Project Plan For

Preventing Black Hole

Attacks In Manets Using Dynamically

Generated Audit Data

Audience:
Project sponsors, project mentors, unit coordinators and all others in the university and ITC community interested in this project.

Purpose:
The purpose of this document is to clarify the scope, methodology and objectives of this capstone project. The main stakeholders should evaluate the project proposal plan and provide feedback and suggestions that could improve any part of the plan.

Authors	Version	Date
Thi Doan, Alan Gaugler, Tristan Hore, Johnson Sangah	1.0	10 March 2023

Approval by Team Members:

Team Member Name	Student ID
Thi Doan	u3090674
Alan Gaugler	u885853
Tristan Hore	u3218682
Johnson Sangah	u3082492

Table of Contents

1. Introduction and description of the project

Mobile Ad-hoc Networks (MANETs) are decentralised networks consisting of low-power mobile devices (nodes) that can communicate with each other without the need for centralised infrastructure. This makes these networks useful in disaster situations where infrastructure is disrupted or in dynamic environments such as communication between autonomous vehicles. Ad hoc On-Demand Distance Vector (AODV) is a reactive routing protocol commonly used MANETs. However, these networks are inherently vulnerable to various security threats, including Blackhole attacks. In a Blackhole attack, malicious nodes falsely advertise that they have the shortest path to the destination node, causing all traffic to be diverted to the malicious node, which then drops or modifies the packets.

The structure of AODV protocol MANETs presents several technical challenges in securing them from Blackhole attacks. First, MANETs lack centralised authority, making detecting and preventing Blackhole attacks difficult. Second, the dynamic topology of MANETs makes it difficult to maintain trust relationships between nodes, and previously honest nodes can become malicious. Third, nodes in MANETs have limited resources, and any security mechanism implemented should not consume excessive resources. Fourth, MANETs do not have a fixed infrastructure, and nodes rely on each other to relay messages, meaning that any security mechanism implemented should not rely on a fixed infrastructure. Finally, the route discovery process in AODV makes it easy for a malicious node to launch a Blackhole attack by falsely advertising that it has the shortest path to the destination.

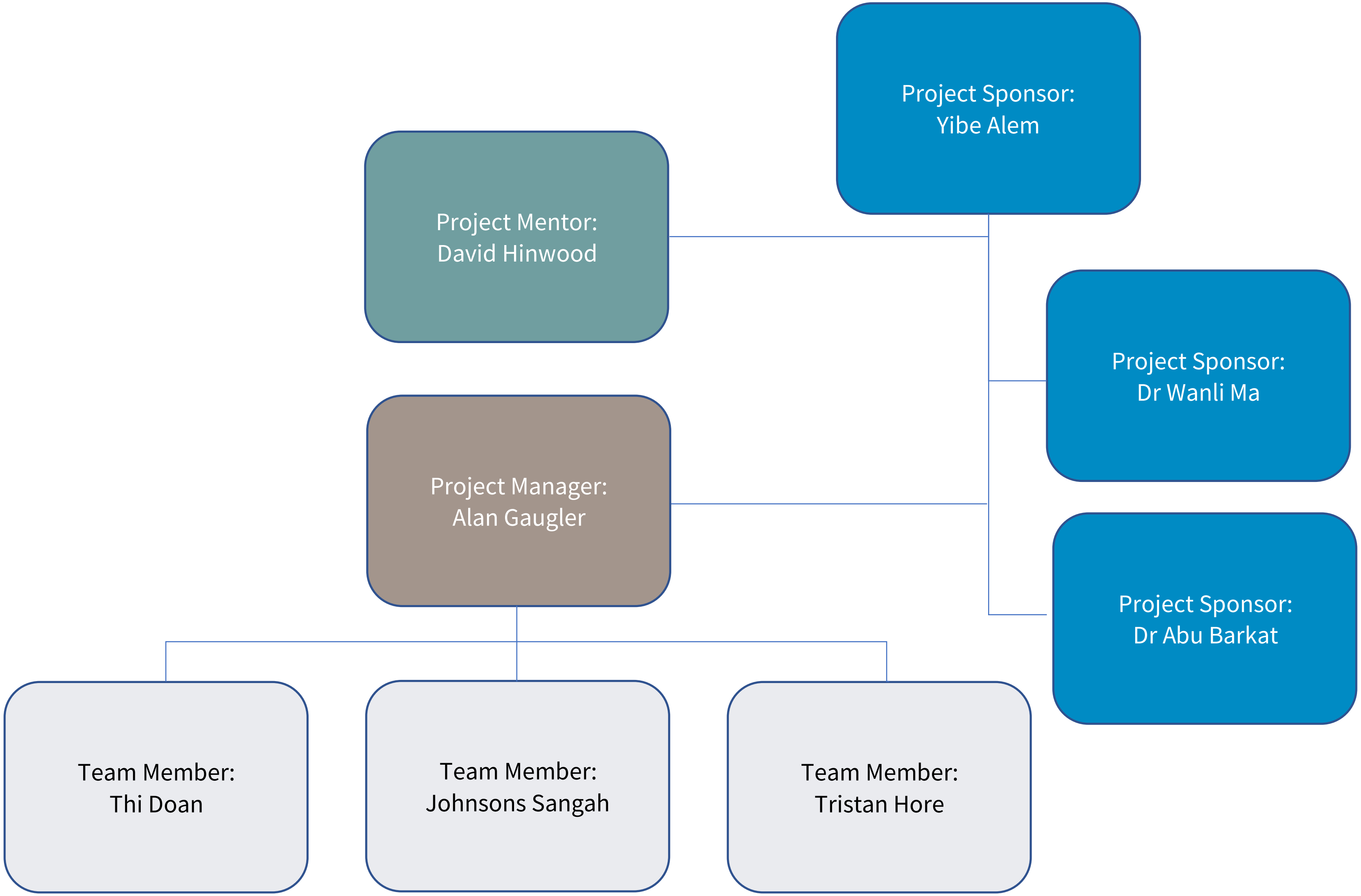
Trust-based mechanisms, secure routing protocols, intrusion detection systems, and game-theory-based approaches have been proposed to address the issue of Blackhole attacks in MANETs. This project will use machine learning (ML) approaches to improve the reliability of the MANET under attack by detecting and isolating the malicious nodes responsible. We will simulate MANETs in the NS-3 network simulator and then capture the network traffic from these simulations. The captured data will be used to produce datasets for training ML models to detect Blackhole attacks and identify malicious nodes. The ML models will be deployed in the simulated nodes in MANET to mitigate the effects of a Blackhole attack. Once the malicious nodes are detected, the nodes will be blocked to prevent further disruption. The effectiveness of the ML models in preventing network performance degradation in the event of a Blackhole attack will be determined. We give details of the proposed approach in the technical description section below.

