A picture containing font, graphics, logo, symbol

Description automatically generated

**Central Queensland University**

**400 Kent Street, Sydney**

**Assignment 1 (Group and individual Work)**

**Of**

**NETWORKS AND INFORMATION SECURITY PROJECT COIT20265 (HT1, 2024)**

**On**

**Drone Based Data Collection from Ground IoT Nodes:Simulation Study in MATLAB**

**Unit Coordinator: Biplob Ray**

**Tutor: Prabhu Singh**

**Submitted By:**

**Name: Student ID:**

**Ali Raza 12191317**

**Santosh Paneru 12210976**

**Namaraj Thapaliya 12200848**

Table of Contents

[1. Project Description and Business Problem 2](#_heading=h.gjdgxs)

[2.Technical Milestones or Deliveries 3](#_heading=h.30j0zll)

[3.Literature Review 4](#_heading=h.1fob9te)

[4.Functional requirement 6](#_heading=h.3znysh7)

[5.Usability requirement 6](#_heading=h.2et92p0)

[6.Reliability requirement 7](#_heading=h.tyjcwt)

[7.Security requirement 7](#_heading=h.3dy6vkm)

[8.Physical/ Logical design of the network 7](#_heading=h.1t3h5sf)

[9. Network and security technologies. 7](#_heading=h.4d34og8)

[9.1 Perception layer 8](#_heading=h.17dp8vu)

[9.2 Network layer. 8](#_heading=h.3rdcrjn)

[9.3 Edge layer 8](#_heading=h.26in1rg)

[9.4 Application layer 8](#_heading=h.lnxbz9)

[9.5 Attacks and solutions on layers 8](#_heading=h.35nkun2)

[10. Drones Path Planning 11](#_heading=h.1ksv4uv)

[11 Individual Part 13](#_heading=h.44sinio)

[11.1 Namaraj Thapaliya 12200848 13](#_heading=h.2jxsxqh)

[11.2 Santosh Paneru- 12210976 14](#_heading=h.z337ya)

[11.3 Ali Raza 12191317 14](#_heading=h.3j2qqm3)

[12. Cost Effective Budget 16](#_heading=h.1y810tw)

[12.1 Budget Table for Simulation Environment Setup 16](#_heading=h.4i7ojhp)

[12.2 Budget Table for Drone Model and IoT Nodes 16](#_heading=h.2xcytpi)

[12.3 Total Budget Table 17](#_heading=h.1ci93xb)

[13 Risk Assessment and a Plan 17](#_heading=h.3whwml4)

[13.1 Risk Assessment Plan 18](#_heading=h.2bn6wsx)

[14. Technical Hardware and Software Components 19](#_heading=h.qsh70q)

[Reference 20](#_heading=h.3as4poj)

Project description and Business Problem

In this technological world we all are well aware that everything is becoming smart. Which means there are various computer programed system, algorithm or Internet on Things device which are designed and developed to make human life easy. There are several real time Internet on Things example where various computer programmed device or system are integrated together to solve the real time problem. In this project also we will use an Internet on things algorithms called Travels sales man problem(TSO) to make a smart farming. For this project, we have a certain amount of agricultural land field where farmer used to do farming in traditional manner. Now to make the process more technologically advance and reduce manual labour for farmer, we will transfer the entire field into smart farming. Before begin in the project we will first create an identical farm and do computer simulation by putting exact same parameter on MATLAB. In the MATLAB we will create same size of farm land and we will implement same amount ground node. Regarding the distance for ground nodes, first we will simulate those nodes on MATLAB and simulate it multiple times. We will only use the best distance that we will get from simulation.

In Australia the farm field are massive in size and to cover all those field with these nodes and UAV it is going to be costly for the farmers. Because of the cost the farmers may not afford to implement these system to their farm. Lack of real time data availability which will effect on the yield of crops. Communication problem with ground nodes and UAV. To create shortest and most efficient path of the UAV to go to each ground nodes, where it can cover all the nodes in shortest time frame Providing powers to all those nodes on the ground is a quite challenging task because when those nodes runs out of battery, it is going to be very difficult to replace it. These are various numbers of problem that we may encounter while implementing the system. But out of various business problems, in this project we will only focus on solving only one problem of the distance. In this entire project we will try to get shortest path for UAV to travel in between the ground nodes and to get the best outcome first we will use computer simulation programme called MATLAB, simulate the condition, get the best result and implement it.

Purposed Solution:

We will be using an existing algorithm to calculate shortest path for UAV called Technical Milestone or Deliveries

1) Implement in MATLAB for simulation: In this part we will implement the existing algorithm in this case in MATLAB for the simulation. In this stage what will happen is we will install MATLAB into our system and implement TSP algorithm into it so that we can calculate the shortest path for the UAV to travel in between the ground nodes. There are some steps that we will perform which I would like to mention here. Firstly we will determine the function that we want to optimize. The function will take an input as vector and return scalar value. After that we will set up the parameters of swarm size.

