Paper ID: 87772
student

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

Author: Mr. Jihoon Suh
The University of Texas at Austin, United States

Dr. Michael Hibbard
The University of Texas at Austin, United States
Dr. Kaoru Teranishi
The University of Texas at Austin, United States
Prof. Takashi Tanaka
The University of Texas at Austin, United States
Prof. Moriba Jah
Privateer Space, Inc., United States
Prof. Maruthi Akella
University of Texas at Austin, United States

ENCRYPTED COLLISION PROBABILITY FOR SECURE SATELLITE CONJUNCTION ANALYSIS

Abstract

The computation of collision probability ($\mathcal{P}_c$) is crucial for space environmentalism and sustainability by providing decision-making knowledge that can prevent collisions between anthropogenic space objects. However, the accuracy and precision of $\mathcal{P}_c$ computations is often compromised by limitations in computational resources and data availability. While significant improvements have been made in the computational aspects, the rising concerns regarding the privacy of collaborative data sharing can be a major limiting factor in the future conjunction analysis and risk assessment, especially as the space environment grows increasingly privatized and competitive with conflicting strategic interests. This paper argues that the importance of privacy measures in space situational awareness (SSA) is underappreciated, and regulatory and compliance measures currently in place are not sufficient by themselves, presenting a significant gap.

To address this gap, we introduce a novel encrypted architecture and computation protocol utilizing homomorphic encryption (HE) to preserve the privacy of entities involved in computing relevant space sustainability metrics, inter alia, $\mathcal{P}_c$. The proposed method integrates the Monte-Carlo approach with HE to allow for the secure computation of collision probabilities without exposing proprietary or otherwise sensitive information. Through detailed analysis and simulations, our study demonstrates the protocol's effectiveness in maintaining both privacy and computational accuracy. This research not only contributes to the innovation in the methodology for secure computation of $\mathcal{P}_c$ but also highlights the importance of innovative privacy solutions to encourage a more secure and cooperative SSA landscape in the future.