almgren, V. Gulisano, and M. Papatriantafilou, Industrial IoT. Springer, 2020.

[211] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial internet of things: Challenges, opportunities, and directions," IEEE transactions on industrial informatics, vol. 14, no. 11, pp. 4724–4734, 2018.

[212] J. Cheng, W. Chen, F. Tao, and C.-L. Lin, "Industrial iot in 5g environment towards smart manufacturing," Journal of Industrial Information Integration, vol. 10, pp. 10–19, 2018.

[213] Y. Meng and J. Li, "Data sharing mechanism of sensors and actuators of industrial iot based on blockchain-assisted identity-based cryptography," Sensors (Basel, Switzerland), vol. 21, 2021.

[214] D. Mourtzis, E. Vlachou, and N. Milas, "Industrial big data as a result of iot adoption in manufacturing," Procedia CIRP, vol. 55, pp. 290–295, 2016.

[215] G. George and S. Thampi, "A graph-based security framework for securing industrial iot networks from vulnerability exploitations," IEEE Access, vol. 6, pp. 43586–43601, 2018.

[216] M. H. Kashani, M. Madanipour, M. Nikravan, P. Asghari, and E. Mahdipour, "A systematic review of iot in healthcare: Applications, techniques, and trends," Journal of Network and Computer Applications, vol. 192, p. 103164, 2021.

[217] B. Pradhan, S. Bhattacharyya, and K. Pal, "Iot-based applications in healthcare devices," Journal of healthcare engineering, vol. 2021, pp. 1–18, 2021.

[218] I. de Morais Barroca Filho and G. S. de Aquino Junior, "Iot-based healthcare applications: a review," in Computational Science and Its Applications–ICCSA 2017: 17th International Conference, Trieste, Italy, July 3-6, 2017, Proceedings, Part VI 17, pp. 47–62, Springer, 2017.

[219] M. N. Bhuiyan, M. M. Rahman, M. M. Billah, and D. Saha, "Internet of things (iot): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities," IEEE Internet of Things Journal, vol. 8, no. 13, pp. 10474–10498, 2021.

[220] S. Xu, Y. Li, R. Deng, Y. Zhang, X. Luo, and X. Liu, "Lightweight and expressive fine-grained access control for healthcare internet-of-things," IEEE Transactions on Cloud Computing, vol. 10, pp. 474–490, 2022.

[221] M. S. Hossain and M. Ghulam, "Cloud-assisted industrial internet of things (iiot) - enabled framework for health monitoring," Comput. Networks, vol. 101, pp. 192–202, 2016.

[222] T. N. Gia, N. K. Thanigaivelan, A.-M. Rahmani, T. Westerlund, P. Liljeberg, and H. Tenhunen, "Customizing 6lowpan networks towards internet-of-things based ubiquitous healthcare systems," in 2014 NORCHIP, pp. 1–6, IEEE, 2014.

[223] T. Poongodi, R. Krishnamurthi, R. Indrakumari, P. Suresh, and B. Balusamy, "Wearable devices and iot," A handbook of Internet of Things in biomedical and cyber physical system, pp. 245–273, 2020.

[224] M. Haghi, K. Thurow, and R. Stoll, "Wearable devices in medical internet of things: scientific research and commercially available devices," Healthcare informatics research, vol. 23, no. 1, pp. 4–15, 2017.

[225] R. S. Bisht, S. Jain, and N. Tewari, "Study of wearable iot devices in 2021: Analysis & future prospects," in 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), pp. 577–581, IEEE, 2021.

[226] O. Arias, J. Wurm, K. Hoang, and Y. Jin, "Privacy and security in internet of things and wearable devices," IEEE transactions on multi-scale computing systems, vol. 1, no. 2, pp. 99–109, 2015.

[227] M. Baig, S. Afifi, H. Gholamhosseini, and F. Mirza, "A systematic review of wearable sensors and iot-based monitoring applications for older adults – a focus on ageing population and independent living," Journal of Medical Systems, vol. 43, pp. 1–11, 2019.

[228] S. Hiremath, G. Yang, and K. Mankodiya, "Wearable internet of things: Concept, architectural components and promises for person-centered healthcare," 2014 4th International Conference on Wireless Mobile Communication and Healthcare - Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH), pp. 304–307, 2014.

[229] A. S. Putra, H. L. H. S. Warnars, F. L. Gaol, B. Soewito, and E. Abdurachman, "A proposed surveillance model in an intelligent transportation system (its)," in 2018 Indonesian association for pattern recognition international conference (INAPR), pp. 156–160, IEEE, 2018.

[230] R. Tatum, M. Bays, J. Hyland, and B. Hartman, "Traffic monitoring using an adaptive sensor power scheduling algorithm," SN Applied Sciences, vol. 1, pp. 1–12, 2019.

[231] A. Marosi, R. Lovas, . Kisari, and E. Simonyi, "A novel iot platform for the era of connected cars," 2018 IEEE International Conference on Future IoT Technologies (Future IoT), pp. 1–11, 2018.

[232] A. Deshmukh, M. Murali, S. Jadhav, and A. Mandhana, "Generic, stand-alone iot solution for cloud connectivity in electric vehicles," in 2022 6th International Conference On Computing, Communication, Control And Automation (ICCUBEA, pp. 1–6, IEEE, 2022.

[233] C. Bıyık, Z. Allam, G. Pieri, D. Moroni, M. Fraifer, E. O'Connell, S. Olariu, and M. Khalid, "Smart parking systems: Reviewing the literature, architecture and ways forward," Smart Cities, vol. 4, pp. 623–642, 2021.

[234] P. Seymer, D. Wijesekera, and C. Kan, "Secure outdoor smart parking using dual mode bluetooth mesh networks," 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), pp. 1–7, 2019.

[235] J. Barriga, J. C. Sulca, J. León, A. Ulloa, D. Portero, J. A. García, and S. Yoo, "A smart parking solution architecture based on lorawan and kubernetes," Applied Sciences, vol. 10, p. 4674, 2020.

[236] A. Balasuriya, D. D, P. P. M, J. D. S, N. Swarnakantha, and U. Rajapaksha, "Secure smart parking solution using image processing and machine learning," 2022 IEEE 7th International conference for Convergence in Technology (I2CT), pp. 1–6, 2022.

[237] C. Kim and Y. Hong, "Traffic signal using smart agent system," American Journal of Applied Sciences, vol. 5, pp. 1487–1493, 2008.

[238] D. Desmira, M. A. Hamid, N. A. Bakar, M. Nurtanto, and S. Sunardi, "A smart traffic light using a microcontroller based on the fuzzy logic," IAES International Journal of Artificial Intelligence (IJ-AI), 2022.

[239] M. Al-qutwani and X. Wang, "Smart traffic lights over vehicular named data networking," Inf., vol. 10, p. 83, 2019.

[240] H. D. Kotha and V. M. Gupta, "Iot application: a survey," Int. J. Eng. Technol, vol. 7, no. 2.7, pp. 891–896, 2018.

[241] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," IEEE internet of things journal, vol. 4, no. 5, pp. 1125–1142, 2017.

[242] R. Gomathi, G. H. S. Krishna, E. Brumancia, and Y. M. Dhas, "A survey on iot technologies, evolution and architecture," in 2018 International Conference on Computer, Communication, and Signal Processing (ICCCSP), pp. 1–5, IEEE, 2018.

[243] E. Ahmed, I. Yaqoob, I. A. T. Hashem, I. Khan, A. I. A. Ahmed, M. Imran, and A. V. Vasilakos, "The role of big data analytics in internet of things," Computer Networks, vol. 129, pp. 459–471, 2017.

[244] J. Hopkins and P. Hawking, "Big data analytics and iot in logistics: a case study," The International Journal of Logistics Management, vol. 29, no. 2, pp. 575–591, 2018.

[245] W. Li, Y. Chai, F. Khan, S. R. U. Jan, S. Verma, V. G. Menon, f. Kavita, and X. Li, "A comprehensive survey on machine learning-based big data analytics for iot-enabled smart healthcare system," Mobile networks and applications, vol. 26, pp. 234–252, 2021.

[246] P. Gulia and A. Chahal, "Big data analytics for iot," International Journal of Advanced Research in Engineering and Technology (IJARET), vol. 11, no. 6, 2020.

