

**Assignment Cover Sheet**

**Designing Human-Computer Interaction, Assignment 3- Semester 1, 2023**

Project Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_Preventing Black Holes in MANETs\_\_\_\_\_\_\_

Project ID: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023-S1-03\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Group ID: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_9785-23-7\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Assignment Topic: \_\_\_\_\_\_\_\_\_Capstone Final Report\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date & Time Submitted: \_\_\_\_25/10/2023 10:00pm\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**I declare that this assignment is solely my own work, except where due acknowledgements are made. I acknowledge that the assessor of this assignment may provide a copy of this assignment to another member of the University, and/or a plagiarism checking service while assessing this assignment. I have read and understood the University policies concerning Student Academic Honesty.**

|  |  |  |
| --- | --- | --- |
| Student ID | Name | Contribution |
| u3201908 | Curtis Richardson | Introduction, Scope and Requirements, Changes from original scope, Professional Documentation, Discussion, Outstanding Issues, Risks Mitigated, Risk Register, Issues Experienced, General Insights, Ethical Issues, Handover Materials, Recommendations to Sponsor, Opportunities for Future Development, Glossary, Annexure A – Risk Matrix; System Administration |
| u3215948 | Daniel Davaris | Introduction, Black Hole Resistant Model, Achievements, Key Results, Resources, Alignment with KPIs, Quality Assurance Measures, Conclusion; Machine Learning |
| u3225675 | Minjeong “Ellie” Kim | Introduction, Impact, Lesson Learned, Resources, General Insights, Ethical Issues, Flow Charts, References, Glossary, Annexure B – AODV Flow Chart Diagram, Annexure C – Black Hole Node Flow Chart Diagram; Research |

Table of Contents

[Introduction 2](#_Toc1582406319)

[Scope and Requirements 3](#_Toc1472120752)

[Changes from original scope 3](#_Toc669456043)

[Project Outcomes 4](#_Toc366891134)

[Deliverables 4](#_Toc265250678)

[Black Hole Resistant Model 4](#_Toc2002794778)

[Professional Documentation 11](#_Toc617837885)

[Achievements 11](#_Toc2110155907)

[Key Results 12](#_Toc513733537)

[Alignment with KPIs 12](#_Toc953168455)

[Discussion 12](#_Toc1144752690)

[Quality Assurance Measures 13](#_Toc1032099222)

[Impact 14](#_Toc1988517396)

[Resources 15](#_Toc644667234)

[Outstanding Issues 16](#_Toc124927826)

[Risks Mitigated 16](#_Toc1582924972)

[Risk Register 16](#_Toc1046917603)

[Issues Experienced 17](#_Toc1481217488)

[Lessons Learned 18](#_Toc738755325)

[General Insights 18](#_Toc390240359)

[Ethical Issues 19](#_Toc1878833272)

[Flow Charts 19](#_Toc243332874)

[Handover Materials 19](#_Toc1112615760)

[Recommendations to Sponsor 20](#_Toc1257197897)

[Opportunities for Future Development 20](#_Toc1309832263)

[Conclusion 21](#_Toc975528836)

[References 21](#_Toc786513721)

[Glossary 22](#_Toc1155039005)

[Annexure A – Risk Matrix 23](#_Toc745945332)

[Annexure B – AODV Flow Chart Diagram 24](#_Toc658067164)

[Annexure C – Black Hole Node Flow Chart Diagram 25](#_Toc1190368758)

# Introduction

As the world becomes increasingly interconnected, devices similarly increasingly are being installed beyond the “edge” of traditional networks – necessitating a local power source, and methods to communicate that recognise energy storage as a resource. AODV (Ad-hoc On-demand Distance Vector) is a communication protocol built for IoT (Internet of Things) and other sensor-based networks that does not require power whenever a communicative action is not taking place. It only activates when there's a need for communication, effectively preserving power when no communicative actions are underway. Unfortunately, while some process improvements have been delivered by the Project Team, the primary goal of implementing a new model has been unsuccessful. However, the Project Team has been able to implement the core functionality required to detected malicious nodes.

In the pursuit of our Project's objectives, our team embarked on a journey of innovation, collaboration, and continuous learning. As we navigated the complex realm of network security, with a specific focus on mitigating Black Hole Nodes in AODV networks, we made significant strides in various domains. These achievements reflect our commitment to excellence and our dedication to delivering a robust solution. Throughout this report, we will explore our key accomplishments, which include the development of Black Hole Node-resistant modelling, the establishment of reproducible environment build instructions, the creation of a real-world dataset through simulation, the provision of clear and comprehensive documentation on AODV and Black Hole Nodes for our Project Sponsor, and meticulous project history documentation through source control workflow tooling, exemplified by our use of GitHub. These accomplishments collectively underline the comprehensive and successful nature of our project's execution.

The Project Team recommends the Project Sponsor initiates another Project to undertake the goal of implementing this mitigation strategy via Machine Learning (ML) modelling – especially now that substantial foundations have been set.

# Scope and Requirements

The Project’s desired deliverables included:

1. A behavioural model that facilitates some mitigation of the “Black Hole Node” vulnerability within AODV networks, which has been output from applying ML to simulated AODV network traffic (including Black Hole nodes)
   1. The model that mitigates BH vulnerabilities is energy efficient enough to be realistically applied to sensor-based networks
2. Professional documentation on the Project Team’s processes and procedures in undertaking the project; inclusive of both items directly relating to Project tasks, as well as items submitted to UC for the Capstone unit assessments
3. Project output must be novel, and contribute to the wider academic community/understanding of the vulnerability mitigations being addressed
4. Any output solution from the Project should be able to be deployed to NS3 software for verification, and improvement

## Changes from original scope

1. GitHub Project utilisation
   1. Early on, Microsoft Teams was selected as the primary document repository (“source of truth”) for the Team’s documentation (due to UC licensing providing current students with Office365 software). However, due to the software-based nature of the project, integrated workflow through GitHub Projects (and GitHub’s Repository functionality) were identified as an appropriate solution to migrate to. Access to the GitHub Project and GitHub Repository <cite repository url> were provided to the Project Sponsor and Project Mentor.
2. Separate Microsoft Azure instance usage
   1. Roughly halfway through the project, an issue with UC-managed Azure instances (VMs, containers, etc.) prevented access to centralised compute resources for the Project Team. In order to maintain centralised collaborative functionality, one member organised a separate instance outside the limitations of UC licencing. While the Project Sponsor acquiesced the measure may be temporarily necessary, they emphasised reimbursement may not be forthcoming, and to try limit usage of the resource to limit personal financial costs to the Project Team.
3. Utilise NS2 for dataset generation and observation
   1. While a majority of the work done to enable a simulation environment for the Project focused on the currently-supported project NS3, the dataset being generated was not able to be integrated into NS3’s graphical tools. Due to familiarity with the NS2 version of the program by the Project Sponsor, the Project Team was able to get a dataset generated, and output via the inbuilt tooling included with NS2. Future advancements in this Project space would benefit from getting NS3 working correctly, due to both: support status of the program (NS2 no longer supported), graphical tooling of NS3 *can* be richer/more comprehensive, and modularity of the program (customisation of NS3 is easier).

# Project Outcomes

## Deliverables

Two primary deliverables were required from the Project: building and implementation of a Black Hole resistant model for AODV-based networks, and documentation (to a professional standard) describing both the intent of the Project and how the Project was undertaken (including clear descriptions of the Problem Domain).

