Development of Intelligent Security Controls for SDN-based Space Systems

University of South Australia

Uakomba Uhongora, PhD candidate at UniSA

uhouy001@mymail.unisa.edu.au 0416 756 806

Introduction and Research Aim

Space systems play a vital role in our everyday lives. Global communication, weather prediction, and Internet connectivity for rural and remote areas, are some 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) is a network paradigm that transforms traditional networking architectures by separating the control plane from the data plane. Space systems can leverage the benefits offered by SDN such as scalability and centralized management of a large-scale space system provided by the SDN architecture.

This research **integrates Software-Defined Networking (SDN) in space systems** and **aims to develop intelligent security controls** to secure the SDN-based space system. Figure 1 shows the proposed SDN-based space system architecture with multiple controllers.

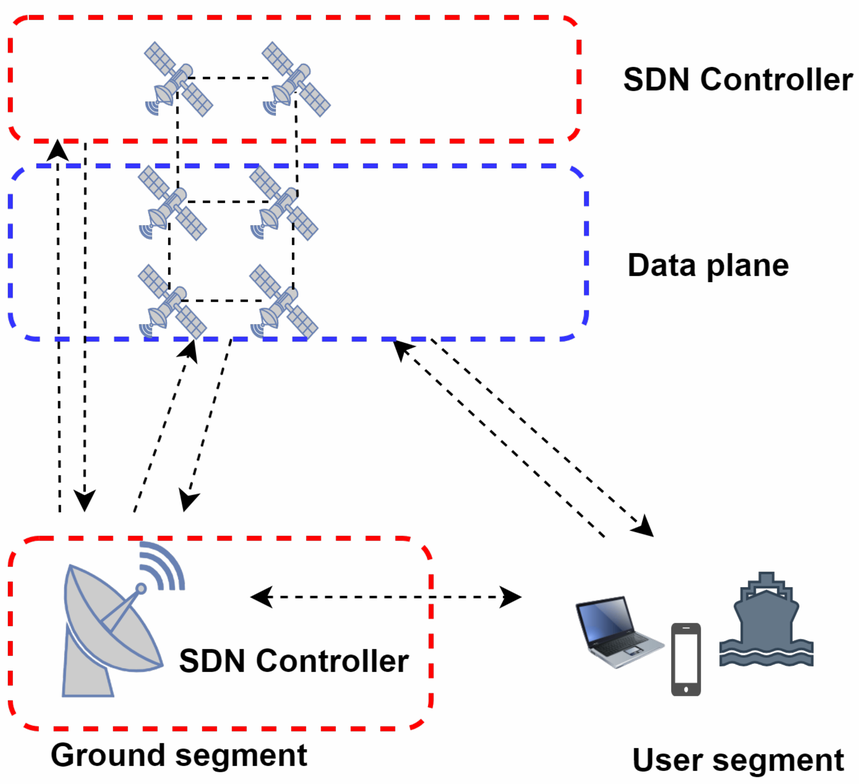

Fig. 1: SDN-based space system

Benefits of SDN in space systems

1. **Real-time centralized view and management**

SDN controller monitors and configures the space network as required which enables flexible and efficient use of resources in a space system.

2. **Redundant architecture (distributed controllers)**

Distributed controllers can eliminate single point of failure for SDN-based space systems.

3. **Scalability**

SDN can make it easy and cost-effective for space system operators to add new components to a space network as the space mission can vary throughout its lifetime.

4. **Security**

The controller can promptly determine a network attack. SDN provides dynamic network segmentation which limits the attack surface of the space system by isolating the compromised segment from the rest of the network.

Methodology and Results

This project applies a quantitative approach. The research is conducted by performing experiments and a peer-reviewed literature search.

- **Threat mapping using the SPARTA framework**

This research explored the benefits and challenges of SDN-based space systems by mapping security threats using the SPARTA framework. The process is depicted in Figure 2 below.

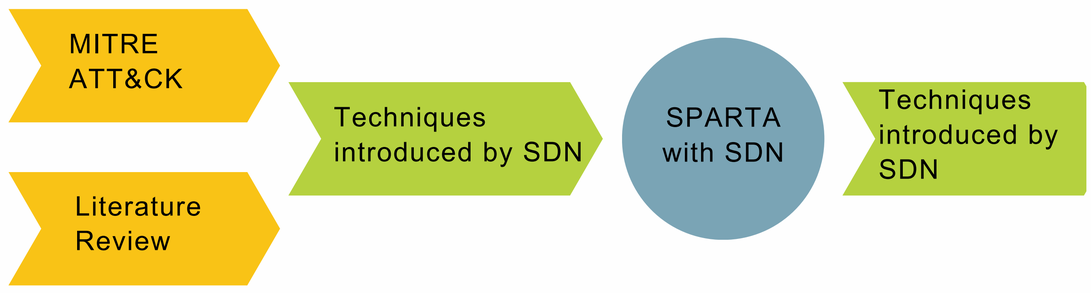

Fig. 2: Threat mapping

- **Cyber security challenges of SDN-based space systems**

Table 1: Threats and attacks against SDN-based space systems

Threats and attacks
DDoS attack
Jamming
Flow rule poisoning or modification
Supply chain attacks
Satellite hijacking
Man-in-the-middle attack
Session hijacking
Centralized single-point of failure

- **Experiments are underway using the following tools:**

Mininet: a network emulator which creates a network of virtual hosts, switches, controllers, and links.

Open Network Operating System (ONOS): an Operating System designed to create an SDN controller.

Ansys Systems Tool Kit (STK): Create and simulate a realistic space network.

- **Implementation of security controls**

The research aims to implement intelligent controls on a simulated SDN-based space network leveraging artificial intelligence techniques to mitigate the identified common attacks.

References

Guo, C., Guo, J., Yu, C., Li, Z., Gong, C., and Waheed, A. "A Safe and Reliable Routing Mechanism of LEO Satellite Based on SDN." 2020.

Falco, G. (2018) 'Cybersecurity Principles for Space Systems '(December 2018).

Manulis, M. et al. (2020) 'Cyber security in New Space: Analysis of threats, key enabling technologies and challenges'

Jiang, W. "Software Defined Satellite Networks: A Survey." Digital Communications and Networks, 2023.

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