The project's timeframe is three months. The required software is open-source, and no new hardware is required, making the project's costs minimal. If additional server processing power is required for network simulations, it is anticipated to be met within the $300 project budget.

2. Project Name

Preventing Black Hole attacks in MANETs using Dynamically Generated Audit Data

3. Project Personnel Chart



4. Scope

- To carry out a literature review focusing on mobile ad-hoc networks (MANETs) and their vulnerability to blackhole attacks, to find ways to identify and mitigate them.

- To set up MANET, using network simulator 3 (NS-3) simulations of a black hole attack from malicious nodes to identify and detect which nodes are malicious.

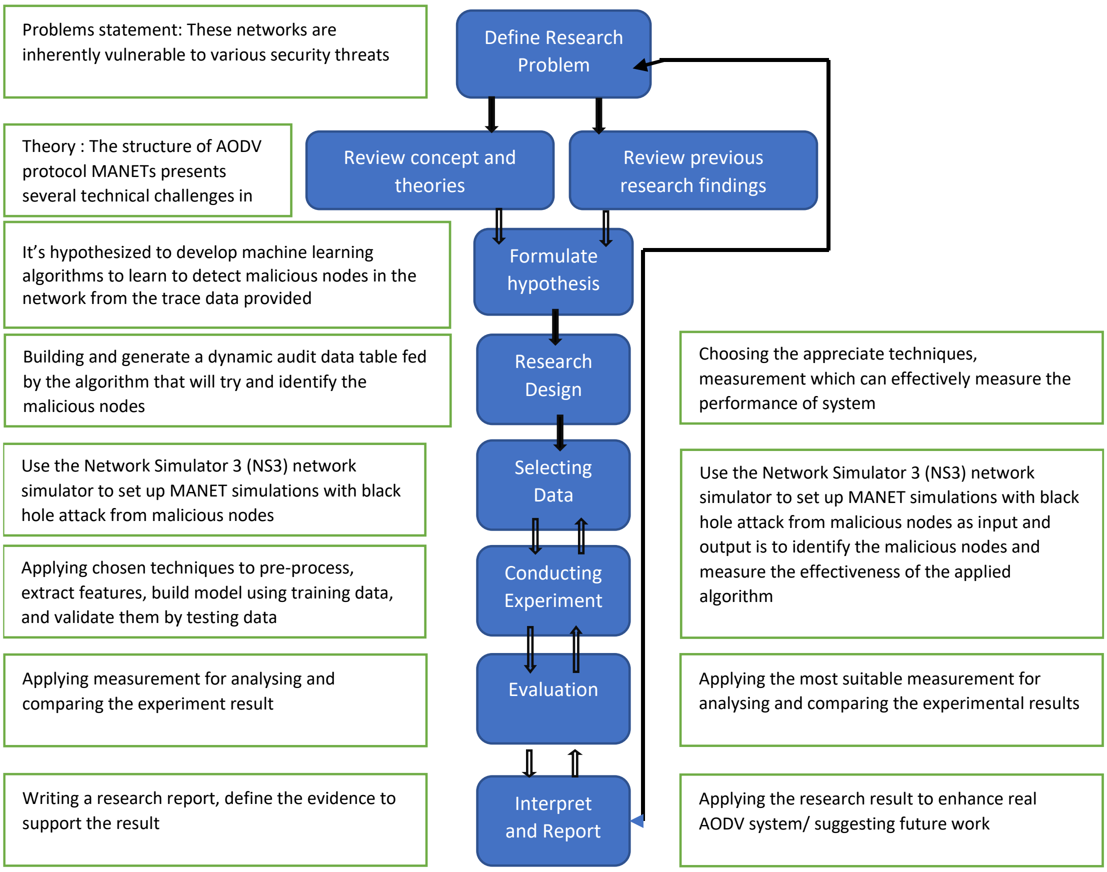
- To generate a dynamic audit data table fed by the algorithm that will try and identify the malicious nodes and measure the effectiveness of the applied algorithm in preventing network performance degradation in the event of a black hole attack.

