An AI-Driven Intrusion Detection System to Defend Against Satellite Hijacking

Karunathilake K. K. H.

Reg. No.: MS24014922

A THESIS
SUBMITTED TO
SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

December 2025

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

____

Mr. Kavinga Yapa Abeywardena

Approved for MSc Research Project:

____

MSc in IT Program Coordinator, SLIIT

Approved for MSc:

____

Head of Graduate Studies, FOC, SLIIT

DECLARATION

This is to certify that the work is entirely my own and not of any other person, unless explicitly acknowledged (including citation of published and unpublished sources). The work has not previously been submitted in any form to the Sri Lanka Institute of Information Technology or to any other institution for assessment for any other purpose.

Signature:

Karunathilake K. K. H.

Date: 01.11.2025

ABSTRACT

An AI- Driven Intrusion Detection System to Defend Against Satellite Hijacking

Himashi Karunathilake
MSc in Information Technology
Supervisor: Mr. Kavinga Yapa Abeywardena
December 2025

The increasing reliance of the world on satellite systems has made them prime targets for cyber threats, with satellite orbital manipulation, a form of satellite hijacking, posing a critical national security risk due to its potential for disrupting essential infrastructure. To address this threat, this research proposes a novel Artificial Intelligence (AI)-based anomaly detection system tailored for identifying suspicious orbital maneuvers. The study employs Machine Learning (ML) models to analyze a custom dataset derived from the public European Space Agency Anomaly Detection Benchmark (ESA-ADB). This dataset was rigorously pre-filtered to include only anomalies occurring within a ±48.00 hours window of a telecommand execution, thereby creating a naturally balanced, command-linked dataset to proxy for the kinematic footprint of a cyberattack. Findings established that temporal pattern recognition is paramount for detecting these attacks. LSTM networks emerged as the most promising model, leveraging their ability to learn sequential dependencies to achieve a high recall rate of 95.64% with a corresponding precision of 90.88%. Furthermore, a novel physics validation gate, grounded in orbital mechanics, was incorporated as a final, non-negotiable security layer. This component is vital, as it confirms that detected anomalies are physically non-nominal deviations, transforming raw statistical alerts into high-confidence cybersecurity indicators and dramatically boosting the overall trustworthiness and suitability of the system for operational deployment.

ACKNOWLEDGEMENT

I might not have been able to successfully conclude this yearlong research, if not for the immeasurable encouragement, guidance, support, and contribution of the many individuals behind the curtains.

Firstly, I would like to thank my Supervisor, Mr. Kavinga Yapa Abeywardena for his immeasurable guidance and support in conducting this research. The knowledge and the experience he shared, undoubtedly paved way for me to successfully complete this research. I would also like to thank Dr. Sara Vecchini, who provided technical supervision for this research, for always pointing me in the correct direction and sharing her knowledge and expertise.

I am also thankful to Mr. Prasanna Shankar who is a part of the Ansys / Synopsys Academic Program Team for his support in obtaining the required licensing for Ansys Systems Tools Kit (STK), which was extremely beneficial for my research.

I would also like to extend my sincere gratitude to all my lecturers and my research panel members for the immense knowledge they shared with me during the course of these past two years, which undoubtedly helped me to achieve my objectives for this research.

I also want to thank my friends for always sharing their feedback and experience with me.

Finally, my utmost gratitude goes out to my parents and my brother, who were there with me since the beginning, supporting me in my journey.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Definition
1DCNN	One-Dimensional Convolutional Neural Network
3D	Three Dimensional
ADAPT-Lite	Advanced Diagnostics And Prognostics Testbed-Lite
AI	Artificial Intelligence
ALFA	Air Laboratory Failure and Anomaly
ARIMA	Auto Regressive Integrated Moving Average
ASAT	Anti-Satellite
AUC	Area Under the Curve
BADMM	Bregman Alternating Direction Method of Multipliers
CAE	Convolutional Autoencoder
CEG	Causality Enhanced Graph
cFS	core Flight System
CPS	Cyber Physical System
CTF	Capture the Flag
DCDSPOT	Double-Criteria Drift Streaming Peaks Over Threshold
DDMN	Deviation Divide Mean over Neighbors
DDTS	Dynamic Detection Threshold Setting
DTW	Dynamic Time Warping
Ecc	Eccentricity
EPS	Electrical Power System
ESA	European Space Agency
ESA-ADB	European Space Agency Anomaly Detection Benchmark

F1PA	F1 Point Adjust
FastICA	Fast Independent Component Analysis
FC	F1-Score Composite
FCC	Flight Control Center
FNR	False Negative Rate
FPR	False Positive Rate
GA	Genetic Algorithm
GCC	Ground Control Center
GNN	Graph Neural Network
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GRU	Gated Recurrent Unit
HPOP	High Precision Orbit Propagator
IDS	Intrusion Detection System
IF-CBLOF	Isolation Forest and Clustering-Based Local Outlier Factor
Inc	Inclination
IQR	Inter-Quartile Range
K-DTWAN	K-Dynamic Time Wrapping Distance Adjacent Nodes
K-SVD	K-Means Singular Value Decomposition
KNN	K-Nearest Neighbors
KDE	Kernel Density Estimation
KL	Kullback-Leibler
LEO	Low Earth Orbit
LIME	Local Interpretable Model-Agnostic Explanations
LRP	Layer-wise Relevance Propagation
LSTM	Long Short-Term Memory
MCDA	Multi-Criteria Decision Analysis
ML	Machine Learning

MSE	Mean Squared Error
MSL	Mars Science Laboratory
MTAD	Multi-Task Anomaly Detection
NASA	National Aeronautics and Space Administration
NB65	Network Battalion 65
OBCS	On-Board Computer System
OCKELM	One-Class Kernel Extreme Learning Machine
OCSVM	One-Class Support Vector Machine
OOL	Out-Of-Limit
PCA	Principal Component Analysis
PR	Precision-Recall
QPSO	Quantum-behaved Particle Swarm Optimization
RaaS	Ransomware-as-a-Service
RNN	Recurrent Neural Network
ROSCOSMOS	Russian State Corporation for Space Activities
RPM	Revolutions Per Minute
RWL	Reaction Wheels
SACS	Satellite Attitude and Control System
SFAD	Sparse Feature-based Anomaly Detection
SHAP	Shapley Addictive Explanations
SJ-21	Shijian-21
SMA	Semi-Major Axis
SMAP	Soil Moisture Active Passive
SSO	Sun-Synchronous Orbit
STCG	Spatial-Temporal Causal Graph
STK	Systems Tool Kit
SVDD	Support Vector Data Description
TGAK	Triangular Global Alignment Kernel

TGAK-OCELM	Triangular Global Alignment Kernel One-Class Extreme Learning Machine
TN	True Negative
TNR	True Negative Rate
TP	True Positive
TPR	True Positive Rate
UAV	Unmanned Aerial Vehicle
VAE	Variational Autoencoder