2) Finding best position for nodes: To get the best path for UAV it is very crucial to implant ground nodes in a perfect location. We need to figure out the distance between the ground nodes for the best optimization. This can be done through the simulation and it is one of our goals in the project for finding the best position and distance for ground nodes.

3) Simulation development in MATLAB: Simulation in MATLAB is one of our technical deliveries in this project. First we will use simulated environment using MATLAB to assure everything that we are using are in right and they will function properly.

Literature Review

An Optimal Multi-UAV Deployment Model for UAV-assisted Smart Farming by Jahan Hassan, Shavbo Salehi, Ayub Bokani

The main gap in this article and our project is that in this project there are multiple UAV but in our project we will be using only one UAV to cover multiple ground nodes. The main advantage we will gain from this project comparing to the article is that cost effective. When we are using less UAV than we will be saving buying cost of it. Other advantage is that the UVA will not collide to each other because there is only one flying over the field. In the literature the authors points out about using 5G mobile network UAV where in our project also we can use that method. In the article the authors are pointing at the positioning of the ground nodes, the significant values of right position of nodes for error free data reading, whereas in our project also the ground positioning of the nodes plays crucial role to read the data in proper manner. This literature explain about many business problems that we will face in our project also. The main difference between the article and our project is that in the article they use multiple UAV for smart farming but in our project model we will use one UAV that will be used to read multiple ground nodes. In the article authors purposed multi- criteria Decision Making (MCDM) where it allows UAVs to provide various services to mobile, dynamic, and randomly distributed ground IoT devices. On the other hand in our project we will use practical swarm optimization algorithm to calculate shortest path. Where they are using k-means algorithm where they classify ground nodes into multiple cluster based on their current location.

This model and approach was purposed for multiple UAVs that will fly over the field to collect data. On the other hand, we are developing the project in similar scenario but unlike the article we will be using single UAV to fly over the field.

LoRa Communications as an Enabler for Internet of Drones towards Large-Scale Livestock Monitoring in Rural Farms by Mehran Behjati, Aishah Binti Mohd Noh, Haider A. H. Alobaidy, Muhammad Aidiel Zulkifley, Rosdiadee Nordin, and Nor Fadzilah Abdullah

In this paper, authors are discussing about the usage of drones and lot nodes to monitoring the livestock in rural farms. The paper main focus is to help farmers to develop a farm monitoring system with the help of UAV, LPWAN and lot technologies. Lot-based water monitoring system is developed to check the quality of water because its is important for livestock development. For the communication, author used Long-Range Wide-Area Network (LoRaWAN®) technology, a multi-channel LoRaWAN® gateway and integrated into a drone to collect data from the sensors and upload to the cloud for further analysis. Furthermore, to increase the efficiency of Ariel-bases data collection, author used UAO oath planning optimization to find best path pathways for drones to cover whole livestock farm and used multiply gateways for communication. To find optimizing flight paths, author used PSO and EPSO algorithms. In addition, they explained that by optimizing flight paths and aerial data collection performance with real-time data and with help of graphs and table in shorter time that cover the whole farm within minimum timeframes. Like this project, we used that Travels sales man problem(TSO) to find best drone path that can cover whole farmland.

Functional requirement

1) Ground Node positioning: We need to make sure that all the node are in perfect location and has perfect distance in between them so that an UAV to travel in between them where it can travel through all ground nodes by covering shortest distance.

2) Shortest Path Algorithm for UAV: We should determine that what algorithm we are going to use to determine the shortest path for UAV to cover all the field. In this case we will implement the algorithm called Travels sales man problem(TSO).

3) Valid calculation of shortest path: This is another important functional requirement that we require to perform in our project. We need to make sure that the algorithm that has been implemented must calculate valid path every time when it is collecting the data from ground nodes.

4) Simulation environment in MATLAB: At the beginning, we need to make sure that every tools and algorithm we are using is most efficient. To make sure we do not make any human error we simulate the entire scenario in MATLAB first. When the simulation yields the desirable outcome then only we implement physically.

Usability requirement

1) UI/UX: There must be an interactive user interface of the whole system for any user to operate the programme. The user might form a non-technical background and they also should be able to operate the project easily. For the simulation we will be using the user interface of MATLAB.

2) Documentation: The each and every steps of the project and its operation, how to operate it, the working mechanism, details explanation about software management should be well documented for future purposes.

Reliability requirement

1) Stable management software: The reliable working back end software is needed to maintain and control the UAV, to check the status of the nodes like its battery power, to manipulate the data obtained from the nodes. We could use the software like Azure IoT hub, IBM and data dog etc.