- To carry out a data analysis of the trace from the simulations to find opportunities to mitigate blackhole attacks and contribute to the growing academic literature in this field.

- Pre-process and prepare the collected simulation data for use in machine learning modelling.

- Develop and evaluate reusable machine learning algorithms that identify, detect and respond to malicious nodes in the network from the trace data provided.

- Produce a final project report and poster on our observations and findings to help contribute to the existing academic literature.



Problems statement: These networks are inherently vulnerable to various security threats

Theory : The structure of AODV protocol MANETs presents several technical challenges in

It's hypothesized to develop machine learning algorithms to learn to detect malicious nodes in the network from the trace data provided

Building and generate a dynamic audit data table fed by the algorithm that will try and identify the malicious nodes

Choosing the appreciate techniques, measurement which can effectively measure the performance of system

Use the Network Simulator 3 (NS3) network simulator to set up MANET simulations with black hole attack from malicious nodes

Use the Network Simulator 3 (NS3) network simulator to set up MANET simulations with black hole attack from malicious nodes as input and output is to identify the malicious nodes and measure the effectiveness of the applied algorithm

Applying chosen techniques to pre-process, extract features, build model using training data, and validate them by testing data

Applying measurement for analysing and comparing the experiment result

Applying the most suitable measurement for analysing and comparing the experimental results

Writing a research report, define the evidence to support the result

Applying the research result to enhance real AODV system/ suggesting future work

4.1. Business Rules

1. All team members will communicate with respect to each other.
2. All team members will remain actively engaged and committed to achieving the set goals and objectives.
3. Any issues and/or risks should be raised with team members at the earliest possible time through the WhatsApp or Microsoft Teams group chat.
4. All team members must follow the project schedule.
5. All project deliverables must meet the defined criteria, quality, and deadlines.
6. The deadline for the final report is 03 May 2023. The deadline for the poster is 05 May 2023.
7. The project's maximum budget is $300.
8. All project expenses must be documented and approved by the project sponsor.
9. Any changes to the project's scope must be documented by the project team and approved by the project sponsor.

4.2. Assumptions

Assumption	Description
1	All team members have many of the necessary skills for this project, the dedication to acquire new skills and the work ethic to make this project a success.
2	All team members have a laptop capable of running most of the software tools required for this project.
3	The project team will have access to cloud servers for ML model training where more powerful processing capability is required.