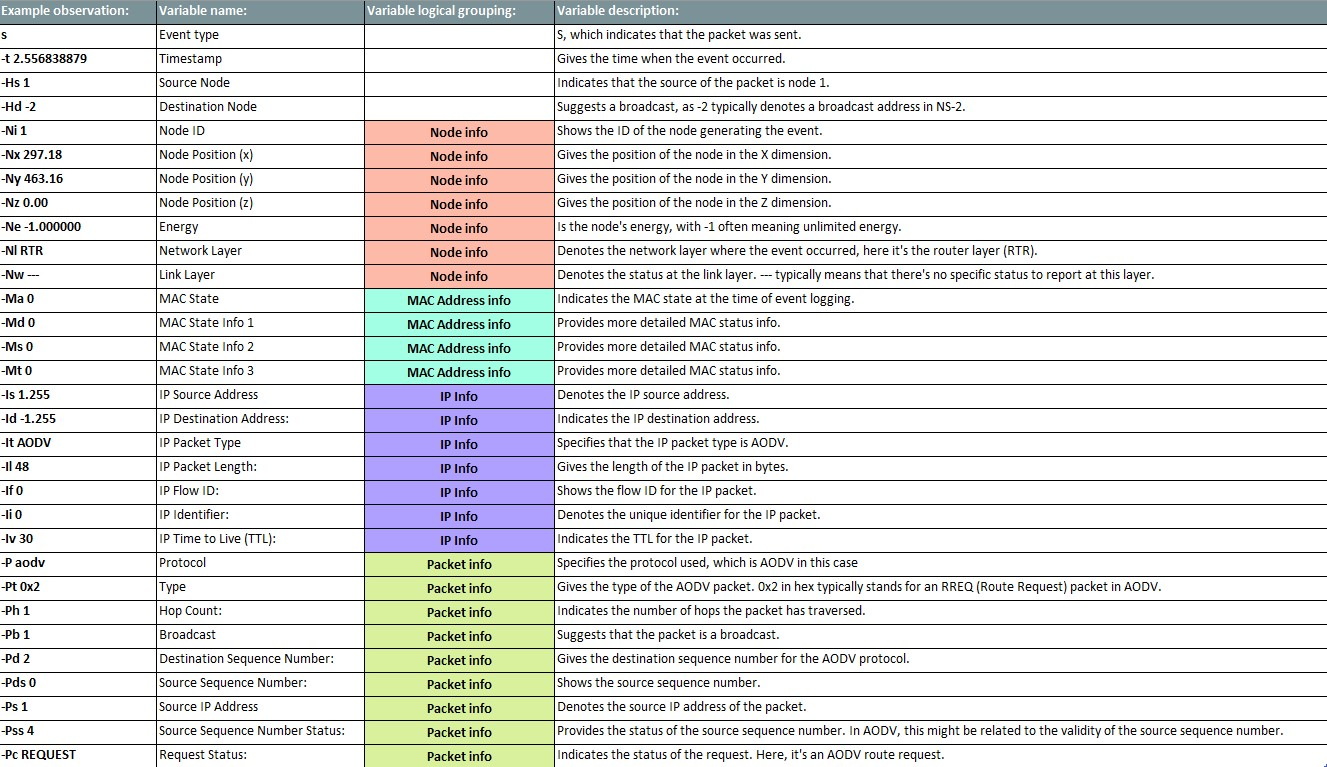
### Black Hole Resistant Model

**Data Ingestion:**

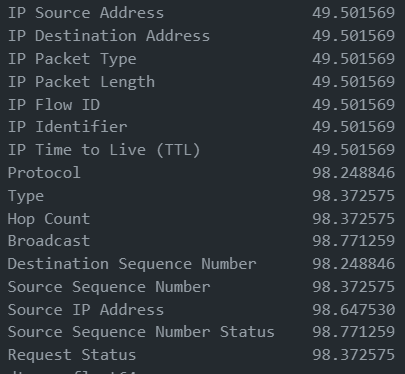
The model is developed through the ingestion of a network trace file generated by the Network Simulator 2 (NS2) open-source software. Three trace files we used, with varying degrees of malicious activity present during the simulation. These trace file contains 17 initial header rows corresponding to the specific simulations network topography. The remaining rows, nearly one million in the initial trace file, correspond to the individual network behaviours between each source and destination node.

The trace files, of the file format ‘.tr’ provide the various trace variables in a single column, which requires manipulation to obtain the variables in their corresponding columns. As the trace files do not contain headings or column names, the next step is to conduct a data understanding process which involves analysing the NS2 source code that produces these trace files and cross-referencing the abbreviations of each observation to derive or at least make an educated guess as to what the columns represents.

**Data Understanding:**

The following data dictionary was created to document and illustrate this data understanding process:  
  


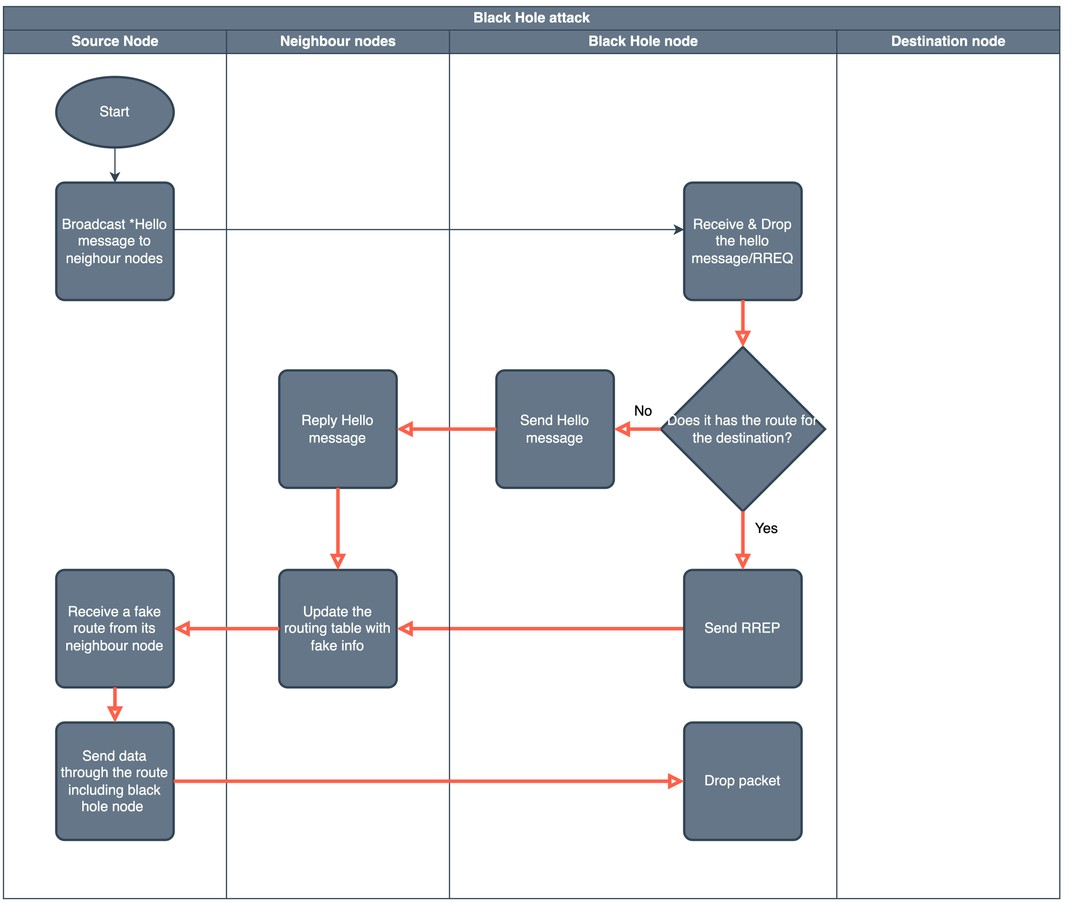
With the variable names known there is now a total of 31 variables which describe the behaviour of 17 unique network nodes. After removing the obvious empty rows, it is noted that many variables contain a vast majority of empty or blank information. Ordinarily, these variables would be discarded, however given the vast volume of data, they are kept for later consideration.

The following extract highlights this observation with each number corresponding to the percentage of missing values.  


**Exploratory Data Analysis (EDA)**

Detecting malicious network nodes, also known as black hole nodes, is the basis of this project. With a comprehensive dataset now established, modelling of the malicious nodes can begin. Black hole nodes falsely advertise themselves as having the shortest route to a destination while dropping all the packets they receive, disrupting the communications in a network. As such, they will exhibit a high reception and no forwarding of packets. This behaviour will be shown through a high number of received packets (event type ‘r’) and a low number of forwarded packets (event type ‘f’). There are many other characterises which also give away a node as being malicious such as a sudden drop in hop count and request status disparity.

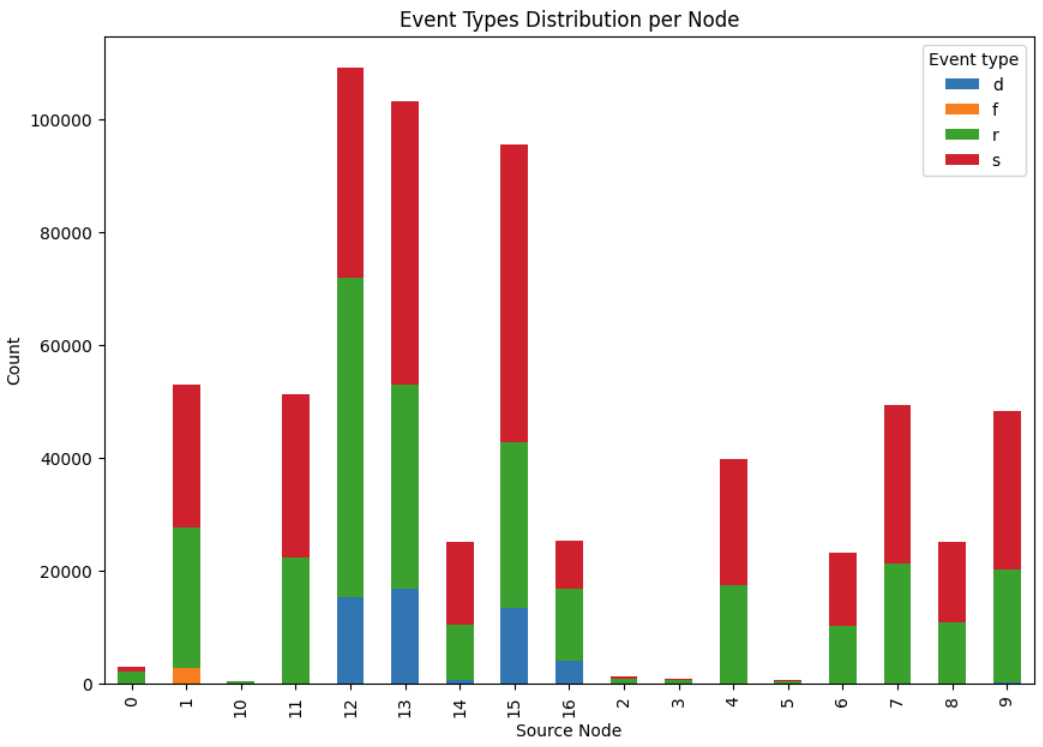
The following figure summarises a malicious nodes behaviour:

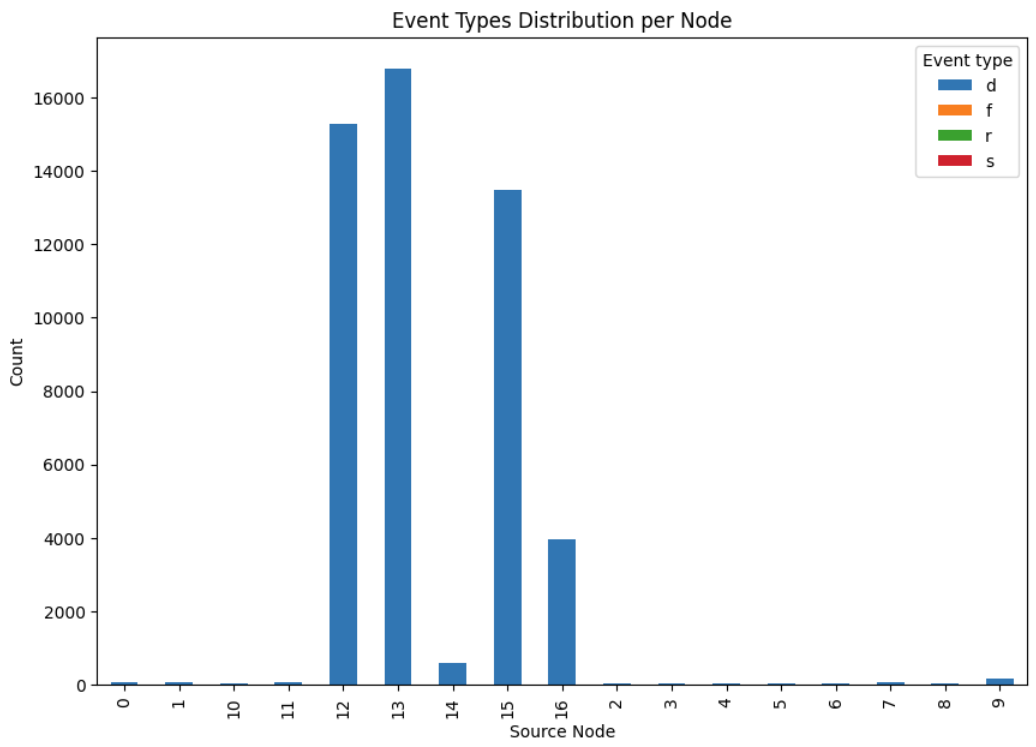
[[1]](#endnote-16628)

(Kaur & Singh 2014; Pandey & Singh 2020; Sbai & Elboukhari 2018) <curtis>

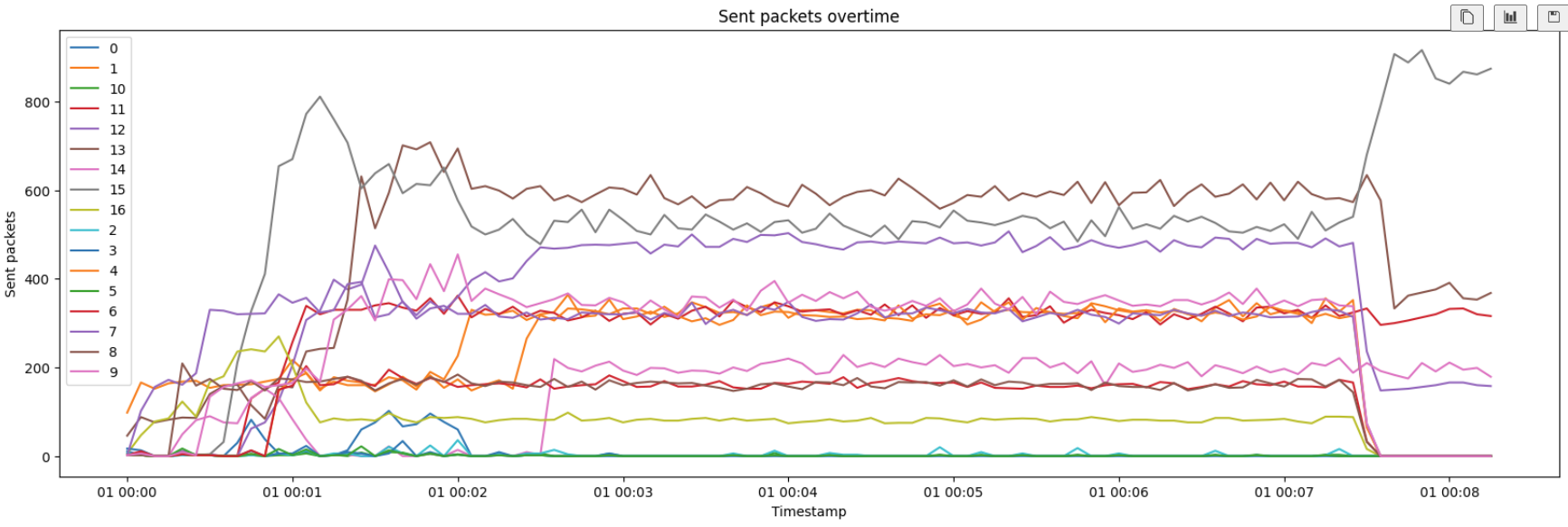
Exploratory data analysis was performed to identify the black hole nodes (BHN). The following graphs establish key insights which will be used by the machine learning model to detect malicious nodes. After performing the EDA, we can conclude that the malicious nodes in the network are nodes 12, 13, 14, 15 and 16.

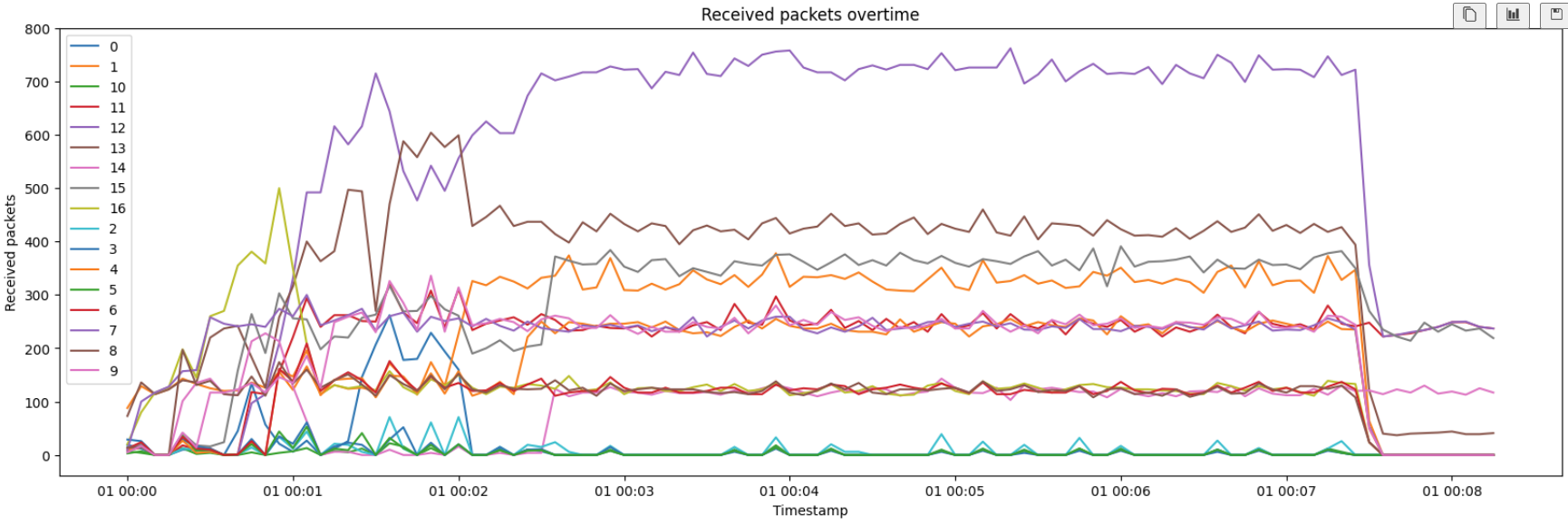
Insight 1) Nodes 12, 13 and 15 show higher activity than normal while nodes 12 to 16 are the only nodes with dropped (d) packets:

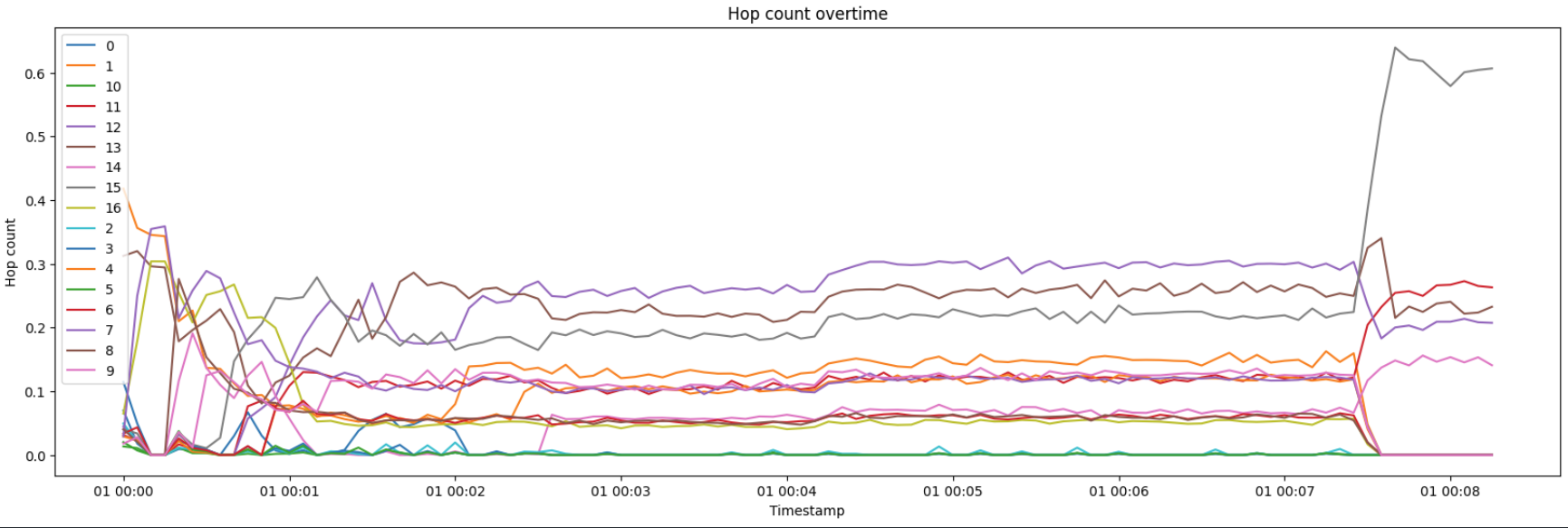




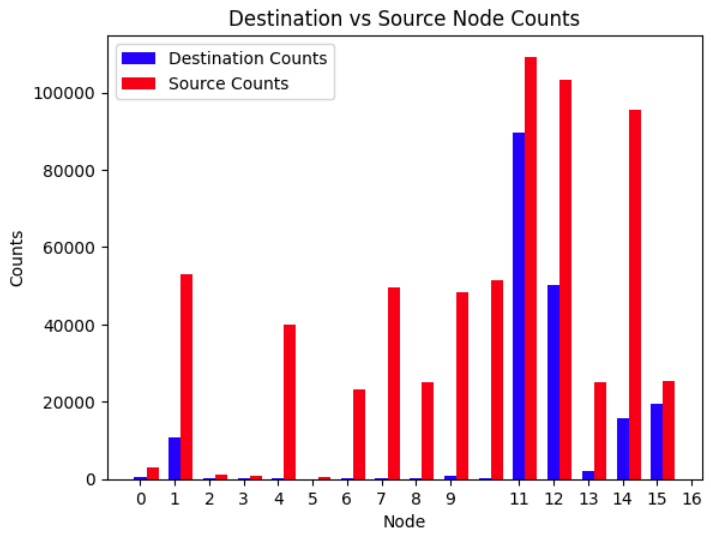
Insight 2) Timeseries exploratory data analysis:



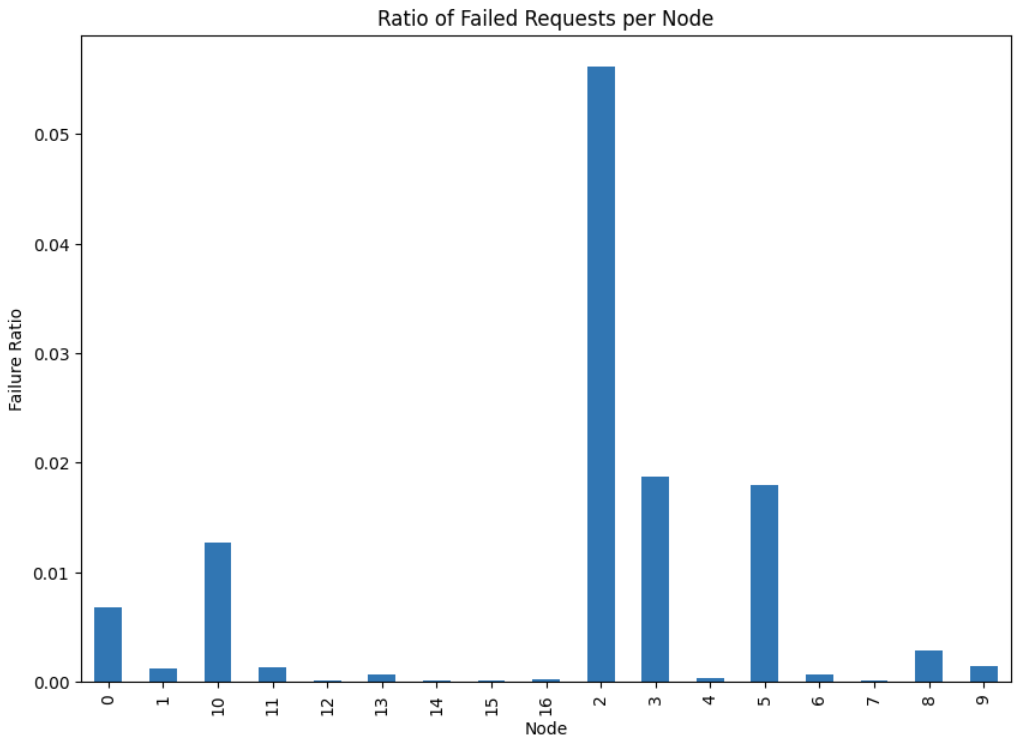




Insight 3) Nodes 12 to 16 are observed to often be the source as well as the destination while other nodes are the source but rarely the destination. This indicates that the BHNs are advertising themselves as the ‘correct’ destination and these packets are not being delivered to the other nodes:



Insight 4) Nodes 12 to 16 also show a very low request failure rate unlike most other nodes:



**Feature Engineering**

The next stage of the data science process is feature engineering, which in this case is imperative. This specific problem cannot be treated in terms of the individual rows. If we look at an individual row in the trace file, no meaningful insight is gained. It is only through analysing the trends for each node and looking at multiple observations for each node that we can then observe the behaviour of a node and make a prediction for whether or not it’s behaviour is malicious and consequently, whether or not it is a black hole node.

In the reality of this problem implementation, we would define a period of time which is enough to collect data to make a good assumption but not too long so that the black hole node can be blocked. Therefore, minimising the amount of data that is lost. Taking action to prevent the BHN from inflicting further damage might be blacklisting a node if its behaviour is deemed to be malicious.

For each variable in the dataset, categorical variables are transposed into various new columns with a count of their values for each category. Numeric variables are then transposed to create additional copies. Finally, the dataset is summarised into ‘sections’, grouped by the source nodes and further grouped into time increments of 15 milliseconds. During this transformation, the previously categorical variables counts are averaged and summary statistics such as min, max, mean, standard deviation and unique count are computed for the numeric variables.

This results into a much smaller dataset. From the 654654 existing observations there are now only 850. With each new observation corresponding to a ‘mini network simulation’. In practice, this process would not occur, and many simulations would be run and summarised to obtain the data points.

**Modelling**

A compressive list of 121 variables was obtained after feature engineering and a target column created with a value of 1 for nodes 12-16 and 0 for other nodes. A correlation matrix was used to find the best features to detect black hole nodes. 80% of the data was used for training and 20% for testing. Finally, a decision tree model (a common type of machine learning algorithm) was implemented to predict black hole nodes.

**Results**

The model achieved an accuracy of 96%, capable of detecting black hole nodes on unseen data 96% of the time. With cross validation implemented, the model's accuracy was found to be 95%. A minimal error rate was also achieved with an f1-score of 97%.

### Professional Documentation

In order to provide the best approach to undertaking this technical Project, we utilised a mix of Agile and PMBOK Project Management frameworks. Agile methodology enabled our team to concurrently work on tasks as we progressed through the unit and keep the Project Sponsor up to date with all ongoing tasks, while the PMBOK methodology provided the structure for documentation, governance and addressing of the assessable pieces required by UC.