2) Error handling: There are possibilities that we will encounter error while collecting the data or using the UAV in the field. We can make sure that we could handle errors by performing multiple level of testing before implementing the project.

3) Hardware: This is another important requirement in this project. We must maintain all of our hardware is in working condition. We must always have backup device for worst case scenario.

Security requirement

1)Encryptions: Our project should consist of encryptions algorithms like Advance Encryption Protocol(AES) while collecting data from ground nodes to UAV

2)Authentication and authorization: In our project user should authenticate themselves before giving them permission to use the system. This can be possible by using strong password system. This will prevent others to give access to the system.

3)Secure Communication channel: We need to establish secure communication channel in between UAV and our database by establishing secure wireless connection. To establish secure wireless connection we need to develop security protocols.

4)Physical security measures: We need to protect our UAV from physical attack. While flying in the field somebody can attack it or it can also be stolen.

# 8.Physical/ Logical design of the network

In this project, logical design explains the communication pathways between nodes and drones. We are using mash technology and protocols for data exchange. Logical design has a network, edge and application layer. These three layers are explained in the network and security technologies topic.

In physical network design, we need to place nodes (sensors) in farmland such as moister sensors, health monitoring sensors environmental sensors and drones. These nodes are placed in farmland in a way that covers the whole area. We will install ground nodes in a way that our drone can cover all nodes within a minimum time. For example, place each node after almost 1000 meters or placed randomly.

# 9. Network and security technologies.

Smart farming systems have four different layers in logical design such as the perception layer, network layer, application layer and edge. Each layer has different responsibilities such as collecting data, transporting data, processing, and storing data **(Mekala, M.S, 2017)**. When the storage, management and data processing connect with the internet it brings issues and security threads.

## 9.1 Perception layer

The perception layer has sensors, cameras, actuators, drones, Tag Radio-Frequency Identification (RFID) and Global Positioning System (GPS) and also called physical layer **(da Silva, E,2020).** In our project, we are using 3 types of sensors on agricultural land: moister, health monitoring and environmental sensors.

## 9.2 Network layer.

The network layer has a connection technology to connect ground nodes to the internet or cloud. This is used for connectivity and transferring data. Routers, protocols, and access points are used as connection devices **(Zhao, W., 2017).** In this project, we can use mesh networking protocols (Zigbee, LoRaWAN, SignFox) for the communication between nodes and drones because, in smart farming, these protocols have robustness and reliability in data transmission. There are other cellular network protocols such as 3G/4G and WiFi but it has vulnerabilities. These network protocols are more exposed to the world and can be compromised easily.

## 9.3 Edge layer

The edge layer includes security features, an in-out interface, diverse resources, and gateways. Security features ensure the security protocols (Encryption and decryption), integrity, availability and confidentiality of the data and system **(Kumar, S.A, 2016).** The communication between nodes and drones will be fully encrypted with the cryptographic algorithm (Advanced Encryption Standard) and prevent system form attacks and unauthorized access.

## 9.4 Application layer

The application layer is the last layer of the smart farming system. It has a database, web tools such as MATLAB, a system of decision making and end-user applications **(Sikdar, B., 2019).** During project implementation, we use MATLAB application to apply algorithms to find the shortest path for drones to complete the whole ground field.

## 9.5 Attacks and solutions on layers

Here is the list of attacks that happen on different layers.