[247] J. Pourqasem, "Cloud-based iot: integration cloud computing with internet of things," International Journal of Research, vol. 7, pp. 482–494, 2018.

[248] S. Mukhopadhyay, "Secure distributed storage for the internet of things," Women Securing the Future with TIPPSS for IoT, 2019.

[249] J. Kang, S. Yin, and W. Meng, "An intelligent storage management system based on cloud computing and internet of things," pp. 499–505, 2014.

[250] M. Satyanarayanan, "Edge computing," Computer, vol. 50, pp. 36–38, 2017.

[251] K. Ueta, X. Xue, Y. Nakamoto, and S. Murakami, "A distributed graph database for the data management of iot systems," 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 299–304, 2016.

[252] A. Cuzzocrea, "Big data compression paradigms for supporting efficient and scalable data-intensive iot frameworks," Proceedings of the Sixth International Conference on Emerging Databases: Technologies, Applications, and Theory, 2016.

[253] S. Routray, A. Javali, A. Sahoo, W. Semunigus, and M. Pappa, "Lossless compression techniques for low bandwidth io ts," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 177–181, 2020.

[254] J. Kim, J. Yun, S.-C. Choi, D. Seed, G. Lu, M. Bauer, A. Al-Hezmi, K. Campowsky, and J. Song, "Standard-based iot platforms interworking: implementation, experiences, and lessons learned," IEEE Communications Magazine, vol. 54, pp. 48–54, 2016.

[255] D. Bhattacharjee, V. Pudi, and A. Chattopadhyay, "Sha-3 implementation using reram based in-memory computing architecture," 2017 18th International Symposium on Quality Electronic Design (ISQED), pp. 325–330, 2017.

[256] Y. Qu, S. Yu, W. Zhou, S. Peng, G. Wang, and K. Xiao, "Privacy of things: Emerging challenges and opportunities in wireless internet of things," IEEE Wireless Communications, vol. 25, pp. 91–97, 2018.

[257] S. Wang, Z. Zhang, Z. Ye, X. Wang, X. Lin, and S. Chen, "Application of environmental internet of things on water quality management of urban scenic river," International Journal of Sustainable Development & World Ecology, vol. 20, no. 3, pp. 216–222, 2013.

[258] H. Eisenbeiss et al., "A mini unmanned aerial vehicle (uav): system overview and image acquisition," International Archives of Photogrammetry. Remote Sensing and Spatial Information Sciences, vol. 36, no. 5/W1, pp. 1–7, 2004.

[259] Y. Tan and S. K. Moon, "Inflatable wing design for micro uavs using indirect 3d printing," 2014 11th International Conference on Ubiquitous Robots and Ambient Intelligence (URAI), pp. 545–546, 2014.

[260] V. R. Kumar and N. Michael, "Opportunities and challenges with autonomous micro aerial vehicles," The International Journal of Robotics Research, vol. 31, pp. 1279 – 1291, 2012.

[261] A. A. Doshi, A. Postula, A. Fletcher, and S. P. N. Singh, "Development of micro-uav with integrated motion planning for open-cut mining surveillance," Microprocess. Microsystems, vol. 39, pp. 829–835, 2015.

[262] M. Ilarslan, M. K. Bayrakceken, and A. Arisoy, "Avionics system design of a mini vtol uav," IEEE Aerospace and Electronic Systems Magazine, vol. 26, pp. 35–40, 2011.

[263] M. Tyan, N. Nguyen, S. Kim, and J.-W. Lee, "Comprehensive preliminary sizing/resizing method for a fixed wing – vtol electric uav," Aerospace Science and Technology, vol. 71, pp. 30–41, 2017.

[264] M. Ilarslan, M. Bayrakceken, and A. Arisoy, "Avionics system design of a mini vtol uav," 29th Digital Avionics Systems Conference, pp. 6.A.3–1–6.A.3–7, 2010.

[265] J. Sun, B. Li, C. Wen, and C.-K. Chen, "Design and implementation of a real-time hardware-in-the-loop testing platform for a dual-rotor tail-sitter unmanned aerial vehicle," Mechatronics, 2018.

[266] W. Lu, D. Zhang, J. Zhang, T. Li, and T. Hu, "Design and implementation of a gasoline-electric hybrid propulsion system for a micro triple tilt-rotor vtol uav," 2017 6th Data Driven Control and Learning Systems (DDCLS), pp. 433–438, 2017.

[267] E. Servais, B. d'Andréa Novel, and H. Mounier, "Ground control of a hybrid tricopter," 2015 International Conference on Unmanned Aircraft Systems (ICUAS), pp. 945–950, 2015.

[268] D. Paley and D. Warshawsky, "Reduced-order dynamic modeling and stabilizing control of a micro-helicopter," 2009.

[269] E. S. Espinoza, O. García, I. Lugo, P. Ordaz, A. Malo, and R. Lozano, "Modeling and sliding mode control of a micro helicopter-airplane system," Journal of Intelligent & Robotic Systems, vol. 73, pp. 469–486, 2014.

[270] M. Saska, D. Heřt, T. Báča, V. Krátký, and T. Nascimento, "Formation control of unmanned micro aerial vehicles for straitened environments," Autonomous Robots, vol. 44, pp. 991 – 1008, 2020.

[271] Z. Haider, M. M. Zohaib, F. Haider, and E. Shaghaei, "Mathematical modeling and control system design of flapping wing unmanned air vehicle," 2021 4th International Conference on Robotics, Control and Automation Engineering (RCAE), pp. 224–228, 2021.

[272] A. Wissa, Y. Tummala, J. Hubbard, M. Frecker, and A. Brown, "Testing of novel compliant spines for passive wing morphing," pp. 733–742, 2011.

[273] C. Yun, I. Park, I. Hwang, and S. Kim, "Thrust control mechanism of vtol uav cyclocopter with cycloidal blades system," Journal of Intelligent Material Systems and Structures, vol. 16, pp. 937 – 943, 2005.

[274] M. Benedict, E. Shrestha, V. Hrishikeshavan, and I. Chopra, "Development of a micro twin-rotor cyclocopter capable of autonomous hover," Journal of Aircraft, vol. 51, pp. 672–676, 2014.

[275] E. Shrestha, M. Benedict, and I. Chopra, "Autonomous hover capability of cycloidal-rotor micro air vehicle," 2013.

[276] W. Green and P. Oh, "A fixed-wing aircraft for hovering in caves, tunnels, and buildings," 2006 American Control Conference, pp. 6 pp.–, 2006.

[277] M. Hassanalian, M. Radmanesh, and A. Sedaghat, "Increasing flight endurance of mavs using multiple quantum well solar cells," International Journal of Aeronautical and Space Sciences, vol. 15, pp. 212–217, 2014.

[278] M. Hossain, F. Hasan, A. F. M. T. Seraz, and S. Rajib, "Development of design and manufacturing of a fixed wing radio controlled micro air vehicle (mav)," vol. 3, 2011.

[279] M. Varga, M. Basiri, G. Heitz, and D. Floreano, "Distributed formation control of fixed wing micro aerial vehicles for area coverage," 2015 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), pp. 669–674, 2015.

[280] H. Jun, "Research of the latest development trends of fixed-wing micro aerial vehicles," Aero Weaponry, 2008.

[281] H. Su and M. Ryan, "Peak input torque minimization of a flapping wing mechanism for mavs," 2013.

[282] Y. hai Nan, M. Karásek, M. E. Lalami, and A. Preumont, "Experimental optimization of wing shape for a hummingbird-like flapping wing micro air vehicle," Bioinspiration & Biomimetics, vol. 12, 2017.

[283] D. Kumar, M. Shah, M. MohiteP, and S. Kamle, "Structural dynamic analysis of bioinspired carbon fibre/polyethylene mav wings," vol. 3, pp. 7–15, 2014.

[284] C. Chen, Y. Tang, H. Wang, and Y. Wang, "A review of fabrication options and power electronics for flapping-wing robotic insects," International Journal of Advanced Robotic Systems, vol. 10, 2013.

[285] J. Laliberté, K. L. Kraemer, J. W. Dawson, and D. Miyata, "Design and manufacturing of biologically inspired micro aerial vehicle wings using rapid prototyping," International Journal of Micro Air Vehicles, vol. 5, pp. 15 – 38, 2013.

