Paper ID: 98482
student

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

Author: Mr. Khalig Ganbarli
Azerbaijan State Oil and Industry University (ASOIU), Azerbaijan

Mr. Joshgun Mursalov
Azerbaijan State Oil and Industry University (ASOIU), Azerbaijan
Mr. Ruslan Amrahov
Azerbaijan State Oil and Industry University (SABAH Groups), Azerbaijan

THE ADVANCEMENT OF CYBERSECURITY IN SPACE THROUGH ARTIFICIAL İNTELLIGENCE: ADVANTAGES AND RISKS

Abstract

With the rapid development of technology, potential vulnerabilities for new cyberattacks are emerging. This trend also applies to space infrastructure. Cybersecurity programs such as traditional firewalls and antiviruses aren't be able to provide effective protection against new types of viruses and attacks from previously undiscovered vulnerabilities (Zero-day). It is clear that the consequences of successful attacks on space networks will be enormous. Because of this issue, the usage of artificial intelligence-based cybersecurity models is important. For this, Next Generation Firewall (NGFW) and Behavioral-Based Analysis (BBD) based security systems are available. Although, these systems are effective in terrestrial networks, they are not so usable to implement in space networks. The integral cause for this is the high latency in the space environment, limited computing resources, and intermittent connections. This paper suggest the creation of a novel Edge AI-based model for autonomous, real-time threat detection and prevention of security systems such as NGFW and BBD in space networks. In this case, the data is not sent to remote servers therefore advantages include reduced latency and load of network traffic, and increased security due to sensitive data being processed on the device. However, the usage of AI can bring various dangers. We will also touch on this issue. Concurrently, the implementation of Federal Learning (FL) technology is very suitable for our purpose. Namely, when there is a need to get connection with the servers, the FL system does not transmit all the information, but only the necessary information, thus eliminating the need to transfer sensitive data. In addition, the system can dynamically update security rules in real-time based on potential cyber threat data. These are essential for the security of space infrastructure. Moreover, this technology could also play an important role in ensuring cybersecurity on future lunar stations and Mars colonies. At the same time, the proposed approach also plans the use of lightweight and adaptive AI models that can be directly integrated into satellites, lunar stations, and Mars colonies. This can help decrease our dependence on Earth-based infrastructure. Ultimately, this research supports the high-level and adaptive development of cybersecurity away from Earth.