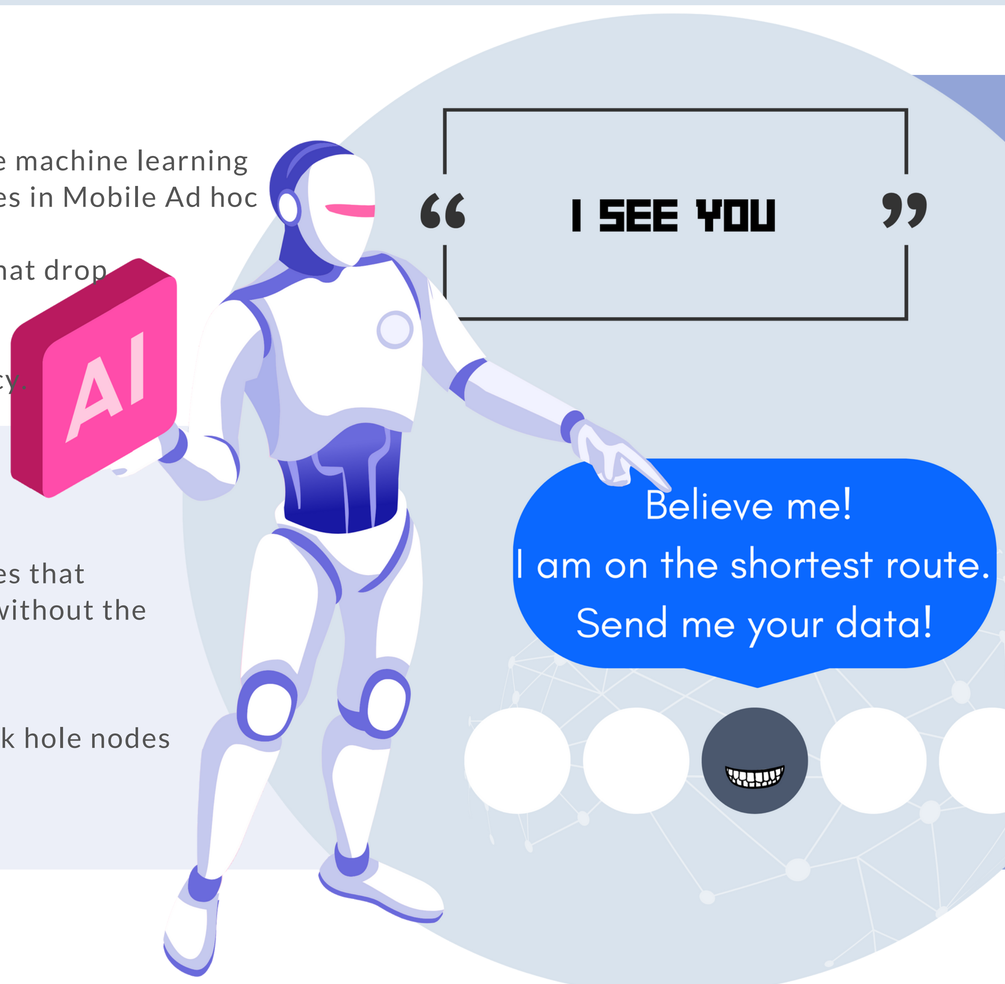
Preventing Black Holes in MANETs Using Machine Learning

9785-23-7

Executive Summary

Group 9875-23-07 won a project to use machine learning to identify and mitigate black hole nodes in Mobile Ad hoc NETworks (MANETs).
Black hole nodes are malicious nodes that drop traffic instead of forwarding it.
The project aims to improve network security, accuracy, and energy efficiency.



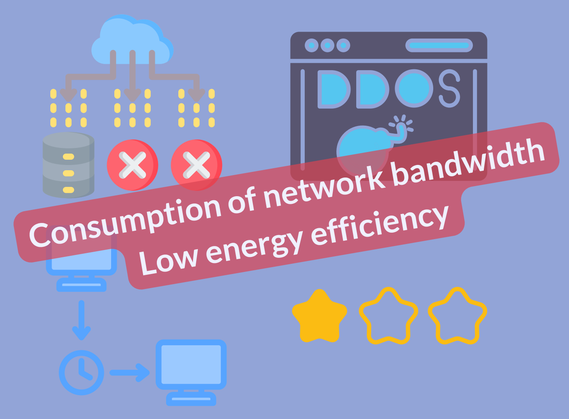
Introduction

MANET:
Decentralised network of mobile devices that communicate directly with each other without the need for a fixed infrastructure.

Machine Learning:
Identify and mitigate the effects of black hole nodes on surrounding legitimate nodes.

Black hole node:
- Deceive its neighbour nodes as if is on the fast route to destination
- Drop the packets instead of forwarding them

Side effect:



Stakeholders

- Smart Cars
- IoT Appliances and Applications
- Inter-space / inter-satellite comms
- Connected Infrastructure
- Smart Cities
- Connected Farms

Material/Methods

- NS-2 and NS-3 (Network Simulators)
- ML algorithms
- Agile Scrum and PMBoK Frameworks
- Cloud and Local Virtual Machines

Project Outcomes

01 Data Ingestion
02 Data Understanding
03 Exploratory Data Analysis
04 Feature Engineering
05 Modelling

Result
95% accuracy
Low error rate (<1%)
100+ features identified

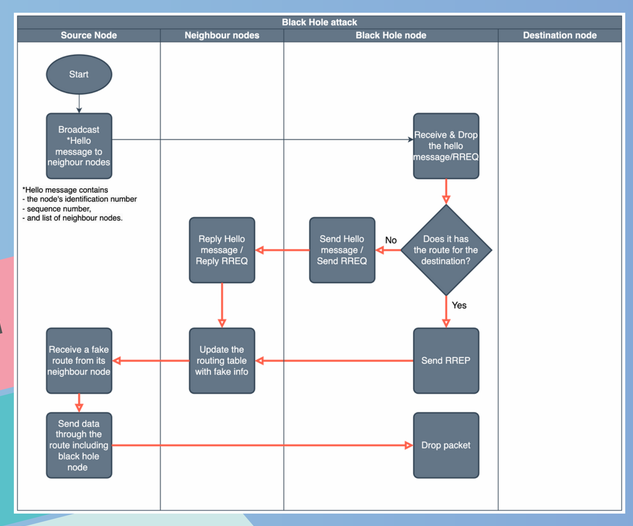
Black Hole resistant model

Reproducible Environment
Build Instructions

Dataset generated through simulation environment

Agile Scrum
PMBOK
Flow Chart Diagrams

Professional Documentation



Recommendations

- Full utilisation of NS3 program
- Refinements to energy usage modelling in NS3 program
- Refinement of features exhibited by Black Hole Nodes
- Higher complexity for Black Hole Node decision-making
- Real-world network capture

Conclusion

- Developed a machine learning model to confidently detect malicious nodes
- Overcame various challenges: Configuration of network simulation software and data engineering for machine learning model training
- Identified many future enhancements
- Core project objective of detection model generation has been delivered
- Implementation of the ML model was unsuccessful

References

- 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.
- 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.
- 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.

Project Team

Dr. Yibe Alem
Project Sponsor

Maryam Sousani
Project Mentor

Daniel Davaris
Programming & Modelling

Minjeong “Ellie” Kim
Research & Project Direction

Curtis Richardson
System Operations & Documentation