[286] M. Hassanalian and A. Abdelkefi, "Methodologies for weight estimation of fixed and flapping wing micro air vehicles," Meccanica, vol. 52, pp. 2047–2068, 2017.

[287] M. Dorothy, A. Paranjape, P. Kuang, and S.-J. Chung, "Towards bio-inspired robotic aircraft: Control experiments on flapping and gliding flight," 2012.

[288] H. Liu and W. Shyy, "Micro air vehicle-motivated aerodynamics," 2010.

[289] J. Ratti, E. Jones, and G. Vachtsevanos, "Fixed frequency, variable amplitude (fifva) actuation systems for micro aerial vehicles," 2011 IEEE International Conference on Robotics and Automation, pp. 165–171, 2011.

[290] Z. Liu, M. Xu, and J. Moschetta, "A review on conceptual design of nano air vehicles," vol. 55, pp. 3257–3268, 2010.

[291] R. Citroni, A. Leggieri, D. Passi, F. D. Paolo, and A. Carlo, "Nano energy harvesting with plasmonic nano-antennas: A review of mid-ir rectenna and application," Applied and Environmental Microbiology, vol. 6, pp. 1–13, 2017.

[292] M. Naqvi, H. Shah, A. Ali, and F. Naeem, "Design and development of a small scale fixed wing aerial vehicle for over the hill missions in urban warfare," Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 14th - 18th January, 2014, pp. 271–278, 2014.

[293] J. Jo, Y. Kim, S. W. Park, and R. Myong, "A study of certification of lightning indirect effects on cable harness in personal air vehicles," Journal of The Korean Society for Aeronautical & Space Sciences, vol. 49, pp. 251–262, 2021.

[294] A. Hardman, L. Crispo, T. Sirola, J.-B. Ann, J. Lee, J. H. Song, and I. Kim, "Structural design optimization for cfrp in a personal aerial vehicle," AIAA AVIATION 2021 FORUM, 2021.

[295] D. Kim, Y. Lee, S. Oh, Y. Park, J. Choi, and D. Park, "Aerodynamic analysis and static stability analysis of manned/unmanned distributed propulsion aircrafts using actuator methods," Journal of Wind Engineering and Industrial Aerodynamics, 2021.

[296] A. Hekmatmanesh, P. Nardelli, and H. Handroos, "Review of the state-of-the-art on bio-signal-based brain-controlled vehicles," arXiv: Signal Processing, 2020.

[297] B. Ben-Moshe, Y. Landau, R. Marbel, and A. Mishiner, "Bio-inspired micro drones," 2018 IEEE International Conference on the Science of Electrical Engineering in Israel (ICSEE), pp. 1–5, 2018.

[298] Z. Wang, A. S. Griffin, A. Lucas, and K. Wong, "Psychological warfare in vineyard: Using drones and bird psychology to control bird damage to wine grapes," Crop Protection, 2019.

[299] J.-S. Choi and H. Ho-won, "A study on the development status and economic impacts of drone taxis," Journal of the Korean Society for Aviation and Aeronautics, 2020.

[300] R. J. Wood, "Liftoff of a 60mg flapping-wing mav," in 2007 IEEE/RSJ International Conference on Intelligent Robots and Systems, pp. 1889–1894, IEEE, 2007.

[301] A. S. Saeed, A. Younes, C. Cai, and G. Cai, "A survey of hybrid unmanned aerial vehicles," Progress in Aerospace Sciences, vol. 98, pp. 91–105, 2018.

[302] P. T. Dewi, G. S. Hadi, M. R. Kusnaedi, A. Budiyarto, and A. Budiyono, "Design of separate lift and thrust hybrid uav," vol. 2, pp. 45–51, 2016.

[303] R. M. Rodríguez, F. Alarcón, D. S. Rubio, and A. Ollero, "Autonomous management of an uav airfield," in proceedings of the 3rd international conference on application and theory of automation in command and control systems, Naples, Italy, pp. 28–30, 2013.

[304] B. Siddappaji, P. K. Hajoary, and K. Akhilesh, "Uavs/drones-based iot services," Smart Technologies, 2019.

[305] N. Elmeseiry, N. Alshaer, and T. Ismail, "A detailed survey and future directions of unmanned aerial vehicles (uavs) with potential applications," Aerospace, 2021.

[306] E. Mitka and S. G. Mouroutsos, "Classification of drones," Am. J. Eng. Res, vol. 6, no. 7, pp. 36–41, 2017.

[307] M. G. Pensieri, M. Garau, and P. Barone, "Drones as an integral part of remote sensing technologies to help missing people," Drones, 2020.

[308] S. Pikalov, E. Azaria, S. Sonnenberg, B. Ben-Moshe, and A. Azaria, "Vision-less sensing for autonomous micro-drones," Sensors (Basel, Switzerland), vol. 21, 2021.

[309] B. Dan, A. Elzawawy, and H. Rahemi, "Innovative drone design for the ahs micro air vehicle competition," 2017.

[310] X. Sun and W. Zhang, "Implementation of target tracking system based on small drone," 2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), vol. 1, pp. 1863–1866, 2019.

[311] K. O. Said, M. Onifade, J. Githiria, J. Abdulsalam, M. Bodunrin, B. Genc, O. T. Johnson, and J. M. Akande, "On the application of drones: a progress report in mining operations," International Journal of Mining, Reclamation and Environment, vol. 35, pp. 235 – 267, 2020.

[312] J. Green, "Mine rescue robots requirements outcomes from an industry workshop," in 2013 6th Robotics and Mechatronics Conference (RobMech), pp. 111–116, IEEE, 2013.

[313] T. Xiang, G. Xia, and L. Zhang, "Mini-uav-based remote sensing: Techniques," Applications and Prospectives. arXiv, vol. 1812, 2018.

[314] R. Schroedter, "Using photogrammetry to transform mining," 2019.

[315] S. Raval, "Smart sensing for mineral exploration through to mine closure," International Journal of Georesources and Environment, 2018.

[316] P. Gruchlik and A. Kowalski, "Application of new measurement technology for deformation study of structures in mining areas," vol. 55, p. 00008, 2018.

[317] V. Carabassa, P. Montero, M. Crespo, J.-C. Padró, X. Pons, J. Balagué, L. Brotóns, and J. Alcañiz, "Unmanned aerial system protocol for quarry restoration and mineral extraction monitoring.," Journal of environmental management, vol. 270, p. 110717, 2020.

[318] J. Robinson and P. Kinghan, "Using drone based hyperspectral analysis to characterize the geochemistry of soil and water," vol. 6, 2018.

[319] A. Mirzaeinia, J. Shahmoradi, P. Roghanchi, and M. Hassanalian, "Autonomous routing and power management of drones in gps-denied environments through dijkstra algorithm," in AIAA Propulsion and Energy 2019 Forum, p. 4462, 2019.

[320] L. Dunnington and M. Nakagawa, "Fast and safe gas detection from underground coal fire by drone fly over," Environmental Pollution, vol. 229, pp. 139–145, 2017.

[321] N. Buzalo, D. Kundryutskov, and R. Ponomarev, "Use of unmanned aerial vehicles in surveying buildings and structures," Construction and Architecture, 2022.

[322] D. Tezza and M. Andujar, "The state-of-the-art of human–drone interaction: A survey," IEEE Access, vol. 7, pp. 167438–167454, 2019.

[323] S. Ahirwar, R. Swarnkar, S. Bhukya, and G. Namwade, "Application of drone in agriculture," International Journal of Current Microbiology and Applied Sciences, vol. 8, no. 01, pp. 2500–2505, 2019.

[324] F. Veroustraete, "The rise of the drones in agriculture," EC agriculture, vol. 2, no. 2, pp. 325–327, 2015.

[325] A. Rejeb, A. Abdollahi, K. Rejeb, and H. Treiblmaier, "Drones in agriculture: A review and bibliometric analysis," Computers and electronics in agriculture, vol. 198, p. 107017, 2022.

[326] F. Xin, J. Zhao, Y. Zhou, G. Wang, X. Han, W. Fu, J. Deng, and Y. Lan, "Effects of dosage and spraying volume on cotton defoliants efficacy: A case study based on application of unmanned aerial vehicles," Agronomy, 2018.

[327] F. Sun, X. Wang, and R. Zhang, "Task scheduling system for uav operations in agricultural plant protection environment," Journal of Ambient Intelligence and Humanized Computing, pp. 1–15, 2020.