As each of the Project Team members had strengths with different aspects of the project (Machine Learning, Research, and System Administration), each took on the role of a Subject Matter Expert (SME) for that area, and worked at educating the other members on what transferrable knowledge was needed. In particular, this led to such descriptive work that can be found in [Annexure B – AODV Flow Chart Diagram](#_Annexure_B_–) and [Annexure C – Black hole Node Flow Chart Diagram](#_Annexure_C_–).

The purpose of the documentation the Project Team has created is to provide both background and technical detail to readers, and for the information to be legible across many different technical knowledge levels.

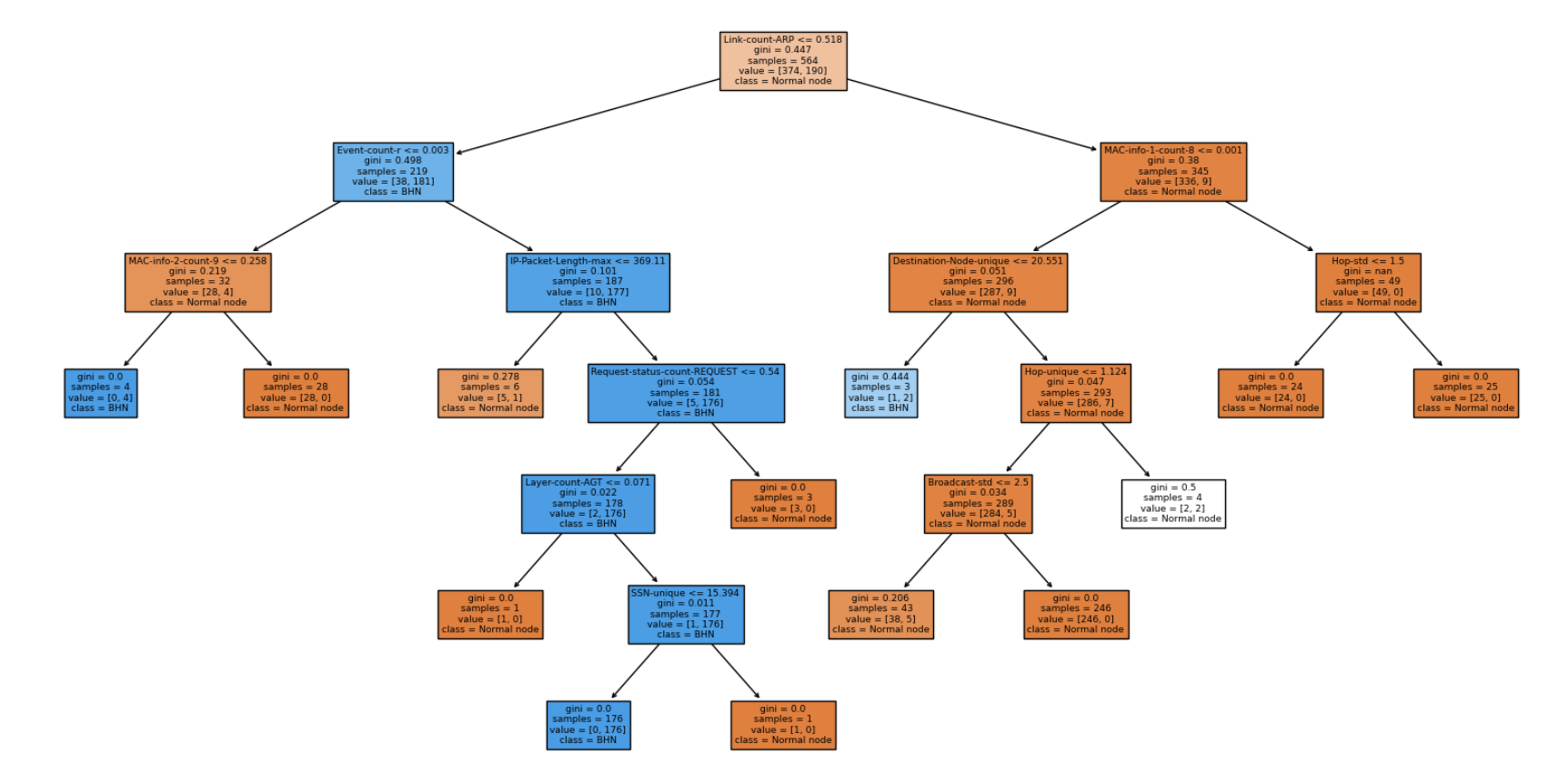
## Achievements

1. Developed highly accurate Black Hole Node resistant modelling for AODV networks
2. Developed reproducible data extract transform load (ETL) scripting
3. Created and evaluated comprehensive list of domain features
4. Reproducable Environment Build Instructions
5. Dataset generated through simulation environment, rather than entirely fabricated
6. Documentation that provides clarity on AODV and Black Hole Nodes presented to Project Sponsor
7. Project history documented through Source Control workflow tooling (GitHub)

## Key Results

1. Highly accurate machine learning model (95% accuracy)
2. Low error rate (< 1%)
3. 100+ features identified

Decision tree machine learning model.



## Alignment with KPIs

|  |  |  |
| --- | --- | --- |
| KPI ID | Key Performance Indicator (KPI) | Rating (Exceeded, Met, Unmet) |
| K1 | Build and deploy a model with an accuracy of at least 80% | Exceeded |
| K2 | Complete the project on time and within the budget | Met |
| K3 | Establish a working model on the NS3 software | Unmet |
| K4 | Address improvements from previous group’s work | Met |
| K5 | Implement a model solution around black hole nodes | Met |
| K6 | Understand the problem domain to be able to critically evaluate the model’s features | Met |

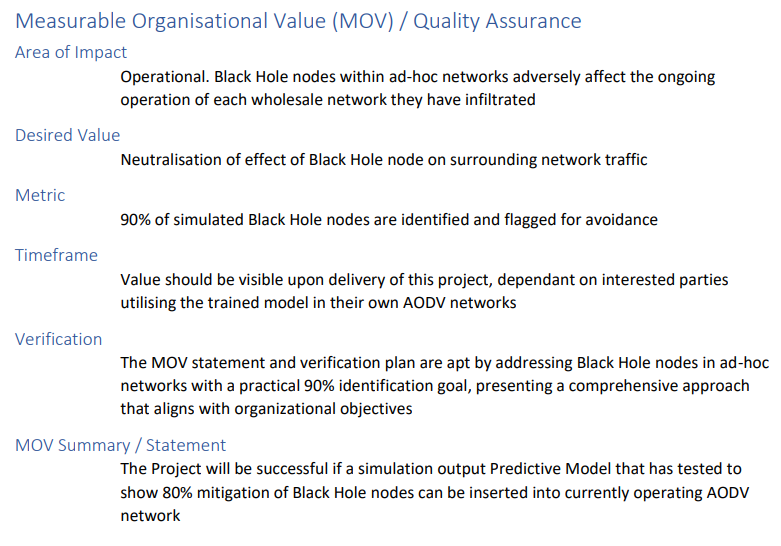
### Discussion

Largely, the implementation of a new model in the project was successful. With some process improvements also delivered – namely, the model has been developed, clearer descriptions of what a Black Hole node is and how they operate have been produced, and a Standard Operating Procedure (SOP) to build NS3 (with Black Hole functionality patched) on an Ubuntu 22.04 server has been developed.

1. K1
   1. A model has been developed, and exceeds the accuracy threshold of the KPI, however the Project Team did not have enough time to successfully deploy the model in either (NS2/3) environment. This KPI is more concerned with the accuracy of the model and is reliant on KPI K5 success.
2. K2
   1. The Project will be closed (under the 2023S2 capstone unit parameters) within budget and time, but without the developed model having been implemented – hence, the rating of “Unmet”.
3. K3
   1. The model the Project Team developed was not able to be successfully deployed through NS3 software.
4. K4
   1. One improvement over the previous group’s work was the use of an actual simulated dataset – however, without implementing the solution in a simulation environment, its comparative effectiveness cannot be measured.
5. K5
   1. While the model was developed, it had not been able to successfully be implemented in a simulated environment.
6. K6
   1. <Understanding of the problem domain has enabled ML procedures to be executed over the simulator-generated dataset to effectively identify Black Hole nodes operating in an AODV network>

## Quality Assurance Measures

The project team was able to implement a model with accuracy greater than 80% which predicts black hole nodes and can be inserted into an AODV simulation. As such the MOV has been met.



## Impact

While not exclusively utilised by owners of sensor-based networks, AODV-based MANETs are almost ubiquitous in situations where the communicating devices/peers are not managed or serviced (I.e., being provided power) by a central system. Such networks can include smart car communications with each other, sensor nodes communicating across a field or farm, and even Satellite-to-Satellite communication. Each of these networks exhibit a common set of attributes:

1. They have their own power source that needs to be maintained (no connection to a generator)
2. The local environment they operate in is always changing (for farms, this may be the climate affecting that farm), so there’s no central controller that can check local peers
3. There’s a possibility that peers can be in remote places / difficult to fix, if anything goes wrong.

