Preface: Security and Privacy for Space-Air-Ground Integrated Networks

Jiangzhou Wang1, Yue Gao2, Cheng Huang3, Haojin Zhu4
1 School of Engineering, University of Kent, Canterbury, CT2 7NT, UK
2 School of Computer Science, Fudan University, Shanghai 200433, China
3 Department of Electrical and Computer Engineering, University of Waterloo, Waterloo N2L 3G1, Canada
4 Department of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai 200030, China


Space-Air-Ground Integrated Networks, i.e., SAGINs, address the limitations of terrestrial networks by integrating satellites in various orbits, aerial drones, and ground networks to enhance network coverage and reliability. This integration aims to ensure seamless communication across vast and remote areas, significantly expanding the reach of network services. Additionally, SAGINs are designed to support a high degree of network resilience and adaptability, facilitating advanced applications such as real-time data processing and global internet connectivity.

However, SAGINs still face significant challenges in maintaining security and privacy. The inherent dynamic and decentralized nature of the networks makes them vulnerable to various cybersecurity threats, such as spoofing and unauthorized access. These vulnerabilities are exacerbated by the complex integration of different network layers and the continuous movement of satellites and drones. Moreover, the diverse protocols involved introduce multiple points of potential failure, increasing the difficulty of implementing a unified security framework. To effectively protect data and maintain privacy, SAGINs require robust secure approaches that can dynamically adapt to changing network conditions and threats, ensuring continuous protection across all network elements and interfaces. Based on the requirements, this special topic focuses on security and privacy for SAGINs, where four papers have been accepted for publication after undergoing rigorous reviews and revisions.

In the paper "Secure and Efficient Covert Communication for Blockchain-Integrated SAGINs [1]," the authors presented CC-BSAGINs, a novel covert communication scheme designed for blockchain-integrated SAGINs, which enhances both security and operational efficiency. The approach obviates the necessity for senders to manage cryptographic keys, through securely mapping covertly transmitted data onto blockchain transactions. Such a method not only simplifies key management but also ensures that ciphertext does not appear overtly within the network. Formal security validations and a thorough performance evaluation demonstrated the efficiency of CC-BSAGINs.

In the paper "Static Program Analysis for IoT Risk Mitigation in Space-Air-Ground Integrated Networks [2]," the authors proposed a novel static program analysis (SPA) technique utilizing zero-knowledge (2K) proofs to address security challenges in SAGINs. The method detects risky interactions among IoT devices without exposing sensitive source codes, thus preserving intellectual property and privacy. It resolves SPA and 2K system incompatibilities by developing a new programming language and abstract domain specifically for SAGINs, translating network algorithms into 2K-suitable arithmetic circuits. The technique was proven to effectively identify risks with minimal computational demand, marking a pioneering advancement in secure network analysis.

In the paper "Privacy-Preserving Location Authentication for Low-altitude UAVs: A Blockchain-based Approach [3]," the authors proposed an effective blockchain-based UAV authentication scheme. The scheme utilizes a distance bounding protocol to establish location proofs, ensuring UAV position authenticity. To protect UAV privacy, anonymous certificates and zero-knowledge proofs are also employed. Security analysis confirmed the scheme's robustness, while experiments demonstrated its efficiency and feasibility in real-world scenarios.

In the paper "Enabling Space-Air Integration: A Satellite-UAV Networking Authentication Scheme [4]," the authors proposed a secure authentication scheme for satellites and UAVs in the Space-Air integrated network scenarios, using elliptic curve public key cryptography and Chebyshev polynomial. The scheme was designed to

* Corresponding author (email: j.z.wang@kent.ac.uk)

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

© The Author(s)2024, published by EDP Sciences and China Science Publishing & Media Ltd.
security challenges like eavesdropping, tampering, and impersonation, in satellite networks with large propagation delays and unstable links. The proposed authentication method can achieve mutual authentication, identity anonymity, and resistance against various attacks, and show obvious advantages in signaling, bandwidth, and computational overhead compared to the state-of-the-art methods.

We believe that the papers in this special topic will be beneficial for both academic research and engineering practice. Lastly, we extend our thanks to all the authors for their valuable contributions to this special topic, and we are grateful to the editors and reviewers for their strong support and valuable assistance.

References