[328] P. Hu, R. Zhang, J. Yang, and L. Chen, "Development status and key technologies of plant protection uavs in china: A review," Drones, 2022.

[329] S. N. A. M. Ghazali, H. A. Anuar, S. N. A. S. Zakaria, and Z. Yusoff, "Determining position of target subjects in maritime search and rescue (msar) operations using rotary wing unmanned aerial vehicles (uavs)," in 2016 international conference on information and communication technology (ICICTM), pp. 1–4, IEEE, 2016.

[330] C. Rees, "Maritime surveillance uav adds new sar capability," 2021. Accessed: 21/12/2023.

[331] L. Gonçalves and B. Damas, "Automatic detection of rescue targets in maritime search and rescue missions using uavs," in 2022 International Conference on Unmanned Aircraft Systems (ICUAS), pp. 1638–1643, IEEE, 2022.

[332] M. Erdelj, E. Natalizio, K. R. Chowdhury, and I. F. Akyildiz, "Help from the sky: Leveraging uavs for disaster management," IEEE Pervasive Computing, vol. 16, no. 1, pp. 24–32, 2017.

[333] M. Narang, W. Liu, J. Gutierrez, and L. Chiaraviglio, "A cyber physical buses-and-drones mobile edge infrastructure for large scale disaster emergency communications," in 2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW), pp. 53–60, IEEE, 2017.

[334] D. Câmara, "Cavalry to the rescue: Drones fleet to help rescuers operations over disasters scenarios," in 2014 IEEE Conference on Antenna Measurements & Applications (CAMA), pp. 1–4, IEEE, 2014.

[335] H. Moon, C. Kim, and W. Lee, "A uav based 3-d positioning framework for detecting locations of buried persons in collapsed disaster area.," International Archives of the Photogrammetry, Remote Sensing & Spatial Information Sciences, vol. 41, 2016.

[336] J. Lee, K. Kim, H. Kim, and H. Kim, "Devising geographic diffusion for drone networks," in 2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN), pp. 76–78, IEEE, 2016.

[337] M. Zhang and X. Li, "Drone-enabled internet-of-things relay for environmental monitoring in remote areas without public networks," IEEE Internet of Things Journal, vol. 7, pp. 7648–7662, 2020.

[338] S. Manfreda, M. F. McCabe, P. E. Miller, R. Lucas, V. Pajuelo Madrigal, G. Mallinis, E. Ben Dor, D. Helman, L. Estes, G. Ciraolo, et al., "On the use of unmanned aerial systems for environmental monitoring," Remote sensing, vol. 10, no. 4, p. 641, 2018.

[339] Z. Zhang and L. Zhu, "A review on unmanned aerial vehicle remote sensing: Platforms, sensors, data processing methods, and applications," Drones, vol. 7, no. 6, p. 398, 2023.

[340] J. G. A. Barbedo, "A review on the use of unmanned aerial vehicles and imaging sensors for monitoring and assessing plant stresses," Drones, vol. 3, no. 2, p. 40, 2019.

[341] D. Olson and J. Anderson, "Review on unmanned aerial vehicles, remote sensors, imagery processing, and their applications in agriculture," Agronomy Journal, vol. 113, no. 2, pp. 971–992, 2021.

[342] R. A. Ramadan, A.-H. Emara, M. Al-Sarem, and M. Elhamahmy, "Internet of drones intrusion detection using deep learning," Electronics, vol. 10, no. 21, p. 2633, 2021.

[343] B. Taha and A. Shoufan, "Machine learning-based drone detection and classification: State-of-the-art in research," IEEE access, vol. 7, pp. 138669–138682, 2019.

[344] J. N. Yasin, S. A. Mohamed, M.-H. Haghbayan, J. Heikkonen, H. Tenhunen, and J. Plosila, "Navigation of autonomous swarm of drones using translational coordinates," in International Conference on Practical Applications of Agents and Multi-Agent Systems, pp. 353–362, Springer, 2020.

[345] W. Power, M. Pavlovski, D. Saranovic, I. Stojkovic, and Z. Obradovic, "Autonomous navigation for drone swarms in gps-denied environments using structured learning," in Artificial Intelligence Applications and Innovations: 16th IFIP WG 12.5 International Conference, AIAI 2020, Neos Marmaras, Greece, June 5–7, 2020, Proceedings, Part II 16, pp. 219–231, Springer, 2020.

[346] A. Majd, A. Ashraf, E. Troubitsyna, and M. Daneshtalab, "Integrating learning, optimization, and prediction for efficient navigation of swarms of drones," in 2018 26th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP), pp. 101–108, IEEE, 2018.

[347] A. Majd, M. Loni, G. Sahebi, and M. Daneshtalab, "Improving motion safety and efficiency of intelligent autonomous swarm of drones," Drones, vol. 4, no. 3, p. 48, 2020.

[348] S. Sarkar, Intelligent Energy-Efficient Drones: Path Planning, Real-Time Monitoring and Decision-Making. University of Louisiana at Lafayette, 2021.

[349] S. Herwitz, L. Johnson, S. Dunagan, R. Higgins, D. Sullivan, J. Zheng, B. Lobitz, J. Leung, B. Gallmeyer, M. Aoyagi, et al., "Imaging from an unmanned aerial vehicle: agricultural surveillance and decision support," Computers and electronics in agriculture, vol. 44, no. 1, pp. 49–61, 2004.

[350] S. Zermani, C. Dezan, and R. Euler, "Embedded decision making for uav missions," in 2017 6th Mediterranean Conference on Embedded Computing (MECO), pp. 1–4, IEEE, 2017.

[351] J. Jiménez López and M. Mulero-Pázmány, "Drones for conservation in protected areas: Present and future," Drones, vol. 3, no. 1, p. 10, 2019.

[352] S. A. Wich and L. P. Koh, Conservation drones: mapping and monitoring biodiversity. Oxford University Press, 2018.

[353] L. P. Koh and S. A. Wich, "Dawn of drone ecology: low-cost autonomous aerial vehicles for conservation," Tropical conservation science, vol. 5, no. 2, pp. 121–132, 2012.

[354] Anonymous, "Amazon teases new details of planned prime air drone delivery service," 2015.

[355] Anonymous, "Two delivery drones built by google soon to be tested in the u.s.," Unknown.

[356] M. Heutger, "Unmanned aerial vehicle in logistics: A dhl perspective on implications and use cases for the logistics industry," tech. rep., DHL Customer Solutions & Innovation, Troisdorf, Germany, 2014.

[357] M. Ulmer and B. W. Thomas, "Same-day delivery with heterogeneous fleets of drones and vehicles," Networks, vol. 72, pp. 475 – 505, 2018.

[358] D. Das, R. Sewani, J. Wang, and M. Tiwari, "Synchronized truck and drone routing in package delivery logistics," IEEE Transactions on Intelligent Transportation Systems, vol. 22, pp. 5772–5782, 2021.

[359] P. Kornatowski, A. Bhaskaran, G. Heitz, S. Mintchev, and D. Floreano, "Last-centimeter personal drone delivery: Field deployment and user interaction," IEEE Robotics and Automation Letters, vol. 3, pp. 3813–3820, 2018.

[360] H. Huang, A. Savkin, and C. Huang, "Drone routing in a time-dependent network: Toward low-cost and large-range parcel delivery," IEEE Transactions on Industrial Informatics, vol. 17, pp. 1526–1534, 2021.

[361] M. Liu, X. Liu, M. Zhu, and F. Zheng, "Stochastic drone fleet deployment and planning problem considering multiple-type delivery service," Sustainability, 2019.

[362] M. Hassanalian, D. Rice, and A. Abdelkefi, "Evolution of space drones for planetary exploration: A review," Progress in Aerospace Sciences, vol. 97, pp. 61–105, 2018.

[363] Anonymous, "Nasa helicopter drones to explore mars," 2015.

[364] Anonymous, "Mars airplane - platform," Unknown. Accessed on:25/12/2023.

[365] B. Peeters, J. Mulder, S. Kraft, J. Leijtens, T. Zegers, D. Lentink, and N. La, "Flapping winged aerobot for autonomous flight in mars atmosphere," tech. rep., Delft University of Technology, Netherlands, Year.