4.3. Solution Options

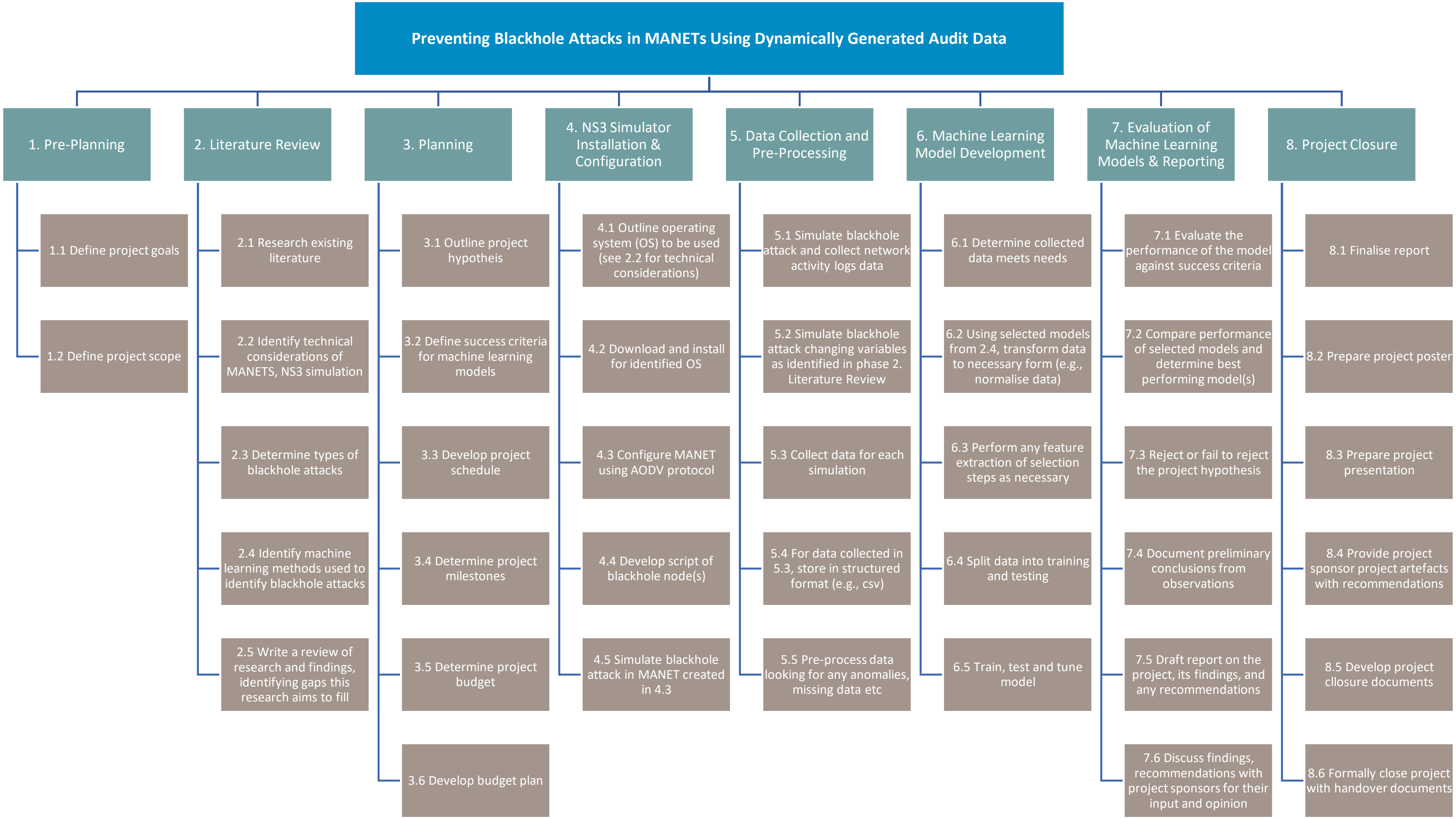
Option 1

As defined in the project scope.

Option 2

In the event of any technical difficulties that will cause the original project scope to change, a change control process has been developed (Section 13), that will be followed throughout the project. In this process, any modification that differs from the original project plan or impacts the project in any capacity will be considered a change. Any proposed changes will be thoroughly documented and require approval from the project sponsors.

Work Breakdown Structure (WBS)



Preventing Blackhole Attacks in MANETs Using Dynamically Generated Audit Data

- 1. Pre-Planning
  - 1.1 Define project goals
  - 1.2 Define project scope
- 2. Literature Review
  - 2.1 Research existing literature
  - 2.2 Identify technical considerations of MANETS, NS3 simulation
  - 2.3 Determine types of blackhole attacks
  - 2.4 Identify machine learning methods used to identify blackhole attacks
  - 2.5 Write a review of research and findings, identifying gaps this research aims to fill
- 3. Planning
  - 3.1 Outline project hypotheis
  - 3.2 Define success criteria for machine learning models
  - 3.3 Develop project schedule
  - 3.4 Determine project milestones
  - 3.5 Determine project budget
  - 3.6 Develop budget plan
- 4. NS3 Simulator Installation & Configuration
  - 4.1 Outline operating system (OS) to be used (see 2.2 for technical considerations)
  - 4.2 Download and install for identified OS
  - 4.3 Configure MANET using AODV protocol
  - 4.4 Develop script of blackhole node(s)
  - 4.5 Simulate blackhole attack in MANET created in 4.3
- 5. Data Collection and Pre-Processing
  - 5.1 Simulate blackhole attack and collect network activity logs data
  - 5.2 Simulate blackhole attack changing variables as identified in phase 2. Literature Review
  - 5.3 Collect data for each simulation
  - 5.4 For data collected in 5.3, store in structured format (e.g., csv)
  - 5.5 Pre-process data looking for any anomalies, missing data etc
- 6. Machine Learning Model Development
  - 6.1 Determine collected data meets needs
  - 6.2 Using selected models from 2.4, transform data to necessary form (e.g., normalise data)
  - 6.3 Perform any feature extraction of selection steps as necessary
  - 6.4 Split data into training and testing
  - 6.5 Train, test and tune model
- 7. Evaluation of Machine Learning Models & Reporting
  - 7.1 Evaluate the performance of the model against success criteria
  - 7.2 Compare performance of selected models and determine best performing model(s)
  - 7.3 Reject or fail to reject the project hypothesis
  - 7.4 Document preliminary conclusions from observations
  - 7.5 Draft report on the project, its findings, and any recommendations
  - 7.6 Discuss findings, recommendations with project sponsors for their input and opinion
- 8. Project Closure
  - 8.1 Finalise report
  - 8.2 Prepare project poster
  - 8.3 Prepare project presentation
  - 8.4 Provide project sponsor project artefacts with recommendations
  - 8.5 Develop project cllosure documents
  - 8.6 Formally close project with handover documents

5. Project Deliverables

- Literature review.
- Project proposal and plan.
- Final Project Report.
- Project Poster.
- Project Presentation.
- Source code for the NS-3 simulations.
- Data traces and datasets produced from the NS-3 simulations.
- Python code for the machine learning process.
- Trained model files.
- Audit data table which identifies malicious nodes.

6. Roles and responsibilities

The project manager holds one of the most crucial roles in guaranteeing a project's success and efficient functioning. They are responsible for ensuring that the project is completed within the given timeline and budgetary constraints while meeting its objectives. This involves managing relationships with all contributors and stakeholders and ensuring that the necessary funding is available.

Alan Gaugler has been appointed as the project manager for our project, and he will be accountable for various responsibilities. These include developing a project plan, managing deliveries in line with the strategy and leading the project team, choosing the appropriate methodology and approving team members, creating a project schedule and identifying each step, assigning tasks to the team members, and interacting with higher authorities.

If the guidance provided by the project manager is suitable for the project, team members will follow it, and they will adopt the correct techniques and processes that benefit the project.

