Acta Astronautica 149 (2018) 61–76

Contents lists available at ScienceDirect

Acta Astronautica

journal homepage: www.elsevier.com/locate/actaastro

Data authentication, integrity and confidentiality mechanisms for federated satellite systems

Olga von Maurich*, Alessandro Golkar

Skolkovo Institute of Science and Technology, Skolkovo Innovation Center, Building 3, Moscow, 143026, Russia

ARTICLE INFO

Keywords:
Federated satellite systems (FSS)
Distributed satellite systems
Public key infrastructure (PKI)
Digital signatures
Hybrid encryption

ABSTRACT

This work addresses a critical topic in federated satellites development: the lack of trust between stakeholders that would prevent any stakeholder joining a satellite federation owned and operated by multiple parties. A characterisation of security needs for federated satellite systems is proposed, showing that in order for a federation to offer an environment for a beneficial cooperation, a notion of identity, both user identity and data authentication, has to be introduced, and stakeholders' security requirements have to be satisfied. This paper presents a public key infrastructure (PKI) based protocol for addressing stakeholders' security requirements and ensuring data authentication, integrity and confidentiality in data transfer operations within satellite federations. The performance and cost overheads of the proposed security protocol are first characterised with an experimental implementation on a Raspberry Pi 2 platform, used as a representative proxy testbed of commercial off-the-shelf avionics for small satellites, and then with a benchmark on a range of CPUs to analyse which platforms achieve set performance goals with radio-based and laser-based communications. Recommendations for implementing security mechanisms in federated satellite systems are thus derived.

1. Introduction

Security is a critical topic in federated satellites development: the lack of trust between stakeholders would prevent any stakeholder joining a satellite federation owned and operated by multiple parties and providing access to her spacecraft. Federated Satellite Systems (FSS) [1] are a *"sharing economy"* approach to space systems that aims to enable distribution of unused capacity among spacecraft by bringing spacecraft into a peer-to-peer (P2P) network and enabling an exchange of resources among spacecraft [2]. The aim of federated satellite systems (FSS) [2] is to provide a beneficial cooperation, which directly depends on the number of participating stakeholders. The more participants join the system, the more applications and a more beneficial cooperation federated satellite systems could offer. Keeping spacecraft interested in joining a satellite federation is therefore of crucial importance for federated satellite systems.

Federated satellite systems enable a large number of applications, where spacecraft' operators decide to collaborate with each other if they find the collaboration beneficial and secure. Security in federated satellite systems is motivated by the desired security requirements of the operators of federated satellite systems' spacecraft: the operators need to be able to verify identity of each other before engaging in a cooperation and have guarantees, that if they pay for a service, the service will be executed correctly.

To offer an environment for a beneficial cooperation, federated satellite systems have to respond to federated satellite systems' security requirements and provide security guarantees. The work in this paper investigates how notions of identity, data authentication, integrity and confidentiality could respond to federated satellite systems' security requirements. This work is conducted in the framework of the ONION "Operational Network of Individual Observation Nodes" project supported by the European Union's Horizon 2020 research and innovation programme. The goal of ONION is to propose a pragmatic, evolutionary and scalable approach, hybridising fractionated and federated satellite system concepts, and augmenting existing space assets for the development of future space missions and new services. Data security within opportunistic intersatellite operations is one of the fundamental challenges to enable innovative distributed satellite system concepts, as the absence of security guarantees between stakeholders would hinder the prospect of future satellite federations owned and operated by multiple parties, as the conducted security need analysis and identified security problems in Section 3.1 and Section 3.2 will show. This paper provides extended results that address not only to the goals of the ONION project, but also aim development of security mechanisms in generic spacecraft operations (not limited to Earth Observation).

The research objectives of the paper are to identify and apply

* Corresponding author.
E-mail addresses: olga.korobova@skolkovotech.ru (O. von Maurich), a.golkar@skoltech.ru (A. Golkar).

https://doi.org/10.1016/j.actaastro.2018.05.003
Received 25 January 2017; Received in revised form 3 November 2017; Accepted 2 May 2018
Available online 10 May 2018

suitable security mechanisms to regulate opportunistic intersatellite operations in federated satellite systems. The focus of the paper is on the space segment only, in particular satellite-to-satellite operations. More specifically, this work unfolds into five research objectives:

(i) to identify data security problems in federated satellite systems' operations and federated satellite systems' needs for authentication, integrity and confidentiality;
(ii) to identify security mechanisms that are suitable for federated satellite systems' operations, i.e., security mechanisms that address formulated security requirements and account for the constraints introduced by opportunistic intersatellite operations, i.e., a computational constraint (accounting for the computational constraint is illustrated throughout the Implementation Section 4.1);
(iii) to provide a security protocol to regulate secure data transactions in federated satellite systems' operations;
(iv) to characterise the performance of the security protocol on a CubeSAT candidate testbed of commercial off-the-shelf avionics for small satellites and a wider range of more powerful CPUs; and
(v) to provide recommendations for developing security mechanisms for opportunistic intersatellite operations in federated satellite systems in the Earth Observation domain, as a representative use case.