**Table 1**

| **Layers** | **Attacks** | **Attacks Explanation** | **Solutions** |
| --- | --- | --- | --- |
| Perception layer | Random sensors incidents | Sensors are deployed in the farmland where they do not have proper protection. The sensors can have incidents such as sensor loss, interaction with animals, damage under the tractor while farming etc. | Needs to provide physical protection to sensors. For example, build a safety wall around the sensors. |
| System hijacking | Hackers can control the tractors and UAVs/ Drones on the farmland. They can control the drones and perform tasks to damage the crops. | Needs to build strong authentication, encryption and decryption methods such as AES. |
| Optical deformation | Reduce the quality of pictures. For example, if cameras are capturing pictures of fruits or vegetables on the land. The quality of the image is lower than expected. It will be hard for farmers to know the real condition of fruit trees. | Regular maintenance of cameras. |
| Irregular measurement | Send a false measurement about farms and the environment to farmers such as energy depletion, severe weather and false input. | Implement a detection system that can identify abnormal environmental readings. |
| Sensor weakening | Sensor effects with environment. For example, wind sensors become dusty and do not work according to requirements. | Dust should be removed from the sensors after every 6 months. |
| Sleep deprivation | Drains the battery of sensors. When the battery of sensors is down they can not collect data from fields. | Needs to implement energy-efficient sensors that work for long period of time. |
| Node capture | Steal the node or device from the farm. An attacker can hack the node, modify the software and inject false data. | Install an alarm system with nodes. Whenever someone touches the node the alarm system should send a signal to the former. |
| Network layer | Dos/DDos | An attacker can effect network delays, and disable devices and internet connectivity while doing Dos/DDos attack. | Built a network security firewall that can filter and block malicious traffic. |
| Data transit attacks | Attack data while transmitting from node to drones and drones to cloud. It happens because of unencrypted wireless and network connections. | Use encryption and decryption methods while transferring data between nodes, clouds and drones. |
| Routing attacks | Get control of routers and traffic paths. Attacks like Sinkholes and wormholes attacks can change communication networks and get access. | Access control mechanisms and network segmentation can prevent the routers from authorized traffic paths and access. |
| Edge layer | Forged control for actuators | Attackers find out the patterns of communication between sensors and gateways or clouds. So he can upload the data with the same pattern on the system. It will be hard for the system to analyse the false data because the pattern is the same. | Data validation and authentication methods can prevent the system from getting wrong/ false commands from attacker. |
| Gateways- cloud request forgery | Gateways and clouds are connected with the help of internet providers of cellular networks. There are so many attacks that can happen on internet connectivity. An attacker can create a frog request from the gateway to the internet and can manipulate the system. | Implement access control policies and secure internet connectivity. |
| Booting | Sensors are smaller and cheaper but do not have boot protection. Companies did not pay attention to the security of sensors. Devices will be vulnerable if they do not have a security system while booting. | A secure booting process can prevent the sensors from authorized malicious boot scripts. |
| Forged measure injection | Perception devices do not have complex security systems. They exchange data with the cloud or gateway with plain text. Attackers who know the pattern can inject the same pattern into the system. In this way, he can send false data to farmers about irrigation and soil moisture measurement. | Sensor data should be encrypted and secure channels should be used during data exchange. It will be hard for attackers to inject wrong /false data. |
| Unauthorised access | All data is passing through the gateways. Unauthorised access to the system can breach the confidentiality, integrity and availability of the system. With access to the system, he can control the communication. | Robust control mechanisms can be used to prevent authorized access to devices and gateways. |
| Man-in-the-middle | In this attack, the attacker hijacks the communication between the client and server and replaces it. Those nodes that do not have security features can be vulnerable to internal and external attacks. it is very hard to find man-in-the-middle attacks for the user because he thinks he is connected to the main server. | Intrusion detection systems and end-to-end encryption can be used to prevent man-in-the-middle attacks. |
| Signature wrapping | Signature wrapping happens when an attacker breaks the algorithm of the signature. After that, he can change the message accordingly. | Needs to update the cryptographic keys regularly to mitigate signature wrapping attacks. |
| Application layer | Phishing | In this attack, the attacker aims to get the user data such as password and ID. After getting the login details, he can send the command to sensors and change the system settings accordingly. | Farmers can use multiple authentication methods to avoid phishing attacks such as e-mail verification via code or link, and some keywords. |
| Malicious scripts | Farmers need to interact with the internet to get online services and information from other forms. Malicious scripts such as Java applets, Active-X scripts and XSS (cross-site scripting) mislead the customer and give wrong information. They will use useless advertisements, and false links to slow down your system. | Update the security details and implement the security policies in the system. The system will automatically avoid malicious scripts that are against the security policies. |
| DOS/DDOS | Give multiple requests to the system and make a system overloaded. | The system can limit the number of requests from users while using Rate-limiting and CAPTCHA mechanisms. For example, the system can only give access to 10 users at a time. |

# 10. Drones Path Planning

In this project, our main focus is on the shortest path planning of drones on farmland. We need to apply algorithms to cover the ground nodes with minimum timeframe and distance. Drones have high-resolution cameras, large wings that can hold the winds and modern batteries. Before drones had normal battery life that would not last longer. Now drones make a lot of development in the field of batteries. The batteries of drones have changed into Lithium-ion batteries which is the most advanced version of batteries. The flying time of small drones that have lithium-ion batteries is 20-30 minutes **(Lyu, Z., 2020).** The is not enough to cover the whole farmland without any path optimisation algorithm. If we increase the size the of battery, the overall weight of drones will increase, and drones use more energy. That means the problem is unsolved. Drones path planning is mainly focused on covering more distance with the minimum timeframe **(Chen, X., 2018).** Drone path planning is dependent on the behaviour of the environment because drones behave differently in different conditions. Mostly, the path planning of drones is divided into two methods online (global) and offline (local) method **(Xu, L., 2019)**. In global path planning, the drones know the environment work according to the plan and complete the mission. On the other hand, in local path planning, the environment was unknown. When the drones start flight they have an additional sensor that detects the environmental condition and uses real-time environmental detection and path planning. It is a complex process to optimize the drone's path planning because it depends on the problems and constraints such as dynamic (external factors that affect the drones during path planning such as environment and weather) and kinematics constraints (motion limitation of the UAV) **(Nordin, R ,2021).** In this project, we will use the latest drones that are specifically designed for large farmlands. Vertical Take-off and Landing (VTOL) drones are also known as AeroHawk. These drones have hybrid fixed wings and work on the mechanism of helicopters. Here is the specification of the drone.

