Security and Safety, Vol. 3, E2024008 (2024)
https://doi.org/10.1051/sands/2024008
sands.edpsciences.org

Editorial

OPEN ACCESS

Preface: Security and privacy for space-air-ground integrated networks

Jiangzhou Wang[1,*], Yue Gao[2], Cheng Huang[2], and Haojin Zhu[3]

[1] *School of Engineering, University of Kent, Canterbury CT2 7NT, UK*
[2] *School of Computer Science, Fudan University, Shanghai 200438, China*
[3] *Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200030, China*

Received: 29 April 2024 / Revised: 29 April 2024/ Accepted: 30 April 2024 / Published online: 30 April 2024

Citation Wang JZ, Gao Y, Huang C and Zhu HJ. Security and privacy for space-air-ground integrated networks. Security and Safety 2024; **3**: E2024008. https://doi.org/10.1051/sands/2024008

Space-air-ground integrated networks (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 (ZK) 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 ZK system incompatibilities by developing a new programming language and abstract

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

domain specifically for SAGINs, translating network algorithms into ZK-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 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 on 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

[1] Li WJ, Zhang Y, He XY et al. Secure and efficient covert communication for blockchain-integrated SAGINs. Secur Saf 2024; **3**: 2024006. https://doi.org/10.1051/sands/2024006

[2] Deng HT, Liu T, Ma XC et al. Static program analysis for IoT risk mitigation in space-air-ground integrated networks. Secur Saf 2024; **3**: 2024007. https://doi.org/10.1051/sands/2024007

[3] Pan HC, Wang YS, Wang W et al. Privacy-preserving location authentication for low-altitude UAVs: A blockchain-based approach. Secur Saf 2024; **3**: 2024004. https://doi.org/10.1051/sands/2024004

[4] Li S, Cao J, Shi X et al. Enabling space-air integration‘: A satellite-UAV networking authentication scheme. Secur Saf 2024; **3**: 2023030. https://doi.org/10.1051/sands/2023030