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] | AsProf. Dave Ormrod[†2] | Dr Ronald Mulinde[†3] | Prof. Jill Slay[†4] | Mr Shane Bennett [‡5§6] |

Introduction

The rapid proliferation of the small space sector, has seen academia and industry emerging as significant players within the domain [1]. This is largely attributed to CubeSats, compact nanosatellites often comprising commercial-off-the-shelf-components (COTS) and 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, as the quality and quantity of available data directly impacts intrusion accuracy, there is a glaring gap in the datasets used to train IDSs on space systems. 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 and space segments).
- 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 limitations of datasets derived from terrestrial networks in addressing space system communications and dynamics.
- Design and implement realistic, benign nominal and fault data, alongside multi-stage cyber threats, specific to space systems in a high fidelity CCSDS satellite emulation package.
- Develop a methodology and the creation of a space intrusion detection dataset, incorporating the distinct communication standards of space, namely the CCSDS.

.

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.

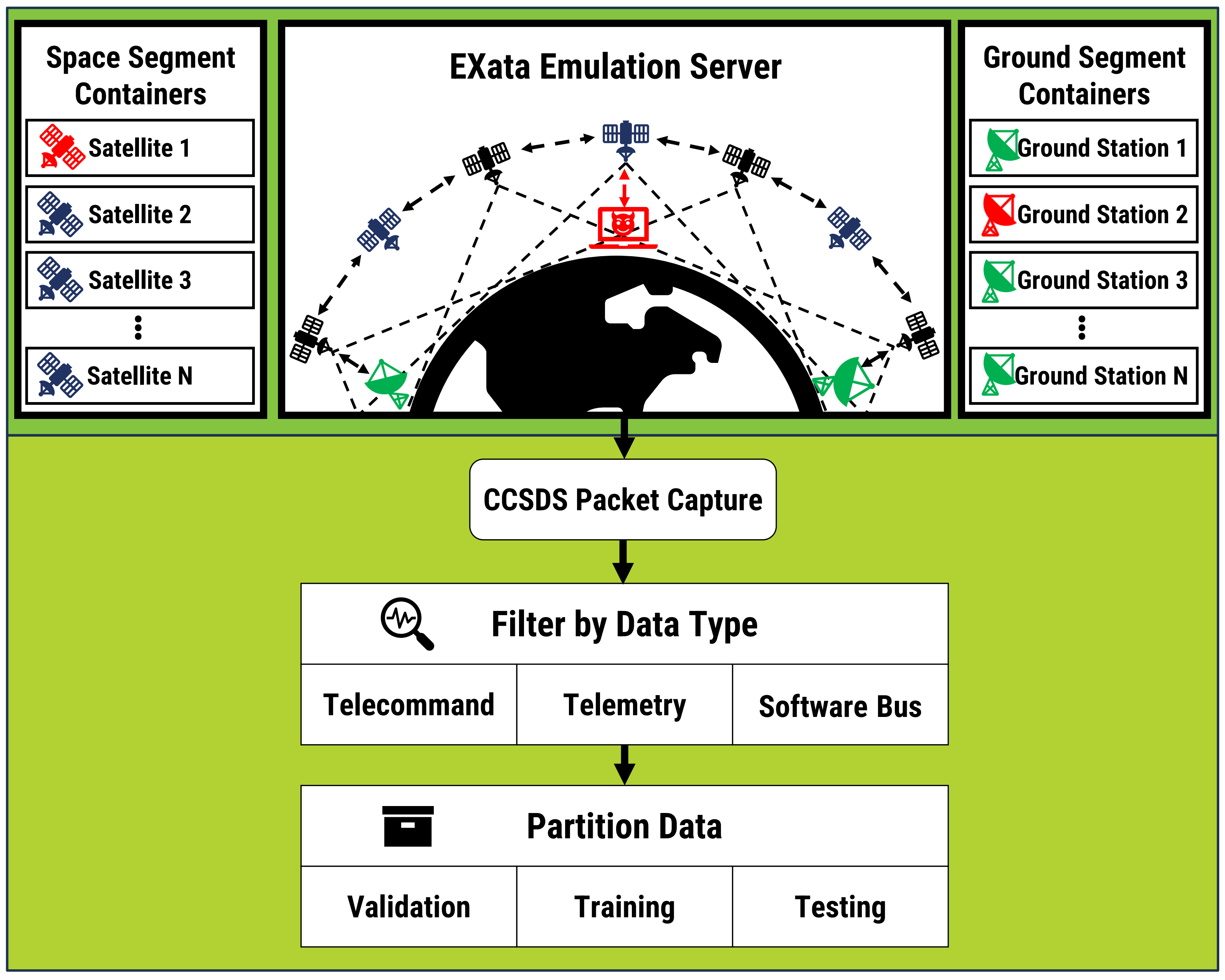
[2] M. Manulis, C. P. Bridges, R. Harrison, V. Sekar, and A. Davis, Cyber security in New Space, International Journal of Information Security 20 (2021), 287–311. https://doi.org/10.1007/s10207-020-00503-w.