Table 2:

| Drone type | Battery Powered VTOL |
| --- | --- |
| Aerodynamic design | Canard design |
| Power distribution | 8\*lifting motors/1\*propulsion motor Capable of hover normally with up to 2\*lifting motors/propellers failure on different sides |
| Size | 6\*3.2\*0.6M |
| Weight | 29Kg |
| Max Take off weight | 68Kg |
| Maximum payload weight | 15kg(One big battery + one small battery)) 20kg(TWO Big Battery ) |
| Maximum ascending speed (VTOL) | 3M/S |
| Maximum descending speed (VTOL) | 2M/S |
| Cruising speed | 25m/s (90km/h) |
| Flying speed | 34.8m/s (125km/h) |
| Maximum takeoff altitude | 4500M |
| Maximum flying altitude | 6000M |
| Maximum wind resistance | Level 7 in cruise |
| Weather proof | IP45 |
| Operation temperature | -20～60℃ |
| Material | Carbon fiber composite in 95% area Glass fiber composite in 5% area |
| Landing accuracy | 1-2m standard 0.5m with RTK |
| Maximum Endurance | 3 hours+ when carrying 10kg Payload 2.5 hours+ when carrying 15kg Payload 6 hours when carrying 1kg Payload |
| Maximum flight range | 500KM |
|  |  |
| Navigation | GNSS+INS |
| Navigation light | YES |
| IMU | 3 SETS |
| Compass&Heading | One compass One set of dual-GNSS antenna |
| AHRS facilitation | 5 mins after GNSS signal lost |
| Flight mode | Autonomous/Semi-autonomous |
| Safety Assurance | One-button RTL/Data link loss RTL/Low battery RTL Abnormal attitude RTL/Key sensor failure RTL/ Up to 2 VTOL motors failure protection/ Gliding after tail rotor thrust failure |
| FDR | YES |
|  | |
| Motor | Brushless electric motor |
| ESC | FOC ESC |
| Propeller | 30 inch customized carbon-fiber VTOL prop. 24 inch customized carbon-fiber Fixed-wing prop |
| Battery type | Li-ion/14S 2 or 3 pieces as options |
| Battery capacity | 61500mAh for each piece/11.8kg each piece |
| Battery charger | Fast charger 2 hour to charge each piece |
|  | |
| Data/Video Integrated link | 1427.9-1447.9MHz by choice |
| Mode | TDMA/5 Time slots Data or Video allocated by need |
| Modulation | OFDM/QPSK/16QAM/64QAM |
| Antenna | 2 as Single Tx Dual Rx |
| Encryption | AES 128 |
| Max Data /Video link range | 100km+ |
| Battery life | Nearly 4 hours |

**Source**: [www.uavfordrone.com](http://www.uavfordrone.com)

Because they don’t take too much time to take off and don’t need a long runway **(Abdullah, N.F., 2021).** For the shortest flight path for drones to cover long distances, we use Traveling Salesman Problem TSP modelled algorithms to solve this problem.

Here are the details of our farmland. The size of the farmland is 500 acres. We are using three types of ground node sensors such as soil, moisture and crop health. We have 50 soil, 50 moisture and 30 crop health sensors. The drone will fly from the ground station and cover all the sensors. Drone ground station will be outside the farmland. We will apply MATLAB code with model and calculate shortest path and time that takes drone to complete task.. We do two simulations in MATLAB one with TSP algorithms and the other without TSP model compare the differences between them.

# 11 Individual Part

## 11.1 Namaraj Thapaliya 12200848

**System Analyst**

<https://www.seek.com.au/IoT-system-analyst-jobs/in-All-Sydney-NSW?jobId=74856721&type=standout>

**Roles and Responsibilities**

* Configure and update the operating system and management software of the project.
* Provide technical support and troubleshooting to the team member regarding the simulation in MATLAB and while determining an algorithm.
* To develop and maintain emerging technologies, trends and best practice in system administration, cyber security and Internet on Things.
* Manage and protect IP assets.
* Collaborate with teams to develop and implement fully functional IT solution like updating of an algorithm and other necessary hardware.
* Implement cyber security polices to protect against threat like malware, phishing and unauthorized access.
* Documentation of IT procedure, configuration of UAV and algorithm and error handling steps for future references.
* To conduct regular security assessment, testing of UAV to identify vulnerabilities and areas that needs to be improved.

