57th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cybersecurity in space systems, risks and countermeasures (4)

Author: Mrs. Anna Barraqué
CYSEC FRANCE, France

Mr. Julien Airaud
Centre National d'Etudes Spatiales (CNES), France

THE USE OF AI IN THE DETECTION OF CYBER INTRUSIONS IN ORBITAL SYSTEMS

Abstract

The Viasat attack, which interrupted the KA-SAT service, took place on February 24, 2022, one hour before Russia's invasion of Ukraine, and a year before the start of this work. It stressed the importance of cybersecurity in all sectors, including space. Satellites play a key role in various aspects of our daily lives. Their availability must be preserved. Traditional space systems were thought beyond the scope of cyber-attackers. However, the latter are gaining in professionalism and resources, threatening ground systems as well as the 7,702 satellites in orbit and the 1,700 'New Space' satellites planned for launch per year until 2030. Detecting cyberattacks on systems requires a wide and permanent scan of parameters, now possible through Artificial Intelligence (AI). This last decade, AI has seen rapid growth and is now essential to process large amounts of data. The CSS project, for Cybersecurity Space Simulation, aims at showing how AI models can detect simulated cyber-attacks on simulated space systems. The project gathers the CNES (Centre National d'Etudes Spatiales, the French space agency), satellite industrials, space security industrials, and research laboratories on cybersecurity and AI. Several models exist in AI. The approach followed by this paper is inspired from a popular and efficient strategy mainly used in XGBoost (eXtreme Gradient Boosting). The idea is to combine different algorithms to build an overall model with higher performances. This work shows that a combination of two anomaly detection algorithms - One-Class Support Vector Machine (OCSVM) and Density-Based Spatial Clustering of Applications with Noise (DBSCAN) - is very efficient to identify whether a network flow represents a normal connection or a cyber-attack. This paper presents the existing cyber threats on space systems depending on their mission and focusing on New Space common architectures, the designed space architecture for the project's simulations, and the development and performances of the AI models to detect cyber-attacks from simulated network flows. The objective is to later transpose these models onto simulated satellite telemetry and evaluate their performance through simulations in a cyber-range. The CSS project contributes to shaping the sector by using new technologies to cope with new problematics.

Keywords: space, cybersecurity, artificial intelligence, network intrusion