With these constraints in mind, the model that our Project is attempting to implement would address the following characteristics:

* Improved Network Security
  + By implementing a model that can (with a reasonable degree) detect or understand the effects of a black hole node, and adapt to that behaviour (I.e. mitigate communication with that peer); communications for the network as a whole will be more secure and trustworthy
* Energy Efficiency
  + Mitigating the wasted communication with a malicious node means the device utilising its own power source isn’t having to repeat actions that consume power for no reason
* Cost Reduction
  + Two strategies could improve the financial aspect: first, with a more trustworthy network of neighbours, fewer peers *could* be procured for a sparser network (placing higher emphasis on trust between peers, than network agility with a greater number of peers); second, less wasted energy use means longer intervals between maintenance/servicing timeframes
* Enhanced Reputation and Trust:
  + With a more secure and efficient network, the organization's reputation is enhanced. This elevated standing translates into increased customer loyalty, making it an attractive choice for new clients and strategic partnerships. The impact on brand perception is invaluable
* Long-term Sustainability
  + In a similar manner to the second Cost Reduction strategy, the less wasted communication with malicious peers means greater reliability and maintenance of that particular network
* Potential for Further Innovation:
  + Beyond its immediate effects, the project opens doors for further innovation. It paves the way for ongoing collaborations and research in the fields of network security and machine learning, driving advancements that can fuel continued success

# Resources

|  |  |  |
| --- | --- | --- |
| Resource | Description | Member – Time (hours) |
| Azure VM (Private) | Centralised IAAS available via personal purchase | Curtis Richardson – 2 hours  Daniel Davaris – 4 hours |
| Azure VM (UC) | Centralised IAAS available via UC licencing | Curtis Richardson – 9 hours  Daniel Davaris – 8 hours  Minjeong Kim – 1 hour |
| Canva | a graphic design platform | Minjeong Kim – 30 hours  Curtis Richardson – 1 hour |
| Draw.io | a graphic design platform for diagram | Minjeong Kim – 10 hours |
| GitHub | Project tracking and git (source control code) repository | Curtis Richardson – 8 hours  Daniel Davaris – 8 hours  Minjeong Kim – 4 hours |
| Google Scholar | Website for literature review | Minjeong Kim – 100 hours |
| Hyper-V | First-party Microsoft hypervisor manager (/platform) to host guest Operating Systems on Windows OS | Curtis Richardson – 150 hours |
| MacOS M1 Ventura 13.5.2 | Apple Operating System for General Computing users | Minjeong Kim – 200 hours |
| Microsoft Office Suite | Document editing tools (word processor, spreadsheet processor, slide editor, etc.) | Curtis Richardson – 50 hours  Daniel Davaris – 50 hours  Minjeong Kim – 40 hours |
| Microsoft Teams | Communications platform enabling both instant messaging, collaborative document editing (via Office365 integration), and document repository | Curtis Richardson – 50 hours  Daniel Davaris – 20 hours  Minjeong Kim – 40 hours |
| ML Algorithms | Development of ML | Daniel Davaris – 75 hours |
| Notion | Web application for note-taking, offering document repository which is able to be shared via generated and hosted URL | Minjeong Kim – 100 hours |
| NS2 and NS3 | Network Simulator software (versions 2.x.y and 3.39.z, respectively) <change versions to exact version numbers> | Curtis Richardson – 70 hours  Daniel Davaris – 70 hours |
| Obsidian | Knowledge Management note-taking application (extensible) using tree-style filesystem of underlying files using generic markdown format | Curtis – 10 hours |
| Ubuntu Server 22.04 | Canonical Operating System, built on Linux, for servers. | Curtis Richardson – 80 hours  Daniel Davaris – 50 hours |
| UC library | Website of UC library | Minjeong Kim-10 hours |
| Windows 10 Pro Education | Microsoft Windows Operating System for users; Pro version enables greater control over OS behaviours (Hyper-V available for all x86\_64 versions of Windows 10); Education edition | Curtis Richardson – 100 hours |
| Windows 11 Pro Education | Microsoft Windows Operating System for users; Pro version enables greater control over OS behaviours and, specifically, enables usage of Hyper-V program; Education edition | Curtis Richardson – 200 hours |
| <ML tools> | \_\_\_ (previous Project Group listed python, matplotlib, etc. - curiously, not Wireshark, which they discuss using in the closure report) | Daniel Davaris – 100 hours |

# Outstanding Issues

The major hurdle yet for the Project Team to overcome is the full implementation of the model in a simulated environment. The model has been output via Machine Learning procedures, but there wasn’t enough time in the Project timeframe to implement within a simulated environment (either NS2 or NS3). For future iterative research (see section Opportunities for Future Development), it would be best to focus on getting the functionality working as desired in the NS3 (NS3.39+) version of the software.

There is currently a planned post-capstone review of the works completed with the Project Sponsor.

# Risks Mitigated

## Risk Register

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Risk | Description | Likelihood | Impact | Mitigation Strategy | Experienced? |
| Delays in NS3 Environment | Delays in having an appropriate environment to test and improve ML modelling | High | Medium | Work on ML models ahead of time and in parallel before NS3 is finalised | Yes |
| Existing ML Model Inaccuracy | Inaccuracy of existing models on live dataset and delays to redevelop models | Low | High | Develop good understanding of literature to be able to develop new successful models | Yes |
| Complexity of Deploying ML Models | Increased complexity in deploying models on NS3 | Medium | Medium | Switch to ETL development | Yes |
| Complexity of Creating ML Models | Increased complexity in creating new ML models | Medium | Medium | Simplify models to achieve a timelier outcome | Yes |
| Illness | Project member becomes ill, and completing tasks becomes difficult | Medium | Low | Group members maintain socially acceptable level of hygiene and cleanliness | No |
| Team Breakdown | Member wants to exit group/team | Low | High | Group members commit to providing advanced notice to rest of team and Project Governance team of any desired movements | No |
| Team Conflict | Members argue with each other, and collaboration becomes difficult | Low | Medium | Group members commit to articulate ideas and feelings in a respectful manner | No |
| Simulation Error | Simulation has errors with (for example) code, algorithm, data set, etc. | High | High | Reproduce executed simulations to produce averaged dataset | No |
| Project Similarity | The degree of resemblance between the current project and the past project | Medium | High | Team conducts comprehensive analysis to discover the unique aspects of the current project and involves stakeholders for the project’s direction | No |
| Inadequate Planning | Lack of planning in the project and to the delivery of the network model and how it will function | Low | High | Develop clear project documentation and planning early and check back in regularly | No |
| Poor Scope Management | Lack of control over the scope and size of the project, as opposed to the defined set of requirements | Medium | High | Established MVP and set the requirements early on, checking back to confirm the original scope | Yes |
| Undefined Roles and Responsibilities | Lack of clarity around defined roles and tasks required for each team member | Low | High | Setup and adhere to regular communication cadence; a “role and responsibilities” document containing definitions | No |
| Ineffective Communication | Lack of effective communication practices to coordinate project objectives | Medium | High | Establish team communication channel, cadence and technology early; be disciplined in the approach to regular communication with structured meetings | No |
| Inadequate Management | Insufficient project management and coordination techniques and procedures | Low | Medium | Establish formal project governance and processes; implement PMBOK practices | No |
| Insufficient Resource Allocation | Inadequate level of resources to complete project | Low | Low | Present business case early and plan project around outcomes | Yes |

## Issues Experienced

1. Delays in NS3 Environment Establishment
   1. Getting a full understanding of the NS3 software stack structure took longer than anticipated, and all available patches to enable the default program to understand the logic of Black Hole nodes in AODV networks were incompatible with the versions available. The workaround for applying the NS3.25 patches to NS3.39 (since package changes meant installation of NS3.25 was no longer an option) was to manually parse the patch changes and implement the feature updates against the updated NS3.39 structure.
2. Existing ML Model Accuracy
   1. As the previous Project Team’s dataset was entirely fabricated (not generated through a simulated environment), the validity of their calculations was unable to be completely trusted. Mitigating this issue was completed via fully understanding the Team’s intent, and investigating more ways to try get a trustworthy/simulation-sourced dataset.
3. Poor Scope Management
   1. An initial understanding of the project was that the body of work the Project Team would be working from was already set – in reality, the method of implementation from the previous Project Team could be solely used as inspiration, rather than a mandated direction. Confusion was cleared up after a meeting with the Project Sponsor during week 8.
4. Insufficient Resource Allocation
   1. During the capstone semester, the centralised compute capability (an Azure cloud VM instance) was unable to be accessed by the Project Team. As the team had already set up a remote code repository in GitHub, mitigation strategies were able to be flexible: personal devices were used to host guest OS’s, and one member procured an Azure VM instance outside of the UC licencing limitations to ensure access wouldn’t be affected by any UC action, while ensuring an always-online compute capability was available.

