* **Title of the tutorial**

Security for Space-Air-Ground Integrated Networks

* **Tentative schedule of the tutorial: Half-day**
* **Name, affiliation, and the short biography**

Professor Jiajia Liu

School of Cybersecurity,

Northwestern Polytechnical University, China

Associate Professor Hongzhi Guo

School of Cybersecurity,

Northwestern Polytechnical University, China

**Jiajia Liu** (S’11-M’12-SM’15) received his B.S. and M.S. degrees both in computer science from Harbin Institute of Technology in 2004 and from Xidian University in 2009, respectively, and received his Ph.D. degree in information sciences from Tohoku University in 2012. He was a JSPS special research fellow in Tohoku University from Apr. 2012 to Oct. 2013, and a data analytics engineer in Aviation Industry Corporation of China from Jul. 2004 to Aug. 2006. He was a Full Professor at the School of Cyber Engineering, Xidian University from 2013 to 2018, and the director of Internet of Things Security Research Center, Xidian Univ from 2016 to 2018. Since Jan. 2019, he has been a full professor at the School of Cybersecurity, Northwestern Polytechnical University. He was selected into the “Huashan Scholars” program by Xidian University in 2015.

He has published more than 130 peer-reviewed papers in many high quality publications, including prestigious IEEE journals and conferences. He received IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award in 2017, IEEE TVT Top Editor Award in 2017, the Best Paper Awards from many international conferences including IEEE flagship events, such as IEEE GLOBECOM in 2016, IEEE WCNC in 2012 and 2014, IEEE IC-NIDC in 2018. He was the recipient of the prestigious 2012 Niwa Yasujiro Outstanding Paper Award due to his exceptional contribution to the analytics modeling of two-hop ad hoc mobile networks, which has been regarded by the award committees as the theoretical foundation for analytical evaluation techniques of future ad hoc mobile networks. He was also a recipient of the Tohoku University President Award 2013, Graduate School of Information Sciences Dean Award 2013, Professor Genkuro Fujino Award 2012, Chinese Government Award for Outstanding Ph.D. Students Abroad 2011 and the RIEC Student Award 2012.

His research interests cover a wide range of areas including wireless and mobile ad hoc networks, space-air-ground integrated networks, intelligent and connected vehicles, mobile/edge/cloud computing and storage, Internet of things security, and 5G. He has been actively joining the society activities, like serving as associate editors for IEEE Transactions on Wireless Communications (May 2018-present), IEEE Transactions on Computers (Oct. 2015-Jun. 2017) and IEEE Transactions on Vehicular Technology (Jan. 2016 - present), editor for IEEE Network (July 2015-present), editor for IEEE Transactions on Cognitive Communications and Networking (January 2019-present), guest editors of top ranking international journals like IEEE Transactions on Emerging Topics in Computing (TETC), IEEE Network Magazine, IEEE Internet of Things (IoT) Journal, etc., and serving as technical program committees of numerous international conferences like the leading symposium co-chair of AHSN symposium for GLOBECOM 2017, CRN symposium for ICC 2018, AHSN symposium for ICC 2019. He is the Secretary of IEEE AHSN TC, and is a Distinguished Lecturer of the IEEE Communications Society.

**Hongzhi Guo** (S'08-M'16) received his B.S. degree in computer science and technology from Harbin Institute of Technology in 2004, M.S. and Ph.D. degrees in computer application technology from Harbin Institute of Technology Shenzhen, China, in 2006 and 2011, respectively. He is currently an Associate Professor with the School of Cybersecurity, Northwestern Polytechnical University. He was a Lecturer with the School of Cyber Engineering, Xidian University, from 2012 to 2018.

During the past three years, he has published more than 20 peer-reviewed papers in many high quality publications, including prestigious IEEE journals and conferences such as IEEE IVT, IEEE IoT Journal, IEEE TETC, IEEE Communications Surveys and Tutorials, IEEE Communications Magazine, IEEE NETWORK, IEEE Wireless Communications Magazine, IEEE Vehicular Technology Magazine, IEEE Communications Letters, IEEE GLOBECOM, IEEE ICC, etc. His research interests cover a wide range of areas including MEC, FiWi, UDN, Big Data and Cloud Computing Security, and IoT Security. He has been actively joining the society activities, like serving as an editor of the International Journal of Multimedia Intelligence and Security (Mar. 2018 - present), reviewers for IEEE TVT, IEEE TWC, IEEE NETWORK, IEEE IoT Journal, IEEE TNSM, IEEE TETC, IEEE Communications Magazine, IEEE TCCN, IEEE Vehicular Technology Magazine, etc.