## 11.2 Santosh Paneru- 12210976

**Network Engineer**

**URL:** [**https://www.seek.com.au/Network-Engineer-jobs-in-information-communication-technology/engineering-network/in-All-Sydney-NSW?jobId=74518946&type=standout**](https://www.seek.com.au/Network-Engineer-jobs-in-information-communication-technology/engineering-network/in-All-Sydney-NSW?jobId=74518946&type=standout)

* **Roles/ Responsibilities**
* Do communication and handle situations for the setup and installation of the software MATLAB and UAV toolbox.
* Updates and installations of network
* Keeps technical documentation at the proper levels.
* Coordinates delivery and support of as needed with third-party provider services
* Complete the post-incident reviews for each priority occurrence and offer assistance in doing so.
* Managing and configuration of hardware components required in the projects for the simulations,
* Connecting and making the configuration of the IoT nodes with the drone
* Ensure the safety rules and regulations for the use of the devices.
* **Capabilities**
* Experience in doing proper communication and technical network services.
* Basic knowledge of the UAV technology and IoT hardware devices.
* Experience in fixing parts of hardware devices.
* Technical skills and ability of working in a group.
* Hardware and software for routers and switches are important.
* To collaborate both individually and as a team
* To advise analysts and make technical reports.
* Setting priorities and assigning work to teams on a priority basis
* Outstanding communication abilities both in writing and speaking

## 11.3 Ali Raza 12191317

**Security specialist**

**Roles and responsibilities:**

**Url:** [**https://www.seek.com.au/job/74654279?type=standout&ref=search-standalone#sol=401a8db06979bb33f66d0c69b51ccab817998a4b**](https://www.seek.com.au/job/74654279?type=standout&ref=search-standalone%23sol=401a8db06979bb33f66d0c69b51ccab817998a4b)

**Roles/ Responsibilities**

* Operating the information security management system in an organization.
* Develop information security polices and strategies according to the company objectives that can be used to minimize the cyber threads to company.
* Make a policy to protect the sensitive data of organization from attackers.
* Always get a knowledge with the latest cybersecurity threats, trends, and technologies.
* Always recommend new and advance enhancements to the company's security posture.
* Meeting with internal and external stakeholders, including IT, legal, and risk management teams, to check the security requirements.
* Support the improvement of our cyber security capabilities in a system.
* Respond to compliance audit requests.
* Demonstrate a strong understanding of compliance frameworks and regulations such as NIST, and CPS234.
* Conduct internal audits report and provide advance recommendations to key stakeholders based on research.
* Implement and maintain security tools.
* Implement systems that can ensure optimal performance and address evolving threats.
* Ensure Secure communication, for example, communication between nodes and drone.
* Always use advance encryption and decryption method while communication.

**Capabilities**

* Experience in information technology, information security, risk management
* Industry certifications such as CISSP, CISM or CISA are highly desirable
* Demonstrated knowledge and understanding of contemporary frameworks and methodologies, such as ISO 27001, NIST 800-53,
* Detailed knowledge of NIST Cyber Security Framework (CSF), and Australian Information Security Manual (ISM)
* Excellent written, oral, and influencing skills with the ability to work autonomously
* A strong focus on continuous improvement of skills.
* Broad knowledge of current Governance, Risk and Compliance (GRC) technological tools and methodologies.
* Detailed knowledge of cryptography
* Problem solving skills in case of attack on system and experience how to mitigate complex security challenges.
* Strong consultative skills, enabling effective communication of complex concepts to both technical and non-technical users.
* A strong desire to learn and expand knowledge in the field of information and network security.

# 12. Cost Effective Budget

For the overall completion of the project, we need different hardware, software, and simulation devices. The tables given below are the detailed cost-effective budget tables that we are using for the completion of the project. The tables are based on the milestones we need to achieve which is shown below:

## 12.1 Budget Table for Simulation Environment Setup

| **Item** | **Description** | **Cost (AUD)** | **Source of Funds** |
| --- | --- | --- | --- |
| MATLAB Simulink | We need the license for the MATLAB Simulink | $1100 | Funded by department |
| Hardware devices | We need to manage the Workstation for the Simulation | $3500 | Group Collection |
| Simulation Software | It is the major requirement: MATLAB UAV Toolbox | $1600 | University funded |
| Cloud computing Devices | Cloud computing subscription is required. | $800 | University Funded |
| Miscellaneous | Connectors, cables, and other materials may be required. | $150 | Fund collection in Group |
| **Total** |  | **$7150** |  |

