Paper ID: 99141
oral

58th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cybersecurity in space systems, risks and countermeasures (4)

Author: Dr. Rabbia Saleem
UNSW Canberra, Australia

Dr. Rizka Purwanto
Monash University, Indonesia
Mr. Syed Shahzad
Australian Defence Force Academy (ADFA), Australia
Dr. Melrose Brown
Australian Defence Force Academy (ADFA), Australia
Mr. Jonnathan Franco Acuna
UNSW Canberra, Australia

DISTRIBUTED LEARNING-DRIVEN DESIGN FOR CYBER SECURE SPACE CONSTELLATION NETWORK

Abstract

The global space network is undergoing a rapid growth, with numerous commercial, defense, and government players launching their satellites into space. The increasing space population is also encountering issues of massive connectivity, leading to the management of vast volumes of data and information and consequently, heightened risks of cyber security. Without proactive security and defense measures, these space assets are vulnerable to cyber threats such as unauthorized access, adversarial attacks, jamming, spoofing, denial of service, etc. Currently, artificial intelligence (AI) techniques based on distributed learning frameworks have revolutionized the solutions to tackle the critical challenges of cyber security in the space industry due to their inherent capability to support collaborative networks as opposed to centralized systems. The research work proposes a federated learning-based intrusion detection strategy in a satellite constellation network against unauthorized access. The mechanism is deployed on Intelligent Satellite Constellation Sandbox (ISaCS) testbed, an advanced simulation-based framework equipped with eight flatsats of high AI capability that can replicate real satellite functions. Within this framework, both centralized and distributed intelligent environment is explored for testing, learning, and assessing the responses of the satellite network against cyber threats. Unlike centralized learning that consolidates data from all satellites into a central server for processing and decision-making, federated learning allows the satellites to collaboratively learn from local data without sharing sensitive information. Furthermore, the model enables monitoring the real-time data for unknown patterns, identification of satellites under attack, adaptive responses, and coordinated operations across the network to carry seamless tasks via unaffected satellites. Therefore, guaranteeing a more secure, autonomous, and robust threat detection and mitigation strategy.