Submission deadline– 30th March 2024

OPEN ACCESS

Call for Papers

Special Topic on

Security and Privacy for Space-Air-Ground Integrated Networks

Guest Editors:

➢ **Jiangzhou WANG**, University of Kent, UK
➢ **Yue GAO**, Fudan University, China
➢ **Cheng HUANG**, University of Waterloo, Canada
➢ **Haojin ZHU**, Shanghai Jiaotong University, China

Call for Papers

Special Topic on

Security and Privacy for Space-Air-Ground Integrated Networks

Background

Although widely established and providing numerous valuable services, terrestrial networks, such as mobile networks, have geographic and deployment cost limitations due to the high reliance on fixed-ground infrastructure. Hence, space-air-ground integrated networks (SAGINs) have been proposed to increase network intelligence, enhance network reliability, and offer ubiquitous wireless coverage via satellite networks including Geosynchronous Orbit (GSO), Geostationary Equatorial Orbit (GEO), Medium Earth Orbit (MEO) and Low Earth Orbit (LEO) satellites, aerial networks (e.g., drone networks), and ground networks (e.g., mobile networks). SAGINs are envisioned to support various promising IoT applications and multimedia services and satisfy the high demands of seamless communications and network Quality of Services (QoS).

Under a hybrid and heterogeneous network architecture, one of the most crucial challenges faced by SAGINs is dealing with security and privacy vulnerabilities and improving system availability. Diverse and unpredictable malicious attacks, such as spoofing attacks and unauthorized access, can seriously decrease the feasibility of SAGINs and cause immeasurable negative consequences on services relying on SAGINs. Even though conventional cryptographic primitives could be utilized to design secure and privacy-preserving solutions for protecting SAGINs, they suffer from inevitable deficiencies, i.e., cryptographic primitives, e.g., encryption and signature, are always heavy in terms of computational and communication overheads and cannot adapt to delay-sensitive services. Other solutions that exploit lightweight techniques, including differential privacy, trusted hardware, and Artificial Intelligence, are also possible while constructing such a unified security and privacy-preserving system for SAGINs is challenging. Moreover, SAGINs naturally require decentralized and dynamic network slicing, data management, and service deployment, considering that networking entities like LEO satellites, drones, and users move constantly. Thus, centralized frameworks may not be applied to SAGINs, and decentralized security and privacy-preserving frameworks such as blockchain could be a potential research direction. Overall, the security and privacy studies for SAGINs are essential but still under-explored.

Aims and Scope of the Special Topic

This special topic aims to provide a collection of high-quality research papers on "Security and Privacy for Space-Air-Ground Integrated Networks". Both theoretical and experimental contributions are encouraged. Potential topics include but are not limited to the following:

- Zero-trust security models for SAGINs
- Security and privacy frameworks for SAGINs
- Lightweight secure and privacy-preserving techniques for SAGINs
- Trust management and evaluation models for SAGINs
- AI-enhanced security techniques for SAGINs
- Secure communication systems for SAGINs
- Zero-trust network security architectures for SAGINs
- Physical-layer security techniques for SAGINs
- Key and certificate management for SAGINs
- Zero-trust access control methods for SAGINs
- Post-quantum security techniques for SAGINs
- Malware and intrusion detection solutions for SAGINs
- Zero-trust data management and processing models for SAGINs
- Simulation test bed for attacks and defences on SAGINs

Submissions

Authors should submit their manuscripts online directly at: https://sands.nestor-edp.org and choose, during submission, the special topic: **Security and Privacy for Space-Air-Ground Integrated Networks**. All relevant papers will be carefully considered and peer-reviewed by a distinguished team of international experts. The instructions for authors are detailed at: https://sands.edpsciences.org/author-information/instructions-for-authors.

Submission deadline – 30th March 2024

Article Processing Charges - S&S is an Open Access journal and no APCs in 2024.