**Table 2: Budget Table for Simulation Environment**

## 12.2 Budget Table for Drone Model and IoT Nodes

| **Item** | **Description** | **Cost (AUD)** | **Source of Funds** |
| --- | --- | --- | --- |
| **Drone** | DJI Phantom 4 Pro (DJI, 2024) | $2399 | Funded by department |
| **Backup Drone** | Sky Dio 2 (\*2)  Required when main drone used gets problem (Fisher J, 2022). | $3000 | Funded by department |
| **IoT Nodes** | We need IoT development board for the working. | $600 | Funded by University |
| **Communication Modules** | GSM/GPRS Module is required for tracking the information based on GPRS tracking from certain distance (Akanda, N.I 2022) | $150 | Fund collection in Group |
| **Miscellaneous** | Mounts, handle, kits, Housing, and other tools may be further required as backup. | $350 | Fund collection in Group |
| **Total** |  | **$6499** |  |

Table 3:Budget Table for Drone Modeland IoT nodes

Also, for working on the trajectories and path finding, to view the Performance Strategy of the simulation in MATLAB we need to keep on storing the data based on the variation distance calculations. For this we need to set up the software in MATLAB so that we can get the accurate simulation data. The overall budget calculation is given in below table:

## 12.3 Total Budget Table

| **Category** | **Total Cost in AUD $** |
| --- | --- |
| **Simulation Environment Setup** | $ 7000 |
| **Drone Model and IoT Nodes** | $ 6250 |
| **Miscellaneous** | $ 500 |
| **Total** | **$ 13750** |

Table 4: Total Budget Table

# 13 Risk Assessment and a Plan

We may identify some of the risks that may hinder us from achieving our desired outcomes and the milestones and the plan for the mitigation is discussed. Firstly, some of the risks that we may identify are discussed below.

* **Weather Conditions:** Weather conditions are the major risk that may arise. Due to the adverse changes in the weather conditions of the surroundings, drone operations and the data collection may be affected (Gao, M 2021).
* **Technical Failure**: Drones have different nodes which are used for the movements and also for the functioning of the overall drone performance, but there may be malfunction or the breakdown of the drones or IoT nodes during the data collection time.
* **Regulatory Compliance:** We may fail to comply with Local rules and the regulations for the use of the drones and we need may fail to keep the data private while working in the real environment during data collection.
* **Data Loss and data breach:** Unauthorized access of the data while transferring data may cause the risk of data breaching. Also, data may be deleted and causes our data loss.

## 13.1 Risk Assessment Plan

For the risk that may arises during the project time, we can do the plan based on the threat modelling process which is explained in the below points:

**Identifying the likely threats:** We need to identify the threats that may arises in the project that may be data, hardware and other components.

**Threat and likelihood assessment:** Once the threat are identified we can use the threat modelling process to access the impact and likelihood so that we being all the team members can priotize and focuse on the task based on the resources.

**Risk analysis and mitigation:** We can analyse the risk based on the impack and likelihood which impact on the project. It makes us easier to develop the strategies for miniming the risk that are identified by implementing security measures, patches and so on.

Further we nee d to follow the following steps for managing the risk that we may get during the simulation time. Some of the major points are described below:

* **Weather Conditions**
* Mitigation: We need to do the regular monitor in the weather forecast. Based on the weather conditions we need to make our schedule of the drone operations based on the suitable conditions.
* Contingency: While using the ground-based sensors we need to make a backup plan for the collection of the data because of the weather condition.
* **Technical Failure**
* Mitigation: We need to do regular checkups for the maintenance of the hardware devices and try to repair them as necessary.
* Contingency: During the simulation time we need to take the backup devices like drones and IT nodes so that failure of one device can be used with another device.
* **Regulatory Compliance**
* Mitigation: There may be rules and regulations in different environments for the use of drones. We need to take the license for the drone operations and stay updated for local regulation every time as needed.
* Contingency: We need to ensure compliance with the data privacy rules. Need to put the legal person if possible.
* **Data loss and data breach**
* Mitigation: We need to make secure data encryption for the transmission of the data and to store the data in the devices.
* Contingency: Need to be more careful with the identification of vulnerabilities and take action to remove them carefully.

# 14. Technical Hardware and Software Components

| **Hardware and Software Components** | | | |
| --- | --- | --- | --- |
| **Hardware** | | **Software** | |
| **Name** | **Number** | **Name** | **Number** |
| **Drone**  **(Backup)** | 1  2 | **MATLAB UAV Toolbox** | 1 |
| **IoT Nodes** | 30 | **MATLAB Networking Toolbox** | 1 |
| **Communication Modules** | 30 | **MATLAB Simulink** | 1 |
|  |  | **Operating System** | 1 |
|  |  | **Communication Protocols** | 1 |