The remainder of this paper is structured as follows. Section 2 proposes a literature review discussing related work, including security research in satellite systems and the Copernicus Security Framework [3] in the Earth Observation domain. Section 3 describes the approach of this work: first, a stakeholder need analysis and a security problem discussion is conducted to identify satellite systems' stakeholders' security requirements for opportunistic intersatellite operations; then a security protocol for data relay addressing these requirements is formulated. Section 4 discusses security guarantees and presents an experimental characterisation of the computational and network overhead on a range of commercial platforms benchmarking results with performance data using the ECRYPT Benchmarking of Cryptographic Systems. Performance goals of the proposed protocol and platforms that achieve this goal are discussed. Section 5 provides the summary of the paper, lists limitations, states the contribution and discusses future work.

2. Literature review

This section presents an overview of security research in satellite systems and the Copernicus Security Framework (CSF) [3]. CSF is taken as a representative security policy for existing satellite systems, as applied to Earth Observation satellites. The framework addresses the ground segment security aspects only - therefore, the CSF framework will not be able to respond to all federated satellite systems' security requirements and regulate opportunistic intersatellite operations within federated satellite systems.

2.1. Security research in satellite systems

A thorough survey of the security and related issues in satellite systems, with both military and commercial destination of use, is discussed in Ref. [4]. The authors discuss authenticated key-exchange (AKE) protocols that could establish secure channels between spacecraft, explain why Internet Protocol Security (IPsec) [5], Transport Layer Security (TLS) [6], Transmission Control Protocol (TCP) [7] cause performance degradation when applied to satellite networks and list research directions (e.g., selective retransmission with User Datagram Protocol (UDP)) [8] towards the protocols' performance optimisation [4]. Distributed Denial of Service Attacks (DDOS) [9], its classification and detection, is discussed as one of the most harmful attacks in satellite communication networks; furthermore, an overview of the command link protection system deployed by the American Satellite Company (ASC) is given [4].

Security of satellite networks has mainly been researched in relation to mobile satellite communication and focused on efficient authentication, encryption and key update mechanisms, as discussed in Refs. [10] [11], and [12]. As mobile satellite communication systems provide real-time services, any additional time delay is critical for the systems' performance. The above work has been concentrated on minimising the computation overhead caused by the public key infrastructure (PKI) (PKI is introduced in Section 3.4.1).

Security parameters as fault management [13] [14] and multi-level security across applications [15] [13] [14] have defined a novel set of capabilities of fractionated spacecraft and spacecraft clusters. The distinctive and innovative characteristics of software platforms for distributed spacecraft are spatial and temporal isolation between missions and shared resources approached by running applications in isolated partitions [14] [16], fault isolation among applications [17], data isolation between different stakeholders based on security label checking and constrained information flow [14] [18].

Fault tolerant models and hardware implementations of cryptographic algorithms are other directions towards recovering spacecraft from failures and targeted attacks. Developing cryptographic primitives for a harsh space environment is challenging due to an increasing probability of single event upsets (SEUs). The PhD dissertation of Marcio Juliato [19] addresses fault tolerant cryptographic primitives for on-board security in spacecraft (i.e. SEUs-recovery techniques [20], SEU-resistant SHA-256 design [20]); a fault-tolerant model of AES was introduced by Ref. [21]; an SEUs-resistant FPGA-based implementation of the substitution transformation in AES was published by Ref. [22].

An example of an operational security framework that addresses unclassified satellite information security from its acquisition and storage to elaboration and distribution to the users is the Copernicus Security Framework [3] developed and deployed by the European Space Agency (ESA) to mitigate security risks within the Copernicus programme based on a threat assessment and Copernicus regulations [23] [3]. The focus of the framework is on the information security and access control: data integrity and availability and special data confidentiality are fundamental for services like emergency management or security surveillance.

The Copernicus Security Framework states data security as fundamental to many satellite systems' services. Currently the CSF framework addresses the ground segment security only, which motivates us to propose a security protocol for intersatellite operations within federated satellite systems.

3. Approach

This section describes the approach proposed in this paper. The approach is two-phased: first, a stakeholder analysis is conducted on a representative case of satellite operations to identify typical security needs; then a security protocol for data relay addressing such needs for federated satellite systems is formulated.

3.1. Federated satellite systems stakeholder need analysis

The stakeholder need analysis for federated satellite systems is prototyped and based on the stakeholder need analysis of the Copernicus Earth Observation system and extended to address the network's and stakeholders' specifics of federated satellite systems. The Copernicus Earth Observation system serves a representative use case: (i) Earth observation is among the most beneficial potential applications of federated satellite systems; and (ii) being under deployment at the time of writing of this paper, the Copernicus programme is representative of the needs of present and future Earth Observation missions, which are seen as promising customer candidates of federated satellite systems' services [1].