# Lessons Learned

## General Insights

1. Understanding MANETs:
   1. The project provided an opportunity to delve into the complex world of MANETs. Through research and hands-on experience, I learned the intricacies of MANETs, their vulnerabilities, and the importance of securing these dynamic and self-configuring networks. Understanding the foundation was crucial for the success of the project.
2. Continuous Learning and Research:
   1. One of the key lessons was the necessity of continuous learning and staying updated with the latest developments in the field of network security. Research and exploration of emerging technologies were crucial in developing innovative solutions to prevent black hole attacks.
3. The Power of Project Management:
   1. Effective project management played a significant role in keeping the project on track. Timelines, milestones, and clear objectives helped ensure that everyone was on the same page. This project highlighted the importance of setting clear goals and monitoring progress.
4. Continuous Learning and Research:
   1. One of the key lessons was the necessity of continuous learning and staying updated with the latest developments in the field of network security. Research and exploration of emerging technologies were crucial in developing innovative solutions to prevent black hole attacks.
5. Documentation and Knowledge Sharing:
   1. Proper documentation was essential for ensuring knowledge sharing within the team. Documenting our progress, decisions, and solutions facilitated continuity and made it easier for team members to step in when needed.
6. Belief and Trust in the Team:
   1. The project underscored the importance of trust and belief within a team. Each team member's confidence in the skills and contributions of others was pivotal in ensuring a harmonious work environment. It instilled a sense of unity and a shared vision, which translated into better productivity and creativity.
7. Understanding Black Hole Nodes and MITM Attacks in AODV:
   1. The project deepened our understanding of specific network threats, such as Black Hole Nodes and Man-in-the-Middle (MITM) attacks in the context of the Ad-hoc On-Demand Distance Vector (AODV) routing protocol. Learning to identify and counteract these malicious behaviours was an essential aspect of the project. It emphasized the significance of recognizing attack vectors that are unique to mobile ad hoc networks and the need for tailored security measures to safeguard against them. This knowledge can be valuable not only for the current project but also for addressing similar challenges in the future.
8. Adapting to resourcing issues
   1. To enable centralised always-online access to compute resourcing, the Project Sponsor organised an Azure VM instance (under UC licencing arrangement) to be available to the Project Team during the capstone unit. A big positive of this is that it was seen as an operational expense for UC to enable research, and so didn’t touch the Project budget allocated to each capstone team. An issue occurred during the semester that locked out access to any device not on the internal ring of the UC VPN, preventing access to the resource for the Project Team. The team adapted fairly and quickly, with one member purchasing an instance for the group to continue working (which gave that particular member great insight into the procurement process for cloud infrastructure). We believe that as UC’s utilisation of cloud infrastructure in their curriculum matures, an equivalent drop in ACL (or similar) issues would eventuate.

## Ethical Issues

1. Motivation
   1. Limitations to motivation for either the Project work, or capstone unit assessment items was a challenge for students nearing the end of their multi-year degrees. The clash of a desire to complete the Project goal (which often required focused technical attention) against the effort to complete assessment items that, in and of themselves, do not contribute to a successful outcome of the goal. It’s difficult to imagine a way in which Motivation due to the capstone assessment items could improve without significant changes to how the capstone unit is structured. We found that utilising individual group member’s strengths for certain tasks (both Project and capstone), having some informal time during team meetings (catching up about our lives), and keeping imminent graduation in mind, were the keys to successfully staying motivated during the semester (with all involved tasks).
2. Academic Pressure
   1. In the same circumstance as the ‘Motivation’ issue, students may have felt pressured to prioritise assessment items, which often come with strict deadlines and grading criteria. This academic pressure can inadvertently diminish their enthusiasm and creative energy for project work, potentially hindering the project's overall quality and outcomes.

## Flow Charts

To fully understand the technical elements of the Project, one member had built flow chart diagrams to explain the concepts of the AODV protocol (see [Annexure B – AODV Flow Chart Diagram](#_Annexure_B_–)) and Black Hole nodes (see [Annuexure C – Black Hole Node Flow Chart Diagram](#_Annexure_C_–)).

# Handover Materials

|  |  |  |
| --- | --- | --- |
| Item ID | Material Name | Description |
| H1 | Meeting Minutes | Documents detailing the contents of meetings members facilitated – especially, earlier in the semester |
| H2 | Source Control Access | Project Sponsor GitHub credentials added as contributor to the GitHub Project and GitHub Repository used for source control workflow for the capstone project |
| H3 | Project Proposal | Second capstone unit (2023S2) assignment – containing expected direction of the project |
| H4 | NS3 Reproducible Build Instructions / Run Sheet | Document detailing the commands required to get an NS3 environment configured for operation (including with generic logic to understand Black Hole nodes in AODV networks) - though further refinements could (or should) be made, per [Opportunities for Future Development](#_Opportunities_for_Future) |
| H5 | Model derived from ML | Python Jupyter notebook file |
| H6 | Final Report | Third capstone unit (2023S2) assignment – concerning project delivery (status and detail), history, and recommendations for future work and/or study |

# Recommendations to Sponsor

This was the second semester for this Project to be offered and undertaken, with each successive semester getting closer to the goal of implementing a model that can help nodes within AODV-based networks to detect and mitigate communication with malicious nodes, specifically Black Hole nodes.

This semester saw the major step of a model being created via a dataset sourced from a simulation (NS2), rather than entirely fabricated. Additionally, documentation providing clear descriptions of all the elements involved with the Problem Domain (MANETs, AODV, Black Hole nodes, etc.) and how to get NS3 operational on a modern Linux OS.

The implementation of the Project’s goal is incredibly close. While some aspects were handled with NS2 simulation environment this semester, if a future iteration of the Project were to emphasise movement to NS3 (using the groundwork covered by this Project Team) - especially given NS3’s more modularised (and supported) structure, academic and industry contributions would be further improved.

We recommend the Project Sponsor backs another Project to tackle the goal of implementing this mitigation strategy via ML modelling – especially now that substantial foundations have been set.

# Opportunities for Future Development

1. Full utilisation of NS3 program
   1. Having a single, current (up-to-date and supported) simulation platform to build from is ideal. NS3’s modular structure facilitates a cleaner structure to customisations made to the software stack and would make transportability of the necessary files that much easier for collaborative (or reproducible) experimentation.
2. Refinements to energy usage modelling in NS3 program
   1. Support for Energy consumption modelling has existed since NS2, but improvements were made during the lifecycle of NS3 to the point that for fine-tuning of energy consumption and tracking, NS3 is the preferred platform, over NS2.
3. Refinement of features exhibited by Black Hole Nodes
   1. Currently, most research investigates Black Hole nodes as a Denial of Service (DoS) malicious node, but with increasing uptake of devices that communicate over a network with protocols such as AODV, the risk of more sophisticated adversary actors wanting to consume that information themselves (exfiltration), rather than just drop it (tradition DoS) may also increase.
4. Higher complexity for Black Hole Node decision-making (“smarter/more intelligent” malicious nodes)
   1. The behavioural characteristics of the Black Hole node in our simulations (and often in wider research) is fairly simple – the node rarely modules its behaviour to get around detection models, or uses its own logic to target specific nodes. Future research that implements a more sophisticated logic structure to the Black Hole node would further improve modelling and strategies to mitigate even more complex malicious entities.
5. Real-world network capture (and experimentation/implementation)
   1. When full implementation within a simulated environment is achieved, experimentation with actual networks would be beneficial both to verify the model, but also to verify the accuracy of the simulation software itself – which may assist in improving the simulation platform as a product, and thereby benefit future iterative research.

# Conclusion

Overall, the project was a success, with a machine learning model developed to confidently detect malicious nodes. There were many challenges to overcome through the project, namely the configuration of the network simulation software and the data engineering required to train a machine learning model. Many future enhancements have been identified to create more Indepth features, deploy the model and assess the energy efficiency of the solution. Holistically, the core project objective has been delivered and a leap forward archived from the previous project implementation.

# References

**There are no sources in the current document.**

Kaur, R. and Singh, P., 2014, “Review of black hole and grey hole attack”. *The International Journal of Multimedia & Its Applications*, *6*(6), p.35.

Kumar, Ankit, Vijayakumar, V, Kumar, Abhishek, Dadheech, P, Choudhary, SS, Kumar, V, Panigrahi, BK & Veluvolu, KC 2021, “Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm,” *Microprocessors and Microsystems*, 80103352, <https://doi.org/10.1016/j.micpro.2020.103352>.

Pandey, S & Singh, VB 2020, “Blackhole attack detection using Machine Learning approach on MANET,” *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*, <https://doi.org/10.1109/icesc48915.2020.9155770>.

Rollins, S 2008, *Routing/AODV*, August 25, 2023, <https://www.cs.usfca.edu/~srollins/courses/cs686-f08/web/notes/routing.html>.

