Paper ID: 35767
oral

23rd IAA SYMPOSIUM ON SMALL SATELLITE MISSIONS (B4)
Highly Integrated Distributed Systems (7)

Author: Ms. Olga Korobova
Skolkovo Institute of Science and Technology, Russian Federation

Prof. Alessandro Golkar
Skolkovo Institute of Science and Technology, Russian Federation

DATA AUTHENTICATION, INTEGRITY AND CONFIDENTIALITY MECHANISMS FOR FEDERATED SATELLITE SYSTEMS

Abstract

We address a critical issue in federated satellites development: lack of trust between stakeholders that would prevent any user joining a satellite federation owned and operated by multiple parties. We propose a first characterization of security needs for federated satellite systems showing that in order for a federation to offer an environment for a beneficial cooperation, we need to introduce a notion of identity, while satisfying users' security requirements and provide security guarantees. This work presents a framework for addressing users security requirements and ensuring data authentication, integrity and confidentiality in data transfer operations within satellite federations, characterizing their performance and costs and providing recommendations for implementing security mechanisms in federated satellite systems.

The paper starts with a user need analysis, where we identify satellite federation users, analyze their needs and formulate their requirements to data security and desired security guarantees. The paper then proposes a system architecture for implementing security mechanisms in satellite federations, defining interfaces in federated satellite operations, addressing related security issues, and formulating metrics to evaluate the impact of security in federated satellite operations.

The proposed framework is based on a Public Key Infrastructure system for security in data transfer in federated satellite systems. The paper characterizes performances and costs tradeoffs of the proposed security mechanisms. It is illustrated how Public Key Infrastructure can be applied to satellite federations to bring the notion of identity to federated satellite systems and achieve its security goals. We identify security mechanisms that are suitable with federated satellite operations and present a protocol that enhances federated data relay applications with data authentication, integrity and confidentiality. The public key infrastructure framework here proposed allows spacecraft to reliably verify each other's identity before engaging in a cooperation, immediately detects a change in the relayed data content and identifies malicious spacecraft; it also ensures data authentication and data confidentiality.

The paper concludes with an experimental characterization of the proposed framework, as implemented on Raspberry Pi 2 and BeagleBone platforms, used as candidate testbeds of commercial off the shelf avionics for small satellites. Our preliminary evaluations of computation time and the network overhead of the framework suggest that the protocol's deployment may be feasible within satellite federations of realistic size.