[366] P. Menges, "Artificial neural membrane flapping wing niac phase i study, final report," tech. rep., Ph.D. Principal Investigator Aerospace Research Systems, USA, May 2006.

[367] W. Koski, T. Allen, D. Ireland, G. Buck, P. Smith, A. Macrander, M. Halick, C. Rushing, D. Sliwa, and T. McDonald, "Evaluation of an unmanned airborne system for monitoring marine mammals," Aquatic Mammals, vol. 35, no. 3, p. 347, 2009.

[368] "The ethical concerns in drone technology." Accessed on:25/12/2023.

[369] "How drones raised privacy concerns across cyberspace." Accessed on:25/12/2023.

[370] D. Sella-Villa, "Drones and data: A limited impact on privacy," U. Rich. L. Rev., vol. 55, p. 991, 2020.

[371] "Drone surveillance in the u.s.: Privacy or property rights issue?." Accessed on:25/12/2023.

[372] "Privacy and security issues with drones." Accessed on:25/12/2023.

[373] V. Alarcón, M. García, F. Alarcón, A. Viguria, Ángel Martínez, D. Janisch, J. J. Acevedo, I. Maza, and A. Ollero, "Procedures for the integration of drones into the airspace based on u-space services," Aerospace, 2020.

[374] B. Schäffer, R. Pieren, K. Heutschi, J. Wunderli, and S. Becker, "Drone noise emission characteristics and noise effects on humans—a systematic review," International Journal of Environmental Research and Public Health, vol. 18, 2021.

[375] J. Kim, Y. Choi, S. Jeon, J. Kang, and H. Cha, "Optrone: Maximizing performance and energy resources of drone batteries," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 39, pp. 3931–3943, 2020.

[376] "Know your drone - drone rules." The Civil Aviation Safety Authority (CASA) outlines drone rules in this source.

[377] "Drone regulations in south africa." Starlite Aviation offers information on drone regulations specific to South Africa.

[378] "Drone regulations: What you need to know." This source from PCMag provides information on drone regulations.

[379] S. D. Muruganathan, X. Lin, H.-L. Maattanen, J. Sedin, Z. Zou, W. A. Hapsari, and S. Yasukawa, "An overview of 3gpp release-15 study on enhanced lte support for connected drones," arXiv preprint arXiv:1805.00826, 2018.

[380] U. Challita, A. Ferdowsi, M. Chen, and W. Saad, "Artificial intelligence for wireless connectivity and security of cellular-connected uavs," arXiv preprint arXiv:1804.05348, 2018.

[381] A. Bürkle, F. Segor, and M. Kollmann, "Towards autonomous micro uav swarms," Journal of intelligent & robotic systems, vol. 61, no. 1, pp. 339–353, 2011.

[382] T.-Y. Chi, Y. Ming, S.-Y. Kuo, C.-C. Liao, et al., "Civil uav path planning algorithm for considering connection with cellular data network," in 2012 IEEE 12th International Conference on Computer and Information Technology, pp. 327–331, IEEE, 2012.

[383] A. L. Christensen, S. M. Oliveira, O. Postolache, M. J. De Oliveira, S. Sargento, P. Santana, L. Nunes, F. Velez, P. Sebastião, V. Costa, et al., "Design of communication and control for swarms of aquatic surface drones," in ICAART 2015-7th International Conference on Agents and Artificial Intelligence, Proceedings, pp. 548–555, 2015.

[384] M. A. Rahman, "Enabling drone communications with wimax technology," in IISA 2014, The 5th International Conference on Information, Intelligence, Systems and Applications, pp. 323–328, IEEE, 2014.

[385] A. Koubâa, B. Qureshi, M.-F. Sriti, Y. Javed, and E. Tovar, "A service-oriented cloud-based management system for the internet-of-drones," in 2017 IEEE International Conference on Autonomous Robot Systems and Competitions (ICARSC), pp. 329–335, IEEE, 2017.

[386] T. Long, M. Ozger, O. Cetinkaya, and O. B. Akan, "Energy neutral internet of drones," IEEE Communications Magazine, vol. 56, no. 1, pp. 22–28, 2018.

[387] J. H. Cheon, K. Han, S.-M. Hong, H. J. Kim, J. Kim, S. Kim, H. Seo, H. Shim, and Y. Song, "Toward a secure drone system: Flying with real-time homomorphic authenticated encryption," IEEE access, vol. 6, pp. 24325–24339, 2018.

[388] A. Singandhupe, H. M. La, and D. Feil-Seifer, "Reliable security algorithm for drones using individual characteristics from an eeg signal," IEEE Access, vol. 6, pp. 22976–22986, 2018.

[389] Q.-A. Kester, L. Nana, and A. C. Pascu, "A novel cryptographic encryption technique of video images using quantum cryptography for satellite communications," in 2013 International Conference on Adaptive Science and Technology, pp. 1–6, IEEE, 2013.

[390] J. A. Steinmann, R. F. Babiceanu, and R. Seker, "Uas security: Encryption key negotiation for partitioned data," in 2016 Integrated Communications Navigation and Surveillance (ICNS), pp. 1E4–1, IEEE, 2016.

[391] M. Coppola, K. N. McGuire, K. Y. Scheper, and G. C. de Croon, "On-board communication-based relative localization for collision avoidance in micro air vehicle teams," Autonomous robots, vol. 42, no. 8, pp. 1787–1805, 2018.

[392] N. Ramdhan, M. Sliti, and N. Boudriga, "Codeword-based data collection protocol for optical unmanned aerial vehicle networks," in 2016 HONET-ICT, pp. 35–39, IEEE, 2016.

[393] O. Shrit, S. Martin, K. Alagha, and G. Pujolle, "A new approach to realize drone swarm using ad-hoc network," in 2017 16th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net), pp. 1–5, IEEE, 2017.

[394] J. Park, Y. Kim, and J. Seok, "Prediction of information propagation in a drone network by using machine learning," in 2016 International Conference on Information and Communication Technology Convergence (ICTC), pp. 147–149, IEEE, 2016.

[395] T. Wu, P. Yang, Y. Yan, X. Rao, P. Li, and W. Xu, "Orsca: Optimal route selection and communication association for drones in wsns," in 2017 Fifth International Conference on Advanced Cloud and Big Data (CBD), pp. 420–424, IEEE, 2017.

[396] W.-S. Jung, J. Yim, Y.-B. Ko, and S. Singh, "Acods: adaptive computation offloading for drone surveillance system," in 2017 16th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net), pp. 1–6, IEEE, 2017.

[397] D. Zorbas, T. Razafindralambo, F. Guerriero, et al., "Energy efficient mobile target tracking using flying drones," Procedia Computer Science, vol. 19, pp. 80–87, 2013.

[398] D. Aleksandrov and I. Penkov, "Energy consumption of mini uav helicopters with different number of rotors," in 11th International Symposium" Topical Problems in the Field of Electrical and Power Engineering, pp. 259–262, 2012.

[399] F. Wu, D. Yang, L. Xiao, and L. Cuthbert, "Energy consumption and completion time tradeoff in rotary-wing uav enabled wpcn," IEEE Access, vol. 7, pp. 79617–79635, 2019.

[400] Y. Zeng and R. Zhang, "Energy-efficient uav communication with trajectory optimization," IEEE Transactions on Wireless Communications, vol. 16, no. 6, pp. 3747–3760, 2017.

[401] D. He, S. Chan, and M. Guizani, "Drone-assisted public safety networks: The security aspect," IEEE Communications Magazine, vol. 55, no. 8, pp. 218–223, 2017.

[402] B. Siddappaji and K. Akhilesh, "Role of cyber security in drone technology," in Smart Technologies, pp. 169–178, Springer, 2020.

[403] M. Conoscenti, A. Vetro, and J. C. De Martin, "Peer to peer for privacy and decentralization in the internet of things," in 2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C), pp. 288–290, IEEE, 2017.

[404] D. He, Y. Qiao, S. Chan, and N. Guizani, "Flight security and safety of drones in airborne fog computing systems," IEEE Communications Magazine, vol. 56, no. 5, pp. 66–71, 2018.

[405] X. Hou, Z. Ren, J. Wang, S. Zheng, W. Cheng, and H. Zhang, "Distributed fog computing for latency and reliability guaranteed swarm of drones," IEEE Access, vol. 8, pp. 7117–7130, 2020.