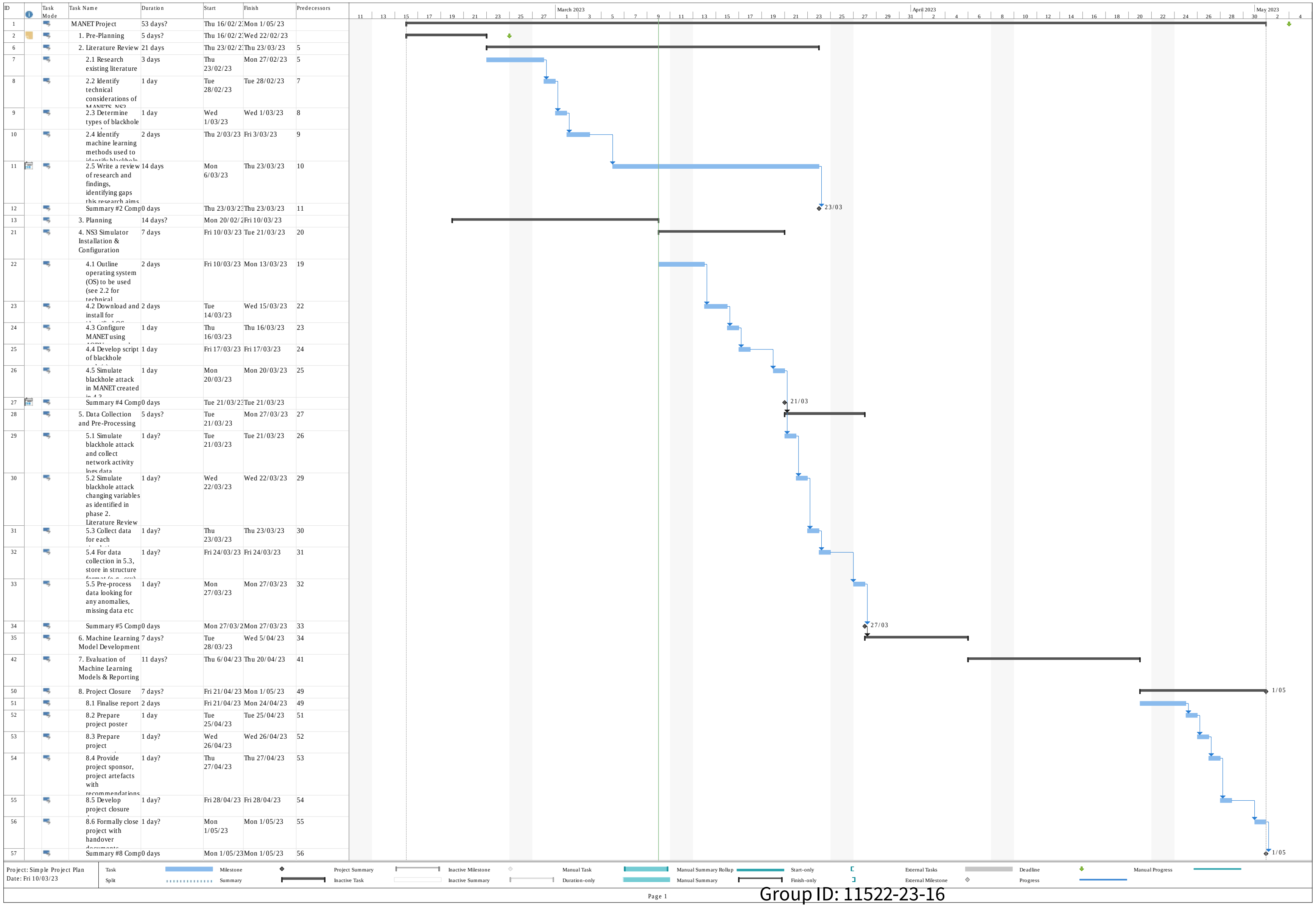
Roles and responsibilities of project team members include contributing to the overall project goals, completing individual allocated tasks, providing expertise, collaborating with users to identify and meet business requirements, and keeping track of the procedure.

The project sponsor and mentor work closely with the project manager to validate the project's goals and participate in high-level project planning. They are also frequently involved in resolving issues and removing impediments that arise throughout the project life cycle. Additionally, they provide sign-off approvals required to advance every stage of the project. Responsibilities of project sponsors include making critical project strategic decisions, approving the project's budget, maintaining the required resources, and disseminating the project's objectives throughout the organisation.

The following governance arrangements have been established by the project team. All four project team members will be involved in all major tasks; however, task leads have been assigned to these teams who will bear the major responsibilities.

Role	Task Lead	Description
Project sponsor	Primary: Dr Yibe Alem	Making critical project strategic decisions. Approval of the project's budget, project's scope. To identify and fix problems or difficulties that are blocking progress and hindering the achievement of goals.
Project mentor	Primary: David Hinwood	Validate that the project's objectives are achievable and consistent with the intended outcome. Participate in the high-level planning of the project.
Research team	Primary: Tristan, Alan	Literature review. The acceptance criteria for each measurement will be established.
Technical team	Primary: Johnsons, Tristan	NS-3 set up and data collection. ML model training validation. Training the selected machine learning algorithms.
Analysis team	Primary: Thi Doan, Johnsons	Responsible for Data cleansing. Exploratory Data Analysis. Visualisation.
Project team	Primary: Alan, Thi Doan	Responsible for the project proposal, final report, project poster and final presentation.

