QR Code

DO NOT REMOVE

SMARTSAT COOPERATIVE RESEARCH CENTRE

University of South Australia

Development of Intelligent Security Controls for SDN-based Space Systems

Uakomba Uhongora

Introduction

Space systems play a vital role in our everyday lives. Global communication, weather prediction, and Internet connectivity to rural and remote areas, are some of the services that rely on space systems. The space systems' increased importance to national security, and critical infrastructure has attracted entities who aim to compromise the services that depend on space systems. Software-Defined Networking (SDN) transforms traditional networking architectures by separating the control plane from the data plane. This separation enhances scalability and centralized management of networks. The integration of SDN in space systems can provide the benefits of managing and the ease of configuring a large-scale space system. This research integrates SDN in space systems and the development of security controls to safeguard SDN-based space systems from malicious activities.

Knowledge gap

The research project addresses three major knowledge gaps:

1. Securing space systems.
2. Integrating space systems and SDN.
3. Implement intelligent security controls for SDN-based space systems

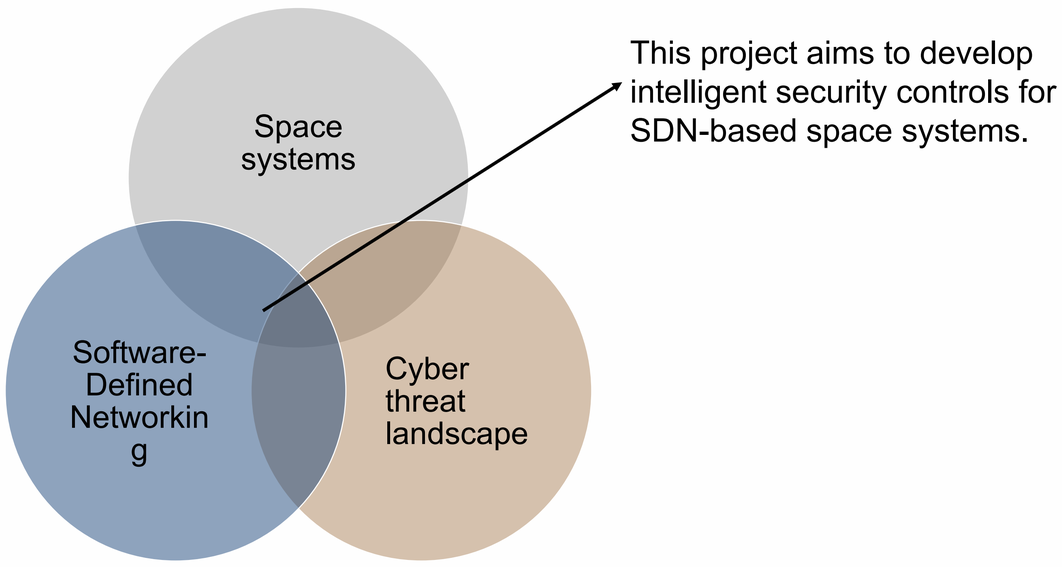


Fig. 1: Research scope

Motivation

- Space systems are vulnerable to cyber-attacks [1] [2] [3].
- Space systems are manually configured and controlled [4].
- SDN can provide automation, a centralized view, and control of a space system [4][5].
- SDN can provide ease of deploying security policy in a space system.
- Though SDN offers exceptional features for space systems, it is vulnerable mainly at its control plane.
- Security controls need to be developed to secure SDN-based space systems.

Methodology

This project applies a quantitative approach, using a deductive method (step-by-step). The research will be conducted by performing experiments and a peer-reviewed literature search.

The diagram below shows an example of SDN integration in a space system [6].

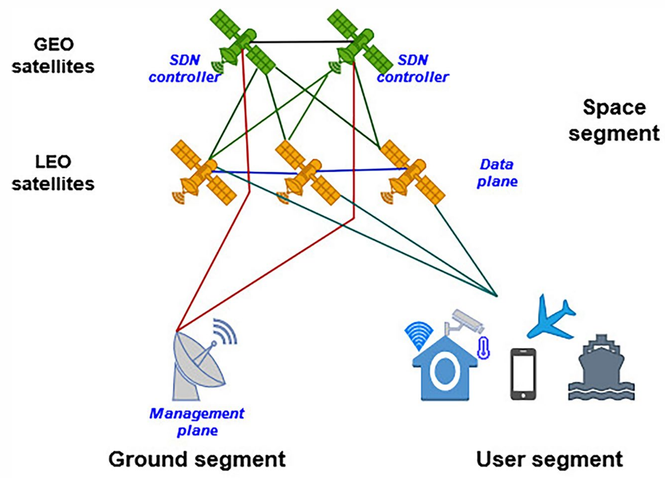
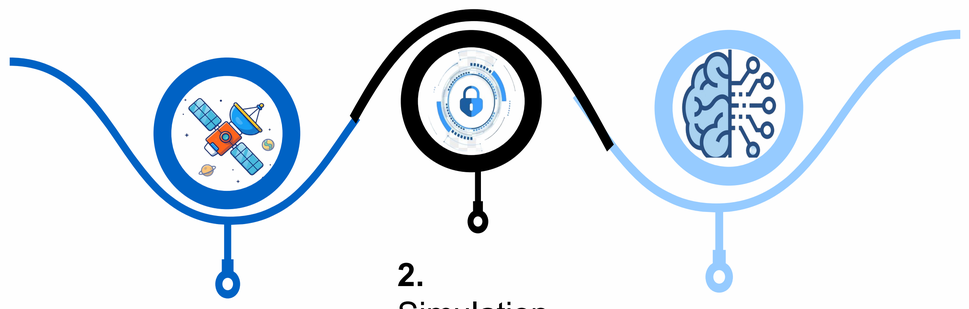


Fig. 2: SDN-based space system

To achieve the project's objective the following process illustrated in Fig 3. is followed.



1. Perform a detailed security analysis based on security frameworks, i.e., MITRE's ATT&CK, and SPARTA.

2. Simulation of SDN-based space system i.e. Mininet.

3. Investigate, develop, and application of DL-based anomaly detection.

Fig. 3: Methodology

References

[1] Falco, G. (2018) 'Cybersecurity Principles for Space Systems', Journal of Aerospace Information Systems, (December 2018). Available at: https://doi.org/10.2514/1.I010693.

[2] Plotnek, J. and Slay, J. (2022) 'Space Systems Security: A Definition and Knowledge Domain for the Contemporary Context', Journal of Information Warfare, 21(3), pp. 103–119. Available at: https://www.jinfowar.com/journal-issue/volume-21-issue-3.

[3] Manulis, M. et al. (2020) 'Cyber security in New Space: Analysis of threats, key enabling technologies and challenges', International Journal of Information Security, 20(3), pp. 287–311. Available at: https://doi.org/10.1007/s10207-020-00503-w.

[4] Semmoud, A. and Benmammar, B. (2021) 'Intelligent Security of Computer Networks', in Intelligent Network Management and Control. John Wiley & Sons, Ltd, pp. 1–24. Available at: https://doi.org/10.1002/9781119817840.

[5] Pradhan, A. and Mathew, R. (2020) 'Solutions to Vulnerabilities and Threats in Software Defined Networking (SDN)', Procedia Computer Science, 171, pp. 2581–2589. Available at: https://doi.org/10.1016/j.procs.2020.04.280.

[6] Jiang, W. "Software Defined Satellite Networks: A Survey." *Digital Communications and Networks*, 2023. https://doi.org/10.1016/j.dcan.2023.01.016.

University of South Australia (UniSA)

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