**Table 5: Hardware and Software Components**

# Reference

* Mekala, M.S. and Viswanathan, P., 2017, August. A Survey: Smart agriculture IoT with cloud computing. In 2017 international conference on microelectronic devices, circuits and systems (ICMDCS) (pp. 1-7). IEEE.
* de Araujo Zanella, A.R., da Silva, E. and Albini, L.C.P., 2020. Security challenges to smart agriculture: Current state, key issues, and future directions. Array, 8, p.100048.
* Kumar, S.A., Vealey, T. and Srivastava, H., 2016, January. Security in internet of things: Challenges, solutions and future directions. In 2016 49th Hawaii International Conference on System Sciences (HICSS) (pp. 5772-5781). IEEE.
* Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H. and Zhao, W., 2017. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE internet of things journal*, *4*(5), pp.1125-1142.
* Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P. and Sikdar, B., 2019. A survey on IoT security: application areas, security threats, and solution architectures. *IEEE Access*, *7*, pp.82721-82743.
* Behjati, M., Mohd Noh, A.B., Alobaidy, H.A., Zulkifley, M.A., Nordin, R. and Abdullah, N.F., 2021. LoRa communications as an enabler for internet of drones towards large-scale livestock monitoring in rural farms. *Sensors*, *21*(15), p.5044.
* Eberhart, R.C. and Shi, Y., 2000, July. Comparing inertia weights and constriction factors in particle swarm optimization. In *Proceedings of the 2000 congress on evolutionary computation. CEC00 (Cat. No. 00TH8512)* (Vol. 1, pp. 84-88). IEEE.
* Zhou, M., Zhou, Z., Liu, L., Huang, J. and Lyu, Z., 2020. Review of vertical take-off and landing fixed-wing UAV and its application prospect in precision agriculture. *International Journal of Precision Agricultural Aviation*, *3*(4).
* Gong, J., Chang, T.H., Shen, C. and Chen, X., 2018. Flight time minimization of UAV for data collection over wireless sensor networks. *IEEE Journal on Selected Areas in Communications*, *36*(9), pp.1942-1954.
* Song, B., Qi, G. and Xu, L., 2019, June. A survey of three-dimensional flight path planning for unmanned aerial vehicle. In *2019 Chinese Control And Decision Conference (CCDC)* (pp. 5010-5015). IEEE.
* Miranda, V. and Fonseca, N., 2002, October. EPSO-evolutionary particle swarm optimization, a new algorithm with applications in power systems. In *IEEE/PES transmission and distribution conference and exhibition* (Vol. 2, pp. 745-750). IEEE.
* Kennedy, J. and Eberhart, R., 1995, November. Particle swarm optimization. In *Proceedings of ICNN'95-international conference on neural networks* (Vol. 4, pp. 1942-1948). ieee.
* Akanda, N.I., Hossain, M.A., Fahad, M.M.I., Rahman, M.N. and Khairunnaher, K., 2022. Cost-effective and user-friendly vehicle tracking system using GPS and GSM technology based on IoT. *Indonesian Journal of Electrical Engineering and Computer Science*, *28*(3), pp.1826-1833., Accessed on 03/04/2024, <https://d1wqtxts1xzle7.cloudfront.net/92710798/16907-libre.pdf?1666198081=&response-content-disposition=inline%3B+filename%3DCost_effective_and_user_friendly_vehicle.pdf&Expires=1712224124&Signature=AdV8YSaRNXfViDGw1l-03rkl4JbgP~GXwdkqaOmJOb5LB9PCDSzjY9gcd~ajqA8Is0zNd3ynBGrStYAiYYS7eYlsAVLV-MvHWs0q8Xso6V0n-FLSxRsNB3OEUcmhCsdJ142yuG1qcp~CnXCAiYJM20iEdEwGdGPPTPVrHiL5H675gS-hMirmolLHXVjMK162TrGNpg-SHAZRYUD54S-a1NbKPD9t5dI7wKJkZHFHX9YNAfFFVy--uYy4xm45Jzh0i75Gu5ibrbbP869xWamh63Y4yIJBSGy-zjV9-jD9hGBnAsqxLOiw0mHO4NeVvLRXi3mPochhvSPdnhdh8vdktg__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA>
* DJI, 2024 Phantom4 ProV2.0, Accessed on 04/04/2024, <https://www.dji.com/au/phantom-4-pro-v2>,
* Fisher J, 2022, Skydio 2+ Adds Antennas, Lowers Price , Accessed on 04/04/2024, <https://au.pcmag.com/drones/91754/skydio-2-adds-antennas-lowers-price#:~:text=The%20Skydio%202%20went%20on,the%20drone's%20original%20asking%20price>.
* Gao, M., Hugenholtz, C.H., Fox, T.A., Kucharczyk, M., Barchyn, T.E. and Nesbit, P.R., 2021. Weather constraints on global drone flyability. *Scientific reports*, *11*(1), p.12092. Accessed on 04/04/2024, <https://www.nature.com/articles/s41598-021-91325-w>