[406] K. Dantu, B. Kate, J. Waterman, P. Bailis, and M. Welsh, "Programming micro-aerial vehicle swarms with karma," in Proceedings of the 9th ACM Conference on Embedded Networked Sensor Systems, pp. 121–134, 2011.

[407] K. Yoshikawa, S. Yamashita, K. Yamamoto, T. Nishio, and M. Morikura, "Resource allocation for 3d drone networks sharing spectrum bands," in 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall), pp. 1–5, IEEE, 2017.

[408] I. Bekmezci, O. K. Sahingoz, and Ş. Temel, "Flying ad-hoc networks (fanets): A survey," Ad Hoc Networks, vol. 11, no. 3, pp. 1254–1270, 2013.

[409] S. A. R. Naqvi, S. A. Hassan, H. Pervaiz, and Q. Ni, "Drone-aided communication as a key enabler for 5g and resilient public safety networks," IEEE Communications Magazine, vol. 56, no. 1, pp. 36–42, 2018.

[410] N. Uchida, M. Kimura, T. Ishida, Y. Shibata, and N. Shiratori, "Evaluation of wireless network communication by autonomous flight wireless nodes for resilient networks," in 2014 17th International Conference on Network-Based Information Systems, pp. 180–185, IEEE, 2014.

[411] O. S. Oubbati, A. Lakas, F. Zhou, M. Güneş, N. Lagraa, and M. B. Yagoubi, "Intelligent uav-assisted routing protocol for urban vanets," Computer communications, vol. 107, pp. 93–111, 2017.

[412] X. Wang, L. Fu, Y. Zhang, X. Gan, and X. Wang, "Vdnet: an infrastructure-less uav-assisted sparse vanet system with vehicle location prediction," Wireless Communications and Mobile Computing, vol. 16, no. 17, pp. 2991–3003, 2016.

[413] H. N. Saha, N. K. Das, S. K. Pal, S. Basu, S. Auddy, R. Dey, A. Nandy, D. Pal, N. Roy, D. Mitra, et al., "A cloud based autonomous multipurpose system with self-communicating bots and swarm of drones," in 2018 IEEE 8th annual computing and communication workshop and conference (CCWC), pp. 649–653, IEEE, 2018.

[414] M. Gowda, J. Manweiler, A. Dhekne, R. R. Choudhury, and J. D. Weisz, "Tracking drone orientation with multiple gps receivers," in Proceedings of the 22nd annual international conference on mobile computing and networking, pp. 280–293, 2016.

[415] T. T. Do and H. Ahn, "Visual-gps combined 'follow-me'tracking for selfie drones," Advanced Robotics, vol. 32, no. 19, pp. 1047–1060, 2018.

[416] P. A. Catherwood, M. Little, D. Finlay, and J. McLaughlin, "Recovery of incapacitated commercial delivery drones using lpwan technology," IEEE Intelligent Transportation Systems Magazine, vol. 12, no. 2, pp. 6–19, 2019.

[417] J. Noh, Y. Kwon, Y. Son, H. Shin, D. Kim, J. Choi, and Y. Kim, "Tractor beam: Safe-hijacking of consumer drones with adaptive gps spoofing," ACM Transactions on Privacy and Security (TOPS), vol. 22, no. 2, pp. 1–26, 2019.

[418] D. T. Tuan and H. Ahn, "Visual-gps combined drone follow-me selfie drone," in Proceedings of the Korea Information Processing Society Conference, pp. 134–137, Korea Information Processing Society, 2017.

[419] M. Gowda, J. Manweiler, A. Dhekne, R. R. Choudhury, and J. D. Weisz, "Integrating glonass with gps for drone orientation tracking," in Communication Systems and Networks: 9th International Conference, COMSNETS 2017, Bengaluru, India, January 4–8, 2017, Revised Selected Papers and Invited Papers 9, pp. 77–92, Springer, 2017.

[420] R. R. Choudhury and J. D. Weisz, "Integrating glonass with gps for drone orientation tracking," in Communication Systems and Networks: 9th International Conference, COMSNETS 2017, Bengaluru, India, January 4–8, 2017, Revised Selected Papers and Invited Papers, vol. 10340, p. 77, Springer, 2017.

[421] M. Angurala, M. Bala, S. S. Bamber, R. Kaur, and P. Singh, "An internet of things assisted drone based approach to reduce rapid spread of covid-19," Journal of Safety Science and Resilience, vol. 1, no. 1, pp. 31–35, 2020.

[422] P. M. Wyder, Y.-S. Chen, A. J. Lasrado, R. J. Pelles, R. Kwiatkowski, E. O. Comas, R. Kennedy, A. Mangla, Z. Huang, X. Hu, et al., "Autonomous drone hunter operating by deep learning and all-onboard computations in gps-denied environments," PloS one, vol. 14, no. 11, p. e0225092, 2019.

[423] M. P. Arthur, "Detecting signal spoofing and jamming attacks in uav networks using a lightweight ids," in 2019 international conference on computer, information and telecommunication systems (CITS), pp. 1–5, IEEE, 2019.

[424] Y. Qiao, Y. Zhang, and X. Du, "A vision-based gps-spoofing detection method for small uavs," in 2017 13th International Conference on Computational Intelligence and Security (CIS), pp. 312–316, IEEE, 2017.

[425] Y.-H. Ho, Y.-T. Huang, H.-H. Chu, and L.-J. Chen, "Adaptive sensing scheme using naive bayes classification for environment monitoring with drone," International Journal of Distributed Sensor Networks, vol. 14, no. 1, p. 1550147718756036, 2018.

[426] M. Pircher, J. Geipel, K. Kusnierek, and A. Korsaeth, "Development of a hybrid uav sensor platform suitable for farm-scale applications in precision agriculture," The International Archives of Photogrammetry, Remote Sensing and Spatial Information Sciences, vol. 42, p. 297, 2017.

[427] B. P. Lewis, A Visual Return-to-home System for GPS-denied Flight. Brigham Young University, 2016.

[428] K. Gozlan, Y. Reuveni, K. Cohen, B. Ben-Moshe, and E. Berliner, "Cost-effective platforms for near-space research and experiments," Space Flight, p. 197, 2018.

[429] A. Gasimova, T. T. Khoei, and N. Kaabouch, "A comparative analysis of the ensemble models for detecting gps spoofing attacks on uavs," in 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0310–0315, IEEE, 2022.

[430] X. Xiao, J. Dufek, T. Woodbury, and R. Murphy, "Uav assisted usv visual navigation for marine mass casualty incident response," in 2017 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), pp. 6105–6110, IEEE, 2017.

[431] M. Schörner, C. Wanninger, A. Hoffmann, O. Kosak, and W. Reif, "Architecture for emergency control of autonomous uav ensembles," in 2021 IEEE/ACM 3rd International Workshop on Robotics Software Engineering (RoSE), pp. 41–46, IEEE, 2021.

[432] D. A. Vallejo, "Electric currents: Programming legal status into autonomous unmanned maritime vehicles," Case W. Res. J. Int'l L., vol. 47, p. 405, 2015.

[433] T. A. Johansen and T. Perez, "Unmanned aerial surveillance system for hazard collision avoidance in autonomous shipping," in 2016 International Conference on Unmanned Aircraft Systems (ICUAS), pp. 1056–1065, IEEE, 2016.

[434] A. Ozturk, "Lessons learned from robotics and ai in a liability context: A sustainability perspective," in Sustainability in the Maritime Domain: Towards Ocean Governance and Beyond, pp. 315–335, Springer, 2021.

[435] M. T. A. Bakar and A. A. Jamal, "Latency issues in internet of things: a review of literature and solution," International Journal, vol. 9, no. 1.3, 2020.

[436] Statista, "Number of iot-connected devices worldwide from 2018 to 2030," 2024. last accessed: 22/01/2024.

[437] M. Ilyas, "Iot applications in smart cities," in 2021 International Conference on Electronic Communications, Internet of Things and Big Data (ICEIB), pp. 44–47, IEEE, 2021.

[438] O. Salman, I. Elhajj, A. Chehab, and A. Kayssi, "Iot survey: An sdn and fog computing perspective," Computer Networks, vol. 143, pp. 221–246, 2018.

