

Cybersecurity in 6G Satellite Communication

Arlette Houndji¹, Giuseppe Caso², Alfonso Iacovazzi¹, Simone Fischer-Hübner², Shahid Raza¹

¹Research Institutes of Sweden, ²Karlstad University

Abstract

The advent of 6G satellite communication (6G SATCOM) proclaims transformative enhancements in global connectivity, promising unprecedented data rates and expanded coverage in remote areas with mobility. However, this progression also surfaces complex cybersecurity challenges. This project explores the various security implications of integrating satellite communications in the 6th generation of networks. From the physical to the application layer, a variety of factors can constitute threats to the integrity of 6G SATCOMs. Since the publication of the Rel-17 by 3GPP, it has been made clear that the integration of satellite networks with terrestrial networks is the focal point of 6G networks, as various use cases depend on it. The benefits of having satellite networks as a native component of 6G networks are numerous: broader coverage, ubiquity, critical communications, as well as advancements in transportation, agriculture, healthcare and XR research. This implies an increase in the attack surface and brings us to scrutinize the ongoing efforts towards the protection of 6G SATCOMs. Also, the criticality of the infrastructures that rely on satellite communications, such as space stations, autonomous ships, airplanes, remote high-risk areas, makes the potential consequences of security breaches highly significant. We cannot, however, apply the same security schemes and techniques currently used in traditional terrestrial networks, as the designs are inherently different, and we can only hope to build on them and adapt to satellite communications. Our work focuses on studying the integration of SATCOM in 6G from a security point of view, developing adequate measures, from the technical to the regulatory aspects, to obtain a secure and resilient 6G.