QR Code

DO NOT REMOVE

SMARTSAT COOPERATIVE RESEARCH CENTRE

SOUTHERN LAUNCH

University of South Australia

Australian Government
Department of Defence

Attack Resilient CubeSat Constellations

(Contact: 0467155057)

| Mr Joshua Davis[†1] | Dr Yee Wei Law[†2] | Dr Ronald Mulinde[†3] | AsProf. Dave Ormrod[†4] | Prof. Jill Slay[†5] | Mr Shane Bennett [‡6§7] |

Introduction

In recent years, the space sector has seen academia and industry emerging as significant players in the small satellite sector [1]. Fueled by CubeSats, compact satellites utilising Field Programmable Gate Arrays (FPGAs), housed in affordable 10cm^3 (1U) modules [2]. However, cyber attacks on space systems have risen exponentially in accordance with the number of satellites launched [2, 4]. Particularly concerning is the rise of sophisticated multi-stage cyber attacks [3]. To combat cyber threats, machine learning-based Intrusion Detection Systems (IDSs) are increasingly adopted. However, there is a glaring gap in the datasets used to train IDSs. Derived primarily from terrestrial networks, existing datasets lack the unique dynamics and communications of space systems, such as limited access windows and space system traffic utilising the standards of the Consultative Committee for Space Data Systems (CCSDS).

Aims

- Develop a comprehensive dataset tailored to the multifaceted segments of space systems (ground, user, space).
- Enhance the efficiency and efficacy of machine-learning-based intrusion detection systems in the space sector, to protect CubeSats and ensure the safety and integrity of the data they handle.

Methods

- Analyse the current shortcomings of datasets derived from terrestrial networks for their inability to fully address the unique dynamics of space systems.
- Design and implement realistic multi-stage cyber threats specific to space systems into a high fidelity CCSDS satellite simulation package.
- Develop a methodology for the creation of a space intrusion detection dataset, incorporating the distinct communication standards of space, namely the CCSDS.
- Validate the developed dataset through iterative testing on FPGA hardware, equivalent small satellite architecture to reduce power and resource consumption.

References

[1] E. Kulu, Nanosatellite launch forecasts 2022: Track record and latest prediction, 2022, Figures last updated 31 May 2023. Available at https://www.nanosats.eu/#figures.

[2] M. Manulis, C. P. Bridges, R. Harrison, V. Sekar, and A. Davis, Cyber security in New Space, International Journal of Information Security 20 (2021), 287–311. https://doi.org/10.1007/s10207-020-00503-w.

[3] G. Falco, A. Viswanathan, and A. Santangelo, Cubesat security attack tree analysis, in 2021 IEEE 8th International Conference on Space Mission Challenges for Information Technology (SMC-IT), 2021, pp. 68–76. https://doi.org/10.1109/SMC-IT51442.2021.00016.

[4] J. Pavur and I. Martinovic, Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight, Journal of Cybersecurity 8 no. 1 (2022). https://doi.org/10.1093/cybsec/tyac008.

Results

- The design and development of space system multi-stage attack scenarios, leveraging historical, theoretical and common software vulnerabilities.
- Integration of vulnerable software applications into simulation platform for the capture of malicious and benign space system CCSDS traffic.
- Dataset creation and segmentation for granularity by encryption, data source or hardware/software component.
- Iterative pipeline for FPGA machine learning-based IDS.