[439] S. Shukla, M. F. Hassan, D. C. Tran, R. Akbar, I. V. Paputungan, and M. K. Khan, "Improving latency in internet-of-things and cloud computing for real-time data transmission: a systematic literature review (slr)," Cluster Computing, pp. 1–24, 2021.

[440] S. Khanagha, S. Ansari, S. Paroutis, and L. Oviedo, "Mutualism and the dynamics of new platform creation: A study of cisco and fog computing," Strategic Management Journal, vol. 43, no. 3, pp. 476–506, 2022.

[441] S. Roy, E. Saxena, and A. Quadir Md, "Minimizing latency while transferring iot data to cloud using gap optimization algorithm," in International Virtual Conference on Industry, pp. 33–46, Springer, 2021.

[442] S.-H. Hsu, C.-H. Lin, C.-Y. Wang, and W.-T. Chen, "Minimizing upload latency for critical tasks in cellular-based iot networks using multiple relays," in 2017 IEEE International Conference on Communications (ICC), pp. 1–7, IEEE, 2017.

[443] N. Tahmasebi-Pouya, M. A. Sarram, and S. Mostafavi, "A reinforcement learning-based load balancing algorithm for fog computing," Telecommunication Systems, vol. 84, no. 3, pp. 321–339, 2023.

[444] E. P. Pereira, E. L. Padoin, R. D. Medina, and J.-F. Méhaut, "Increasing the efficiency of fog nodes through of priority-based load balancing," in 2020 IEEE Symposium on Computers and Communications (ISCC), pp. 1–6, IEEE, 2020.

[445] M. Aqib, D. Kumar, and S. Tripathi, "Machine learning for fog computing: Review, opportunities and a fog application classifier and scheduler," Wireless Personal Communications, vol. 129, no. 2, pp. 853–880, 2023.

[446] M. Hunko, V. Tkachov, A. Kovalenko, and H. Kuchuk, "Advantages of fog computing: A comparative analysis with cloud computing for enhanced edge computing capabilities," in 2023 IEEE 4th KhPI Week on Advanced Technology (KhPIWeek), pp. 1–5, IEEE, 2023.

[447] M. Noura, M. Atiquzzaman, and M. Gaedke, "Interoperability in internet of things: Taxonomies and open challenges," Mobile networks and applications, vol. 24, pp. 796–809, 2019.

[448] S. S. Shree and J. F. G. Poovathy, "Communication technologies in iot and related concepts: A review," in 2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT), pp. 310–314, IEEE, 2022.

[449] R. Beraldi, C. Canali, R. Lancellotti, and G. P. Mattia, "A random walk based load balancing algorithm for fog computing," in 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC), pp. 46–53, IEEE, 2020.

[450] M. A. Jasim, N. Siasi, and A. Aldalbahi, "Pre-overload migration scheme for nfv-based fog computing," in Proceedings of the Int'l ACM Symposium on Mobility Management and Wireless Access, pp. 99–103, 2023.

[451] Q. Fan and N. Ansari, "Towards workload balancing in fog computing empowered iot," IEEE Transactions on Network Science and Engineering, vol. 7, no. 1, pp. 253–262, 2018.

[452] P. Singh and R. Agrawal, "An overloading state computation and load sharing mechanism in fog computing," Journal of Information Technology Research (JITR), vol. 14, no. 4, pp. 94–106, 2021.

[453] M. Al-Khafajiy, T. Baker, A. Waraich, D. Al-Jumeily, and A. Hussain, "Iot-fog optimal workload via fog offloading," in 2018 IEEE/ACM international conference on utility and cloud computing companion (UCC companion), pp. 359–364, IEEE, 2018.

[454] B. Nair and M. S. B. Somasundaram, "Overload prediction and avoidance for maintaining optimal working condition in a fog node," Computers & Electrical Engineering, vol. 77, pp. 147–162, 2019.

[455] C. Yi, S. Huang, and J. Cai, "Joint resource allocation for device-to-device communication assisted fog computing," IEEE Transactions on Mobile Computing, vol. 20, no. 3, pp. 1076–1091, 2019.

[456] J. Vashistha and A. K. Jayswal, "Comparative study of load balancing algorithms," IOSR Journal of Engineering, vol. 3, no. 3, pp. 45–50, 2013.

[457] Q. M. Tran, P. H. Nguyen, T. Tsuchiya, and M. Toulouse, "Designed features for improving openness, scalability and programmability in the fog computing-based iot systems," SN Computer Science, vol. 1, pp. 1–12, 2020.

[458] I. Ahammad, "Fog computing complete review: Concepts, trends, architectures, technologies, simulators, security issues, applications, and open research fields," SN Computer Science, vol. 4, no. 6, p. 765, 2023.

[459] S. Alraddady, B. Soh, M. A. AlZain, and A. S. Li, "Fog computing: strategies for optimal performance and cost effectiveness," Electronics, vol. 11, no. 21, p. 3597, 2022.

[460] J.-y. Baek, G. Kaddoum, S. Garg, K. Kaur, and V. Gravel, "Managing fog networks using reinforcement learning based load balancing algorithm," in 2019 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1–7, IEEE, 2019.

[461] M. Kaur and R. Aron, "A systematic study of load balancing approaches in the fog computing environment," The Journal of supercomputing, vol. 77, no. 8, pp. 9202–9247, 2021.

[462] X. Gao, X. Huang, S. Bian, Z. Shao, and Y. Yang, "Pora: Predictive offloading and resource allocation in dynamic fog computing systems," IEEE Internet of Things Journal, vol. 7, no. 1, pp. 72–87, 2019.

[463] A. Mseddi, W. Jaafar, H. Elbiaze, and W. Ajib, "Joint container placement and task provisioning in dynamic fog computing," IEEE Internet of Things Journal, vol. 6, no. 6, pp. 10028–10040, 2019.

[464] M. Al-Khafajiy, T. Baker, H. Al-Libawy, Z. Maamar, M. Aloqaily, and Y. Jararweh, "Improving fog computing performance via fog-2-fog collaboration," Future Generation Computer Systems, vol. 100, pp. 266–280, 2019.

[465] M. H. Kashani and E. Mahdipour, "Load balancing algorithms in fog computing," IEEE Transactions on Services Computing, vol. 16, no. 2, pp. 1505–1521, 2022.

[466] A. Brogi and S. Forti, "Qos-aware deployment of iot applications through the fog," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1185–1192, 2017.

[467] S. Sarkar and S. Misra, "Theoretical modelling of fog computing: a green computing paradigm to support iot applications," Iet Networks, vol. 5, no. 2, pp. 23–29, 2016.

[468] A. Ahmed, H. Arkian, D. Battulga, A. J. Fahs, M. Farhadi, D. Giouroukis, A. Gougeon, F. O. Gutierrez, G. Pierre, P. R. Souza Jr, et al., "Fog computing applications: Taxonomy and requirements," arXiv preprint arXiv:1907.11621, 2019.

[469] Q. Shen, L. Huang, G. Zhang, and J. Gong, "Policy control and traffic aggregation for m2m services in mobile networks," in Proceedings 2013 International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC), pp. 3391–3395, IEEE, 2013.

[470] A. K. M. Al-Qurabat and A. K. Idrees, "Energy-efficient adaptive distributed data collection method for periodic sensor networks," International Journal of Internet Technology and Secured Transactions, vol. 8, no. 3, pp. 297–335, 2018.

[471] A. K. Idrees and A. K. M. Al-Qurabat, "Distributed adaptive data collection protocol for improving lifetime in periodic sensor networks.," IAENG International Journal of Computer Science, vol. 44, no. 3, 2017.

[472] G. Zhu, J. Xu, K. Huang, and S. Cui, "Over-the-air computing for wireless data aggregation in massive iot," IEEE Wireless Communications, vol. 28, no. 4, pp. 57–65, 2021.

[473] A. K. Idrees, W. L. Al-Yaseen, M. Abou Taam, and O. Zahwe, "Distributed data aggregation based modified k-means technique for energy conservation in periodic wireless sensor networks," in 2018 IEEE middle east and north africa communications conference (MENACOMM), pp. 1–6, IEEE, 2018.

[474] M. H. Homaei, E. Salwana, and S. Shamshirband, "An enhanced distributed data aggregation method in the internet of things," Sensors, vol. 19, no. 14, p. 3173, 2019.