7. Project Milestones



ID		Task Mode	Task Name	Duration	Start	Finish	Predecessors
1			MANET Project	53 days?	Thu 16/02/23	Mon 1/05/23	
2			1. Pre-Planning	5 days?	Thu 16/02/23	Wed 22/02/23	
6			2. Literature Review	21 days	Thu 23/02/23	Thu 23/03/23	5
7			2.1 Research existing literature	3 days	Thu 23/02/23	Mon 27/02/23	5
8			2.2 Identify technical considerations of MANETS, NS3	1 day	Tue 28/02/23	Tue 28/02/23	7
9			2.3 Determine types of blackhole	1 day	Wed 1/03/23	Wed 1/03/23	8
10			2.4 Identify machine learning methods used to identify blackhole	2 days	Thu 2/03/23	Fri 3/03/23	9
11			2.5 Write a review of research and findings, identifying gaps this research aims	14 days	Mon 6/03/23	Thu 23/03/23	10
12			Summary #2 Comp	0 days	Thu 23/03/23	Thu 23/03/23	11
13			3. Planning	14 days?	Mon 20/02/2	Fri 10/03/23	
21			4. NS3 Simulator Installation & Configuration	7 days	Fri 10/03/23	Tue 21/03/23	20
22			4.1 Outline operating system (OS) to be used (see 2.2 for technical	2 days	Fri 10/03/23	Mon 13/03/23	19
23			4.2 Download and install for	2 days	Tue 14/03/23	Wed 15/03/23	22
24			4.3 Configure MANET using	1 day	Thu 16/03/23	Thu 16/03/23	23
25			4.4 Develop script of blackhole	1 day	Fri 17/03/23	Fri 17/03/23	24
26			4.5 Simulate blackhole attack in MANET created	1 day	Mon 20/03/23	Mon 20/03/23	25
27			Summary #4 Comp	0 days	Tue 21/03/23	Tue 21/03/23	
28			5. Data Collection and Pre-Processing	5 days?	Tue 21/03/23	Mon 27/03/23	27
29			5.1 Simulate blackhole attack and collect network activity logs data	1 day?	Tue 21/03/23	Tue 21/03/23	26
30			5.2 Simulate blackhole attack changing variables as identified in phase 2. Literature Review	1 day?	Wed 22/03/23	Wed 22/03/23	29
31			5.3 Collect data for each	1 day?	Thu 23/03/23	Thu 23/03/23	30
32			5.4 For data collection in 5.3, store in structure format (e.g. csv)	1 day?	Fri 24/03/23	Fri 24/03/23	31
33			5.5 Pre-process data looking for any anomalies, missing data etc	1 day?	Mon 27/03/23	Mon 27/03/23	32
34			Summary #5 Comp	0 days	Mon 27/03/2	Mon 27/03/23	33
35			6. Machine Learning Model Development	7 days?	Tue 28/03/23	Wed 5/04/23	34
42			7. Evaluation of Machine Learning Models & Reporting	11 days?	Thu 6/04/23	Thu 20/04/23	41
50			8. Project Closure	7 days?	Fri 21/04/23	Mon 1/05/23	49
51			8.1 Finalise report	2 days	Fri 21/04/23	Mon 24/04/23	49
52			8.2 Prepare project poster	1 day	Tue 25/04/23	Tue 25/04/23	51
53			8.3 Prepare project	1 day?	Wed 26/04/23	Wed 26/04/23	52
54			8.4 Provide project sponsor, project artefacts with recommendations	1 day?	Thu 27/04/23	Thu 27/04/23	53
55			8.5 Develop project closure	1 day?	Fri 28/04/23	Fri 28/04/23	54
56			8.6 Formally close project with handover documents	1 day?	Mon 1/05/23	Mon 1/05/23	55
57			Summary #8 Comp	0 days	Mon 1/05/23	Mon 1/05/23	56

Project: Simple Project Plan
Date: Fri 10/03/23

Page 1

8. Dependencies

The dependencies table displays if the commencement of certain tasks is dependent on completion of any particular earlier tasks. The date the project was assigned to our team is 13 February 2023. The project timeline begins on this date and will end with the final presentation and submission of the poster on 5 May 2023. This results in a total project timeline of 81 days.

Milestone ID	Task	Date	Dependent on Completion of ID	Estimated Duration in Days
0	Preventing Black Hole attacks in MANETs using Dynamically Generated Audit Data.	13 February 2023		81
1	Successful installation of the NS-3 network simulator.	21 March 2023		20
2	Completion of the literature review.	8 March 2023		23
3	Completion & submission of project proposal and plan.	10 March 2023		25
4	Successful NS-3 simulation of black hole attacks in MANETs.	24 March 2023	1	14
5	Completion of development and testing of final machine learning models used for detection of malicious nodes.	14 April 2023	4	21
6	Submission of the project's final report.	3 May 2023	5	19
7	Submission of the project's poster.	5 May 2023	5	21
8	Delivery of the final project presentation.	5 May 2023	5	21

9. Technical Approach

9.1. Technical Assumptions

1. In this investigation, we will not consider the limitations imposed by device processing resources for running the ML Models.
2. This project does not implement any changes to the AODV route discovery process above.
3. All nodes are within a limited area.
4. No nodes move faster than 20ms.
5. The number of black hole nodes is limited.
6. Black holes are not cooperative.
7. RF Transmission effects are neglected.