Guest Editors

Jiangzhou WANG, University of Kent, UK, j.z.wang@kent.ac.uk
Yue GAO, Fudan University, China, gao_yue@fudan.edu.cn
Cheng HUANG, University of Waterloo, Canada, c225huan@uwaterloo.ca
Haojin ZHU, Shanghai Jiaotong University, China, zhu-hj@cs.sjtu.edu.cn

Contact **Yuanyuan LIU,** *Security and Safety* Editorial Office, sands@edpsciences.org

Guest Editor Biographies

Jiangzhou WANG is a Professor with the University of Kent, U.K. He has published more than 400 papers and four books. His research focuses on mobile communications. He was a recipient of the 2022 IEEE Communications Society Leonard G. Abraham Prize and IEEE Globecom2012 Best Paper Award. He was the Technical Program Chair of the 2019 IEEE International Conference on Communications (ICC2019), Shanghai, Executive Chair of the IEEE ICC2015, London, and Technical Program Chair of the IEEE WCNC2013. He is/was the editor of a number of international journals, including IEEE Transactions on Communications from 1998 to 2013. Professor Wang is a foreign academician of the CAE, Fellow of the Royal Academy of Engineering, U.K., Fellow of the IEEE, and Fellow of the IET. He is currently an associate Editor-in-Chief of *Security and Safety* (S&S).

Yue GAO received a PhD from the Queen Mary University of London (QMUL), U.K., in 2007. He is a Professor at the School of Computer Science, Fudan University, China, and a Visiting Professor at the University of Surrey, U.K.. He worked as a Lecturer, a Senior Lecturer, a Reader and the Chair Professor with QMUL and the University of Surrey, respectively. He has published over 200 peer-reviewed journal and conference papers and had over 6600 citations. His research interests include smart antennas, sparse signal processing and cognitive networks for mobile and satellite systems. He was a co-recipient of the EU Horizon Prize Award on Collaborative Spectrum Sharing in 2016 and elected an Engineering and Physical Sciences Research Council Fellow in 2017. He is a member of the Board of Governors and a Distinguished Speaker of the IEEE Vehicular Technology Society (VTS), the Chair of the IEEE ComSoc Wireless Communication Technical Committee, and the Past Chair of the IEEE ComSoc Technical Committee on Cognitive Networks. He has been an Editor of several IEEE Transactions and Journals, the Symposia Chair, the Track Chair, and other roles in the organizing committee of several IEEE ComSoC, VTS, and other conferences. He is currently an associate Editor of *Security and Safety* (S&S).

Cheng HUANG is currently a Postdoctoral Research Fellow with the Department of Electrical and Computer Engineering, University of Waterloo. He received his B.Eng and M.Eng in information security from Xidian University, China, in 2013 and 2016 respectively, and received the Ph.D. degree in Electrical and Computer Engineering, University of Waterloo, ON, Canada in 2020. His research interests are in the areas of security and privacy in vehicular networks and databases. He has published more than 50 high-reputation journal and conference papers, including IEEE Transactions on Vehicular Technology, IEEE Communication Magazine, and ACM ASIACCS, and obtained 3 Best Paper Awards in IEEE ICC, GLOBECOM, and ICCC. His Google citation is more than 1200 with h-index 19.

Haojin ZHU is currently a Professor with Department of Computer Science and Engineering, Shanghai Jiao Tong University, China. I received my B.Sc. degree (2002) from Wuhan University (China), M.Sc.(2005) degree from Shanghai Jiao Tong University (China), both in computer science and the Ph.D. in Electrical and Computer Engineering from the University of Waterloo (Canada), in 2009. He published more than 70 journals, including: JSAC, TDSC, TPDS, TMC, TIFS, TWC, TVT and more than 90 international conference papers, including IEEE S&P, ACM CCS, USENIX Security, ACM MOBICOM, NDSS, ACM MOBIHOC, IEEE INFOCOM, IEEE ICDCS. He received ACM CCS Best Paper Runner-Ups Award (2021), IEEE TCSC Excellence in Scalable Computing (Middle Career Researcher, 2020) Natural Science Award of Ministry of Education (first class, 2018), JSPS Invitational Short-term Fellowships for Research (2017), IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award (2014), Top 100 Most Cited Chinese Papers Published in International Journals (2014), Supervisor of Shanghai Excellent Master Thesis, and best paper awards of IEEE ICC 2007, Chinacom 2008 and best paper award runner up for Globecom 2014, WASA 2017. He is a Fellow of IEEE.