[475] A. Mahjoubfar, J. Chan, M. H. Asghari, and B. Jalali, "Sparsity and self-adaptivity in anamorphic stretch transform," in 2015 49th Annual Conference on Information Sciences and Systems (CISS), pp. 1–3, IEEE, 2015.

[476] B. Di Martino, R. Aversa, G. Cretella, A. Esposito, and J. Kołodziej, "Big data (lost) in the cloud," International Journal of Big Data Intelligence, vol. 1, no. 1-2, pp. 3–17, 2014.

[477] C. Yang, X. Zhang, C. Zhong, C. Liu, J. Pei, K. Ramamohanarao, and J. Chen, "A spatiotemporal compression based approach for efficient big data processing on cloud," Journal of Computer and System Sciences, vol. 80, no. 8, pp. 1563–1583, 2014.

[478] K. Ackermann and S. D. Angus, "A resource efficient big data analysis method for the social sciences: the case of global ip activity," Procedia Computer Science, vol. 29, pp. 2360–2369, 2014.

[479] B. Jalali and M. H. Asghari, "The anamorphic stretch transform: Putting the squeeze on "big data"," Optics and Photonics News, vol. 25, no. 2, pp. 24–31, 2014.

[480] M. Weinstein, F. Meirer, A. Hume, P. Sciau, G. Shaked, R. Hofstetter, E. Persi, A. Mehta, and D. Horn, "Analyzing big data with dynamic quantum clustering," arXiv preprint arXiv:1310.2700, 2013.

[481] A. Cichocki, "Era of big data processing: A new approach via tensor networks and tensor decompositions," arXiv preprint arXiv:1403.2048, 2014.

[482] A. Ukil, S. Bandyopadhyay, and A. Pal, "Iot data compression: Sensor-agnostic approach," in 2015 data compression conference, pp. 303–312, IEEE, 2015.

[483] J. D. A. Correa, A. S. R. Pinto, and C. Montez, "Lossy data compression for iot sensors: A review," Internet of Things, vol. 19, p. 100516, 2022.

[484] C. J. Deepu, C.-H. Heng, and Y. Lian, "A hybrid data compression scheme for power reduction in wireless sensors for iot," IEEE transactions on biomedical circuits and systems, vol. 11, no. 2, pp. 245–254, 2016.

[485] K. Loayza, P. Lucas, and E. Peláez, "A centralized control of movements using a collision avoidance algorithm for a swarm of autonomous agents," in 2017 IEEE Second Ecuador Technical Chapters Meeting (ETCM), pp. 1–6, IEEE, 2017.

[486] S. Dawaliby, A. Aberkane, and A. Bradai, "Blockchain-based iot platform for autonomous drone operations management," in Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and beyond, pp. 31–36, 2020.

[487] M. A. Azam, S. Dey, H. D. Mittelmann, and S. Ragi, "Decentralized uav swarm control for multitarget tracking using approximate dynamic programming," in 2021 IEEE World AI IoT Congress (AIIoT), pp. 0457–0461, IEEE, 2021.

[488] N. Islam, M. M. Rashid, F. Pasandideh, B. Ray, S. Moore, and R. Kadel, "A review of applications and communication technologies for internet of things (iot) and unmanned aerial vehicle (uav) based sustainable smart farming," Sustainability, vol. 13, no. 4, p. 1821, 2021.

[489] L. Xiang, F. Wang, W. Xu, T. Zhang, M. Pan, and Z. Han, "Dynamic uav swarm collaboration for multi-targets tracking under malicious jamming: Joint power, path and target association optimization," arXiv preprint arXiv:2306.16196, 2023.

[490] C. Shen, T.-H. Chang, J. Gong, Y. Zeng, and R. Zhang, "Multi-uav interference coordination via joint trajectory and power control," IEEE Transactions on Signal Processing, vol. 68, pp. 843–858, 2020.

[491] Y. Wu, W. Yang, X. Guan, and Q. Wu, "Energy-efficient trajectory design for uav-enabled communication under malicious jamming," IEEE Wireless Communications Letters, vol. 10, no. 2, pp. 206–210, 2020.

[492] Q. Cui, "Multi-target points path planning for fixed-wing unmanned aerial vehicle performing reconnaissance missions," in 5th International Conference on Information Science, Electrical, and Automation Engineering (ISEAE 2023), vol. 12748, pp. 713–723, SPIE, 2023.

[493] Y. Wu, S. Wu, and X. Hu, "Multi-constrained cooperative path planning of multiple drones for persistent surveillance in urban environments," Complex & Intelligent Systems, vol. 7, pp. 1633–1647, 2021.

[494] G. Tang, C. Tang, H. Zhou, C. Claramunt, and S. Men, "R-dfs: A coverage path planning approach based on region optimal decomposition," Remote Sensing, vol. 13, no. 8, p. 1525, 2021.

[495] L. Li, D. Shi, S. Jin, S. Yang, Y. Lian, and H. Liu, "Sp2e: Online spiral coverage with proactive prevention extremum for unknown environments," Journal of Intelligent & Robotic Systems, vol. 108, no. 2, p. 30, 2023.

[496] T. M. Cabreira, "Energy-aware coverage path planning for unmanned aerial vehicles," 2019.

[497] H. Wang, S. Zhang, X. Zhang, X. Zhang, and J. Liu, "Near-optimal 3-d visual coverage for quadrotor unmanned aerial vehicles under photogrammetric constraints," IEEE Transactions on Industrial Electronics, vol. 69, no. 2, pp. 1694–1704, 2021.

[498] G. Fevgas, T. Lagkas, V. Argyriou, and P. Sarigiannidis, "Coverage path planning methods focusing on energy efficient and cooperative strategies for unmanned aerial vehicles," Sensors, vol. 22, no. 3, p. 1235, 2022.

[499] J. I. Vasquez-Gomez, M. Marciano-Melchor, L. Valentin, and J. C. Herrera-Lozada, "Coverage path planning for 2d convex regions," Journal of Intelligent & Robotic Systems, vol. 97, pp. 81–94, 2020.

[500] J. Muñoz, B. López, F. Quevedo, C. A. Monje, S. Garrido, and L. E. Moreno, "Multi uav coverage path planning in urban environments," Sensors, vol. 21, no. 21, p. 7365, 2021.

[501] L. Zhou, S. Leng, Q. Liu, and Q. Wang, "Intelligent uav swarm cooperation for multiple targets tracking," IEEE Internet of Things Journal, vol. 9, no. 1, pp. 743–754, 2021.

Author's publication

International publications

Mabrek, Zahia, Brahim Farou, Zineddine Kouahla, Nadjette Benhamida, and Hamid Seridi. "A novel drone recovery system in IoT environment." International Journal of Sensor Networks. Lien: https://doi.org/10.1504/IJSNET.2023.131250. May 25, 2023.

Mabrek, Zahia, Brahim Farou, Zineddine Kouahla, Hamid Seridi and Muhammet Kurulay."Fog Node Overload: Dynamic Solution for Enhanced IoT Efficiency" cluster computing.
Current statue:Under Review.

International Communications

Zahia, Mabrek, Farou Brahim, Kouahla Zineddine, and Seridi Hamid. "Optimizing Data Transmission in IoT-Based Drone Networks Through Fog Area Division." In 2023 International Conference on Decision Aid Sciences and Applications (DASA). Lien: 10.1109/DASA59624.2023.10286737. 16-17 September 2023.

Zahia, Mabrek, Farou Brahim, Kouahla Zineddine, and Seridi Hamid. "Enhanced Multi-Target Surveillance and Tracking Algorithm for Collaborative Drones in IoT Environment." In 2023 International Conference on Electrical Engineering and Advanced Technology (ICEEAT). Lien: 10.1109/ICEEAT60471.2023.10426073. 05-07 November 2023.

National Communications

Zahia Mabrek, ines Boulefrakh, Brahim Farou, Zineddine Kouahla and Hamid Seridi, "Organ Segmentation From Medical Images", 5nd Conference on Informatics and Applied Mathematics IAM'2022, Guelma, Algeria, 2022.

Zahia Mabrek, Samir Halaci, Zineddine Kouahla, Muhammet Kurulay and Hamid Seridi, "A Report on the applications of UAVs in Internet of Things (IoT) ", 4nd Conference on Informatics and Applied Mathematics IAM'2021, Guelma, Algeria, 2021.