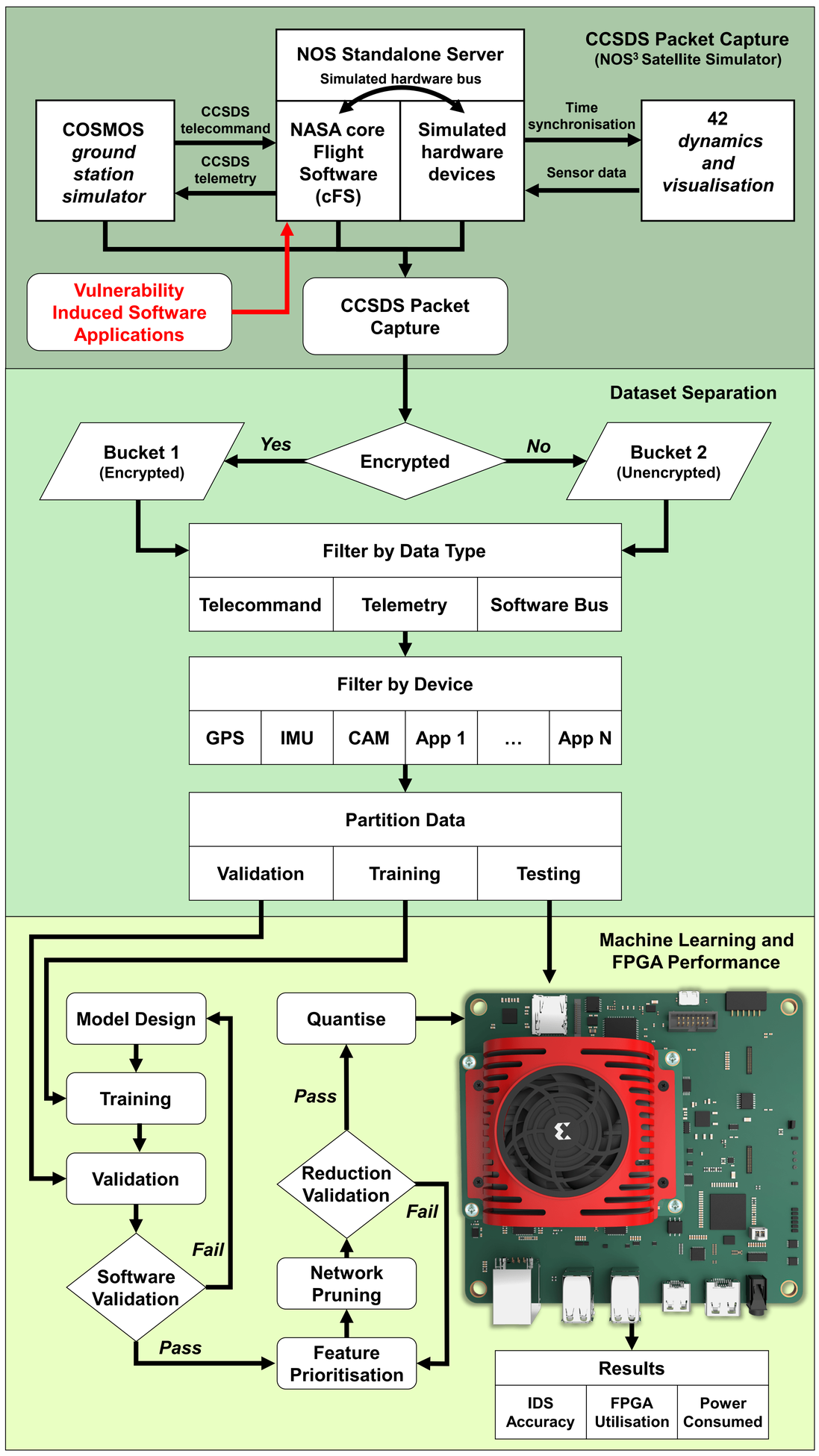

Figure 1. CCSDS Capture, Dataset Creation and FPGA machine learning framework

[†]University of South Australia [‡]Southern Launch [§]Defence Science and Technology Group (DSTG)

[1]PhD Candidate [2]Senior Lecturer [3]Adjunct Research Fellow [4]Enterprise Fellow [5]SmartSat Chair: Cybersecurity [6]Mission Control Manager [7]GL Cyber Integrations

Australian Government
Department of Industry, Science, Energy and Resources
AusIndustry
Cooperative Research Centres Program