48th SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cyber-security threats to space missions and countermeasures to address them (4)

Author: Dr. Dong Yan
Beijing Institute of Spacecraft System Engineering, China Academy of Space Technology(CAST), China, yandong200@163.com

Mr. Ming Gu
Beijing Institute of Spacecraft System EngineeringChina Academy of Space Technology (CAST), China, gumingnr@163.com
Mr. Xiongwen He
Beijing Institute of Spacecraft System Engineering, China Academy of Space Technology(CAST), China, hexw501@hotmail.com
Dr. DAPENG WANG
China Academy of Space Technology (CAST), China, wangdapeng@cast.cn

A NOVEL SPACE NETWORK DOS SUPPRESSION APPROACH WITH CREDIBLE PROBABILISTIC PACKET MARKING

Abstract

Space network is an important part of next generation Internet. It has the advantage of global coverage, and offers a solution of easy access and many types of QoS. It will play an important role in weather forecast, emergency rescue, resource exploration, navigation positioning and others in many fields of science, culture and life. However, the nodes of space network have a limited processing power, which makes an insufficient safety protection and data transmission reliability. The Denial of Service (DoS) intrusion in the network will make the space network performance fell sharply, even collapse. In this paper, we analyze the characters of space network nodes, study the key technologies of space network secure protection, and then propose a novel DoS suppression scheme with credible probabilistic packet marking in space network. The scheme has two stages. In the first stage, the algorithm establishes a proper mathematics model, and then evaluates the nodes reputation with the model. It isolates the incredible nodes, which can make a reliable data transmission. In the second stage, the algorithm uses probabilistic packet marking scheme to mark the data, and then rebuild the path in the victim node. In this way, we can find the attacker and report to the network management center. The management center will suspend the network service of the suspect, and make a thorough check of the suspect system. In the end, the performance of path rebuilding is evaluated by simulations.