[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.

Preliminary Results

- The design and development of space system multi-stage attack scenarios, leveraging historical, theoretical and common software vulnerabilities.
- High fidelity emulated space and ground segment nodes with effective satellite constellation data propagation mechanisms.
- Co-emulation environment development for data capture and potential precursor to hardware-in-the-loop (HITL) pre-flight cyber resilience testing framework.
- Dataset creation and segmentation by granularity of data source or hardware/software components.



Space Segment Containers
Satellite 1
Satellite 2
Satellite 3
⋮
Satellite N
EXata Emulation Server
Ground Segment Containers
Ground Station 1
Ground Station 2
Ground Station 3
⋮
Ground Station N
CCSDS Packet Capture
Filter by Data Type
Telecommand | Telemetry | Software Bus
Partition Data
Validation | Training | Testing

Figure 1. Co-Emulation Framework & Data Process Flow

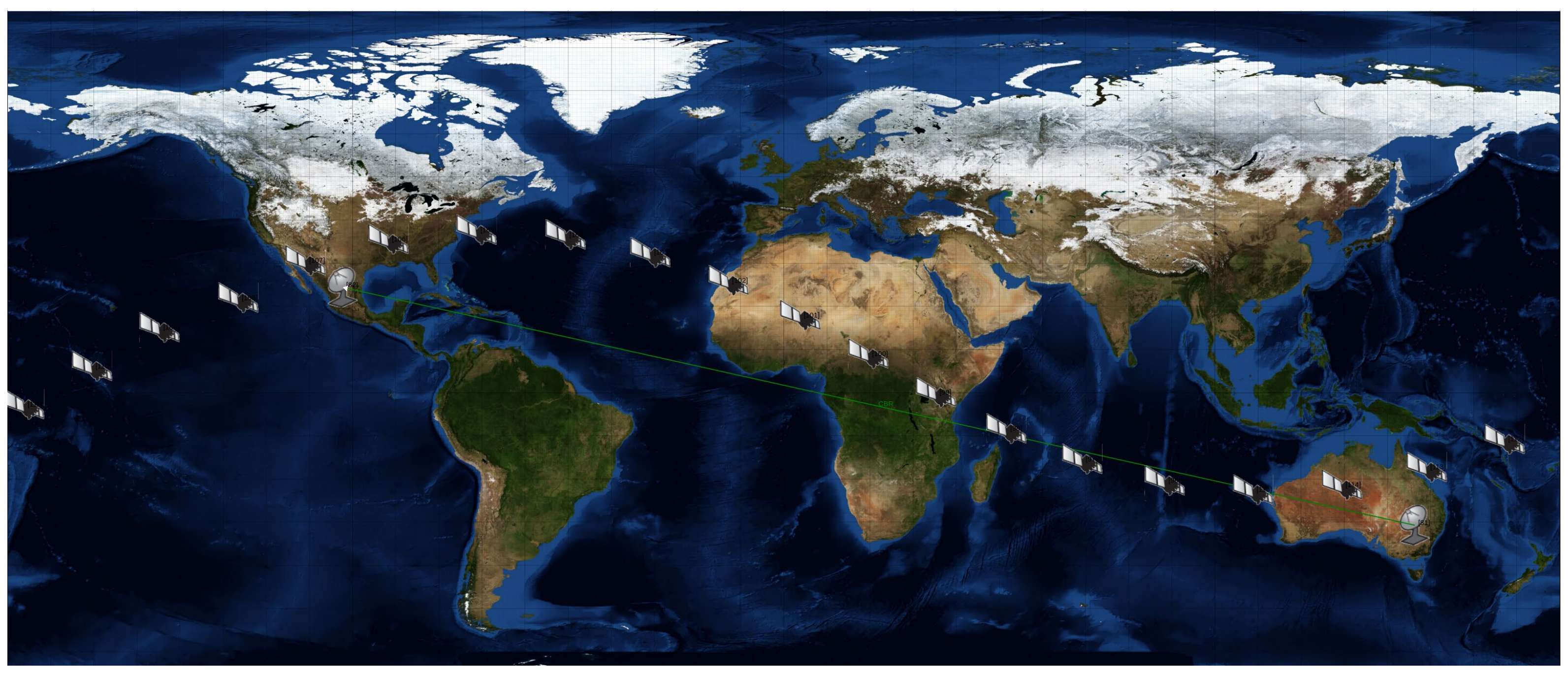


Figure 2. Co-Emulation Scenario Configuration

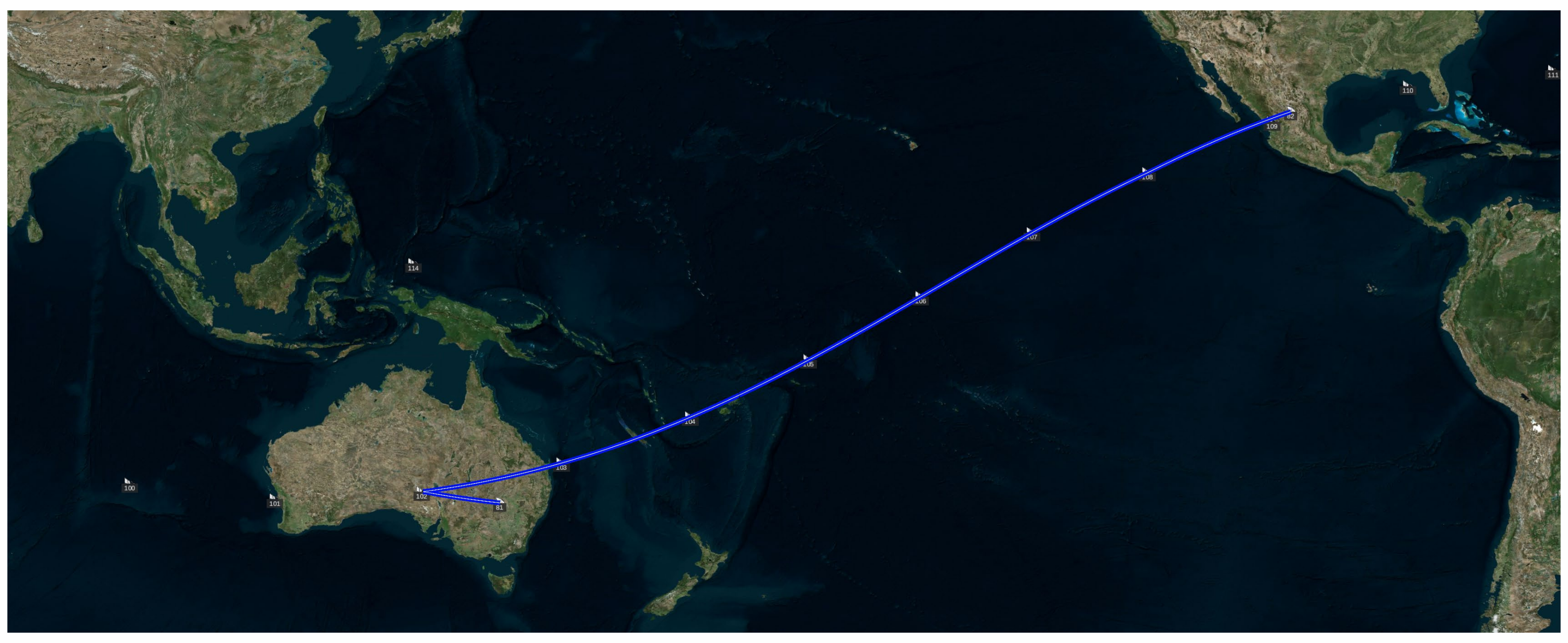


Figure 3. Constellation Multi-Hop Propagation

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

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

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