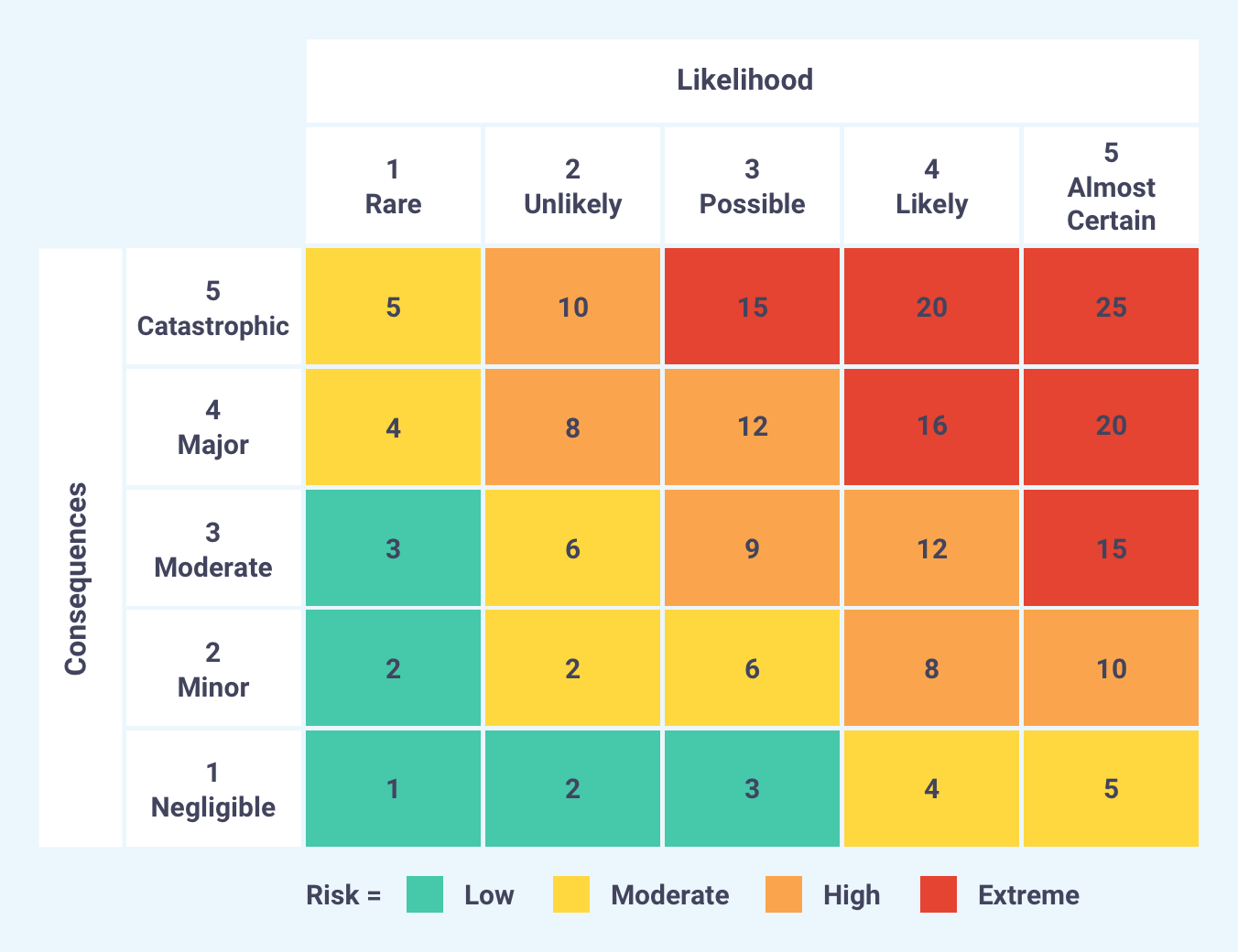
Safran Software Solutions, 2019. “What’s the Difference Between Qualitative and Quantitative Risk Analysis”. [Online]  
Available at: <https://www.safran.com/blog/whats-the-difference-between-qualitative-and-quantitative-risk-analysis>[Accessed 1 September 2023].

Sbai, O & Elboukhari, M 2018, “Simulation of MANET’s Single and Multiple Blackhole Attack with NS-3,” *2018 IEEE 5th International Congress on Information Science and Technology (CiSt)*, <https://doi.org/10.1109/cist.2018.8596606>.

# Glossary

|  |  |
| --- | --- |
| Acronym / Term | Definition |
| AI | Artificial Intelligence |
| AODV | Ad-hoc On-demand Distance Vector |
| CSF | Critical Success Factor |
| DoS | Denial of Service |
| ETL | <Daniel – please advise> |
| IoT | Internet of Things |
| KPI | Key Performance Indicator |
| MANET | Mobile Ad-hoc NETwork |
| MITM | Man-In-The-Middle |
| ML | Machine Learning |
| MVP | Minimum Viable Product |
| NS | Network Simulator |
| SME | Subject Matter Expert |
| SOP | Standard Operating Procedure |
| UC | University of Canberra |

# Annexure A – Risk Matrix

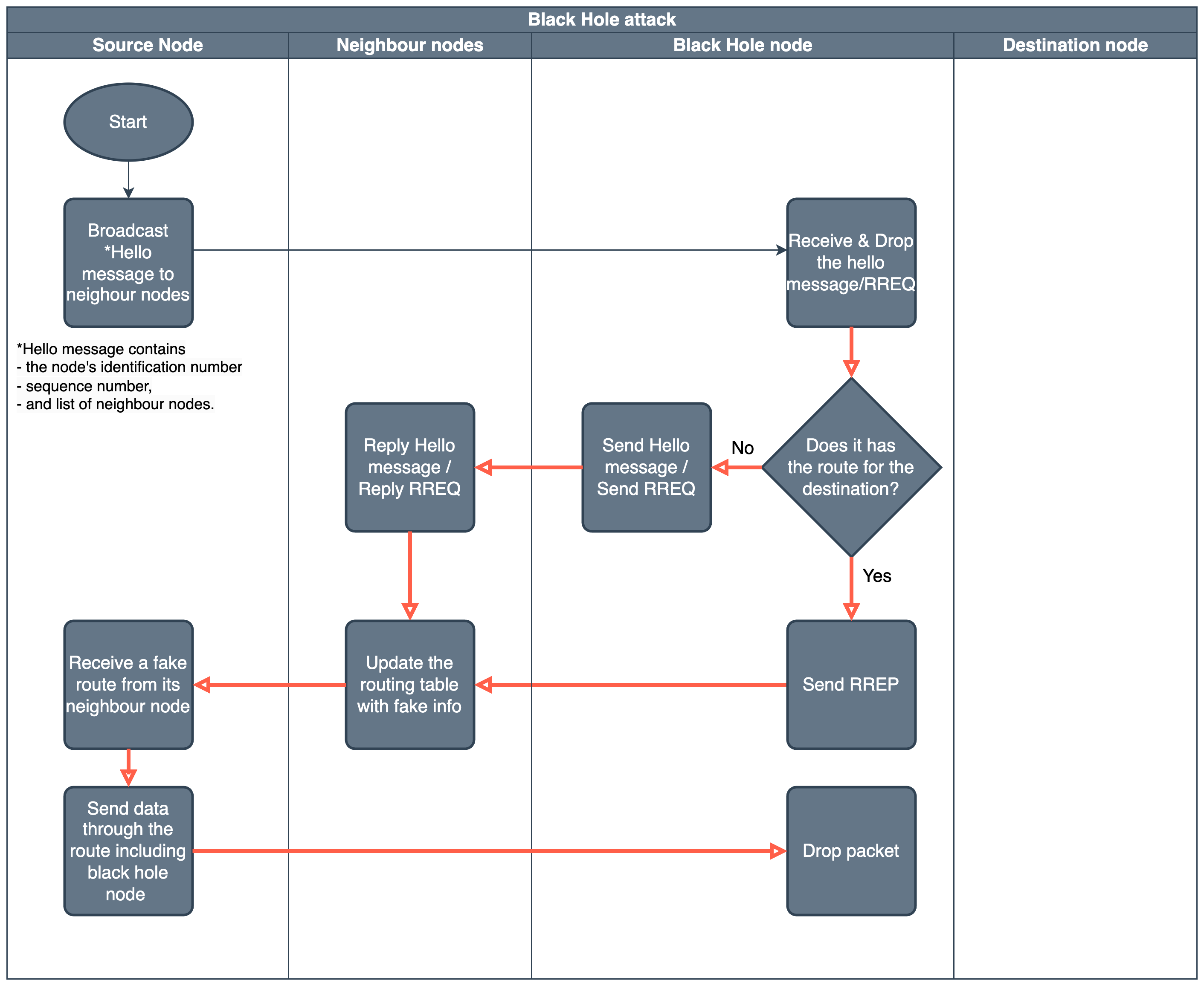
  
(Safran Software Solutions, 2019) <curtis>

# Annexure B – AODV Flow Chart Diagram

# 

(Rollins 2008; Kumar et al. 2021) <curtis>

# Annexure C – Black Hole Node Flow Chart Diagram



(Kaur & Singh 2014; Pandey & Singh 2020; Sbai & Elboukhari 2018) <curtis>

1. [↑](#endnote-ref-16628)