9.2. Solution Plan

Network Simulation

Data generation

Data will be generated in NS-3 discrete-event network simulator using modified versions of the standard AODV.h and AODV.cc files that allow some nodes to behave as malicious nodes.

Simulations will be run with no Black hole nodes, with black hole nodes and no detection and once models have been trained with no Black hole nodes and detection, with black hole nodes and detection.

Basic simulation parameters (after Mahmood 2007)

#	Parameter	Value
1.	Simulation duration	1000s
2.	Simulation area	1000m x 1000m
3.	Number of mobile nodes	30-100
4.	Number of malicious nodes	0-20%
5.	Transmission range	250m
6.	Maximum bandwidth	2Mbps
7.	Mobility model	Random waypoint
8.	Maximum speed	1-20m/s
9.	Traffic type	CBR(UDP)
10.	Data payload	512,1024 bytes
11.	Packet rate	2 pkt/s
12.	Pause time	10s

Packet data will be captured using NS-3 tools to dump the network trace to PCAP files. We can capture packets at any node in the network. Collecting at all the source and target nodes is the initial goal for our purposes. The PCAP file naming should allow the files to be read into a structured format in a CSV. Simulations will be run on laptop hardware, with outputs saved to the cloud.

Data Cleaning

The CSV files will be converted into a data array for processing in python. The captured packets will be pre-processed in Python to extract relevant features such as packet size, protocol, source IP address, destination IP address, and time stamp. Finally, input and output data arrays will be saved to GitHub in CSV format.

The extracted features will be exported into a structured format in a CSV for the machine learning models to consume. The exact data set structure and pre-processing will depend on the target ML model being trained.

Data cleaning will be run on laptop hardware, with outputs saved to the cloud.

Machine Learning Training

The training approach depends on the type of ML model being trained. First, all the training and testing datasets will be labelled with the true network condition and true malicious nodes. Then, models will be trained against the data with the truth values as targets.

Machine Learning Testing & Scoring

The models will be tested and scored on the true and false detection rate on unseen data in 5 trial conditions, with the averages of the scores taken.

ML model training and validation will be done in the cloud on SageMaker or Google Collabs.

Network Simulation ML testing/scoring

ML models will be deployed to simulation using the NS-3-ai module. ML models run in Python on the same host as the NS-3 simulation, communication to NS-3 is through shared memory.
The models will be compared in NS-3 network simulations with the same starting conditions.
The endpoints evaluated are:

1. packet loss rate
2. data transmission rate
3. routing overhead

Each model will be evaluated against the same 5 network conditions and average performance figures taken.
Network simulation with ML models will be run on laptop hardware.

Documentation plan

1. Each simulation will have a unique numerical identifier.
2. Each simulation starting parameter, including the ML model used (none if none used), will be output to a metadata file.
3. Each simulation PCAP trace will be output to a trace file containing the simulation number in the name.
4. Source code for the AODV.h, AODV.CC and AODV.tcl files will be preserved on GitHub.

5. Model metadata and training sets will be recorded for each trained model.
6. Model training input will be saved on GitHub.
7. Finished trained models used in the project will be saved on GitHub.

10. Management Approach

10.1. Risk Management

To ensure stakeholder satisfaction and minimize any potential risks associated with the project, we have put in place a risk management plan. This plan identifies, evaluates, and controls risks that may affect the project's cost, schedule, and performance. Our risk management approach prioritizes and mitigates potential problems by implementing strategies that address these risks. Examples of such risks include:

Risk	Risk Description	Likelihood	Impact	Mitigation
Personnel Issues	It is possible that any project member could become sick or may have to leave the project due to personal issues.	Moderate	Moderate	All members of the project team will be aware of the tasks of the others and will be able to take over their roles should somebody have to take a leave of absence.
Technical Difficulties	Difficulties with configuring the NS-3 environment and building and running the scripts.	Moderate	Severe	This is a critical part of the project; without it, the project cannot be completed. Significant delays will mean that the project scope will be restructured.
Hardware Requirements	Personal Computers may not possess sufficient processing power.	Low	Low	AWS remote environment will be utilised for the NS-3 simulation.
Software Configuration	Issues with running Python scripts or other required software on personal PCs.	Low	Low	Using online platforms such as Google Colab for the ML training.
Hardware Issues	A PC used on the project may be damaged or stolen.	Moderate	Moderate	1. Files will be checked out of team GitHub. 2. Word documents will be edited on the team’s online file repository. 3. Other files should be stored on the team’s online file repository.

