Paper ID: 91485
student

57th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Interactive Presentations - 57th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (IPB)

Author: Mrs. Gouri Deshpande
India

CURRENT ADVANCES OF AI METHODOLOGIES AND ITS APPLICATIONS IN SATELLITE SECURITY SYSTEMS

Abstract

Satellite communication system is one of the immerging fields and is getting commercialized with entry of large private sector players across the globe. This is being termed as next generation communication and will play a key role to deal with increased demands. Enhanced communication needs would arise from massive Internet-of-Things (IoT) devices, required in the form of smart cities, smart health monitoring system, etc.; as well as expanding the reach to remote locations, where ground based wired networks cannot be installed. These applications are expected to grow explosively and as a result several thousands of swarm satellites would be deployed in Lower Earth Orbit (LEO) and Medium Earth Orbit (MEO).

With large Global Navigation Satellite System (GNSS) networks, security breaches would also enhance exponentially. This could be in multiple ways, namely, data spoofing attacks, jamming, confidentiality breach, accessing control by hacking the satellites, and further misusing the satellite for wrong purposes. With advances in technological developments, measures to improve security system are required on priority. In view of this, in the present work, we analyze anti-spoofing techniques and hacking detection/ prevention mechanisms. For this purpose, AI based tools have been explored to detect satellite data spoofing as well as breach detection. Work is split in two parts. In the first parts, we compared various AI/ML methods used in the satellite security systems. In the second part, we assessed use-case based on simulation data, to evaluate 2 most prominent models namely. Neural Networks and block-chain.

Main objective of AI based methods was to make fingerprint features of the satellite. Data trajectory was simulated for several satellites in LEO to assess the swarm effect. Input data is generated to make repetitive trajectory bands with combination of events and thereby generating large training set. Trajectory change scenarios were also generated in the software. Model for anomaly detection was made indicating changing course of action. Model would be further tested in the real-life scenario to detect dead or hacked satellites.

The use case on block chain algorithm was tested to mimic secure end to end data channel development. Block chain algorithm involve series of blocks checks to (a) assess packet dispatch, (b) intermediate satellite check and (c) Ground station receipt authentication.

To summarize, AI based tools and their applications to enhance security of the already operational satellites through software updates could be demonstrated.