Unforeseen Project Delays	Project delays if there are unresolved issues that impede progress along the way. This could result in additional costs if the project were to be delayed.	Moderate	Severe	The project scope will be clearly defined before beginning and ensure that the entire project can be completed within the designated timeframe. By doing so, we aim to prevent potential delays and minimise any associated additional costs that could arise due to project overruns.
Unrealistic Expectations	Unclear or Unrealistic Expectations can arise when there is a lack of mutual understanding among all parties involved in the project. Unrealistic expectations may lead to unattainable project goals or lower quality standards.	Moderate	Moderate	A careful planning process, including the estimation of costs and time required to complete milestones. Additionally, effective communication will be established to ensure that the entire team has a clear understanding of the project's objectives and expectations.
Not Meeting Deadlines	Missing Deadlines and Deliverables.	Low	Severe	Prioritise tasks by allocating more resources to those that are crucial to the project and giving them the highest priority. Conversely, low-priority tasks will receive fewer resources. Identification of dependencies and completion of tasks synchronously whenever possible. Implementing these measures will ensure that all critical deadlines and deliverables are met on time.
Poor Communication	Poor communication among team members and stakeholders.	Moderate	Severe	Stakeholders will be informed of the most effective communication channels. Team members will meet regularly and provide weekly updates to the project manager on the progress of their assigned tasks. Sponsors will receive regular progress reports. This will ensure that all team members are well-informed and that there is no miscommunication. By implementing this strategy, communication will improve, and this will facilitate a better understanding of the project's progress among all stakeholders.

10.2. Communication Management

What	How	When	Who	Achievement
Introduction and planning	Meeting on Whatsapp. Face-to-face in class.	Bi-weekly	Project team	To evaluate the current progress of the project, discuss, how to proceed, provide solutions and resolve issues.
Team meetings	Meeting on Microsoft Teams. Face-to-face at UC.	Fortnightly	Project team Sponsor team	To deliver fortnightly updates on the progress of the project, including demonstrations, and any clarification needed.
Urgent matters	Email, SMS, Messenger Note. Comments.	Anytime needed	Project team Sponsor team	To resolve or provide alternatives to urgent matters.
Reviews	Meeting on Microsoft Teams. Face to face at UC.	One day before meeting the milestone deadline	Project team	To review updates on the progress of each milestone stage.

1. Communication between all members of the project team and the project sponsors will be regular and consistent. It has been proposed to have meetings on campus every second Thursday between the two groups to seek advice from the sponsor's team and to inform them of the project's progress.
2. Additionally, should any issue or query arise it should be raised promptly with the sponsor's team so that it can be addressed.
3. Meetings among the members of the project team will be held regularly, at least bi-weekly. All relevant documents and files will be shared in MS Teams.

10.3. Quality Assurance

1. NS3 configuration quality control: The NS3 configuration will be subject to quality management to ensure that it accurately represents MANETs and black hole attacks in various network configurations and RF conditions.
2. Simulation Data Quality: The output dataset produced from the NS3 simulation will be verified to ensure that it is accurate, complete and of sufficient size to produce accurate results with the machine learning process.
3. Model Configuration, Testing and Validation: The machine learning models will be tested and validated on independent validation datasets that were not used in the machine learning process. This will verify the accuracy and quality of the models.
4. Software development: Best practices and version control will be implemented.
5. Documentation: All steps in the project will be documented and team members will review all software and scripts to ensure that they are configured and running efficiently and accurately.
6. Peer Review: The project sponsor will receive documentation, software and scripts developed in the project to review and confirm the quality of the methodology, output data and model performance.

10.4. Configuration Management

1. Version control in the script and software development through GitHub.
2. Logical and consistent naming conventions will be used for all documents and output files.
3. Documentation and storage of all final scripts, software, output files and reports on GitHub and cloud drives.

11. CHANGE CONTROL

If a change to the project is required or desired, it is proposed to adopt the following change control process.

Identification and evaluation of a change: If a necessary change to the project has been identified, it will be evaluated to determine what impact could have on the rest of the project.

Requesting the project change: If the proposed change is evaluated as feasible, it will be presented in writing to the project sponsor and mentor for review.

Approval or rejection of the change: The project sponsors and mentors will evaluate and either approve or reject the change.

Implementation of the change: If the project sponsor approves the change, the project manager will update the project plan, scheduling and budget if required. All stakeholders will be informed of the implementation of the plan.

12. KPIs and CSFs

Metric	Excellent Outcome	Good Outcome	Poor Outcome
Deliverables successfully completed	90% to 100%	75% to 90%	< 75%
Individual members meeting attendance	90% to 100%	75% to 90%	< 75%
Sponsor satisfaction	90% to 100%	75% to 90%	< 75%
Budget expenditure	< $300	$300	> $300
Simulation of MANET with black hole attacks	Fully working simulation with a wide range of configurations and useable datasets.	Fully working simulation with useable datasets.	Inaccurate simulations.
Machine Learning Modelling	ML models can accurately detect black hole attacks and malicious nodes, and correctly identify non-malicious nodes.	ML models can accurately detect black hole attacks and malicious nodes.	ML Models are poor at detecting black hole attacks and malicious nodes.
Simulation of MANET networks with ML algorithms implemented	Network measures are better than half those of an unprotected network that is not under attack.	Network measures are better than an unprotected network under attack.	Network measures are close to those of an unprotected network under attack.

13. ISSUES AND PROBLEMS

This section shall be updated as issues and problems are encountered.

These may include:
Data collection: Difficulties to generate and concerns around data accuracy

Technical Issues: Overfitting, underfitting, and lack of generalisation are three technical issues that machine learning models for detecting the nodes

Testing and Quality Assurance: Testing and quality control are essential to ensuring that the system works as intended and satisfies project requirements

Limited Resources: such as computing power and data storage can impact the system's effectiveness, resulting in data processing delays.

14. Sign Off:

COMMENTS………………………………………………………………………

……………………………………………………………………………………

SIGN

_____________________________________ _______________

Client Date