* **A description of the technical issues that the tutorial will address, emphasizing its timeliness**

Space-air-ground integrated network (SAGIN), as an integration of satellite systems, aerial networks, and terrestrial communications, has been becoming an emerging architecture and attracted intensive research interest during the past years. In consideration of the inherent advantages in terms of large coverage, high throughput and strong resilience, SAGIN can be used in lots of practical fields, including earth observation and mapping, intelligent transportation system (ITS), military mission, disaster rescue, and so on. SAGIN security, as an important part of cyberspace security, is not only relevant to individual users, but also to national security strategy, and its importance is self-evident.

This tutorial is going to discuss the problem of security and privacy protection in SAGIN, including commonly-used attack methods and safety protection technologies. In particular, the following important issues will be covered in this tutorial.

* + **SAGIN features and open challenges:** As an integration of satellite systems, aerial networks, and terrestrial communications, SAGIN has its own features, and meanwhile, a large number of new challenges emerge in consideration of its complex components, multiple networking techniques, and intricate user and data management. It is significantly necessary and important to emphasize SAGIN architecture, features, and emerging challenges.
	+ **SAGIN security threats:** To protect SAGIN safety, it is strongly necessary to understand and investigate existing attack methods against SAGIN or parts of it. In this part, we partition existing attack techniques, including jamming, masquerader attack, passive eavesdropping, message injection, etc., into three areas, corresponding to the three layers of SAGIN security, i.e., physical security, operational security, and data security.
	+ **Countermeasures & Solutions:** In view of the security requirements of SAGIN, diverse security and privacy protection have been proposed over the past few years. In this part, we first present different security countermeasures against existing SAGIN security threats, including anti-jamming, authentication mechanisms, secure routing and handover, secret key management, etc. After that, the pros and cons of existing solutions are summarized.

In light of its timeliness and the opening research issues listed above, we believe this topic will be of great interest for AICON 2019 and will attract lots of attention from both academia and industry.

* **An outline of the tutorial content, including its tentative schedule**

The outline of the tutorial is as follows:

1. **Space-Air-Ground Integrated Networks**
	1. **Background**
	2. **SAGIN architecture**
	3. **Features & Challenges**
2. **SAGIN Security Threats**
	1. **Physical threats**
		1. **Staffers espionage**
		2. **Irresistible environment factors**
		3. **Signal interference**
		4. **Equipment resource depletion**
	2. **Operation threats**
		1. **Unauthorized access**
		2. **Bypass control**
		3. **Masquerader**
		4. **Implantable threats**
	3. **Network threats**
		1. **False routing**
		2. **Service spoofing**
		3. **Network eavesdropping**
		4. **Unsafe protocol**
	4. **Data/Information security threats**
		1. **Message modification**
		2. **Information leak**
		3. **Data misuse**
		4. **Message injection**
	5. **Other Security Issues**
3. **Attack Methodologies**
	1. **Jamming Attack**
	2. **Side Channel Attack**
	3. **Spoofing Attack**
	4. **Replay Attack**
	5. **Protocol Manipulation Attack**
	6. **Data falsification Attack**
	7. **Denial Of Service**
	8. **Active Attacks on Handover**
4. **Countermeasures & Solutions**
	1. **Physical security countermeasures**
		1. **Backup and Restore**
		2. **Insider Security Work Strengthening**
		3. **Anti-jamming Techniques**
	2. **Operation security countermeasures**
		1. **Authentication schemes**
		2. **Intrusion Detection**
	3. **Network security countermeasures**
		1. **Network Structure Optimization**
		2. **Secure Routing Algorithms and Protocols**
		3. **Handover Management Schemes**
	4. **Data/Information security countermeasures**
		1. **Secret key management**
		2. **Secure transport protocol**
	5. **Other New Technologies**
5. **Discussions & Challenges Ahead**
* **A description of previous tutorial experience of the speaker(s), and past versions of the tutorial**

(1) Jiajia Liu, “Ultra-dense Heterogeneous Small Cell Deployment in 5G and Beyond: A Tutorial on QoE Provisioning,” IEEE GLOBECOM 2017, Singapore, 4-8 December 2017. (**tutorial**)

(2) Jiajia Liu, “Advanced Ad Hoc and Mesh Networks: From Theoretical to Practical,” IEEE International Conference on Communications (ICC 2016), Kuala Lumpur, Malaysia, 23-27 May 2016. (**tutorial**)

(3) Jiajia Liu, “Advanced Ad Hoc and Mesh Networks: From Theoretical to Practical,” IEEE International Conference on Communications in China (ICCC 2015), Shenzhen, China, Nov. 2015. (**tutorial**)

(4) Jiajia Liu, “Fundamental Performance Analysis in Mobile Ad Hoc Networks,” Qufu Normal University, Rizhao, Shandong, December 19-20, 2015. (**invited lecture**)

(5) Jiajia Liu, “Cooperative Jamming in Wireless Networks with Eavesdroppers at Arbitrary Locations,” Qingdao, Shandong, November 2015. (**invited lecture**)

(6) Jiajia Liu, “Device-to-Device Communication for Load Balancing and Coverage Extension in LTE-Advanced Networks,” Zhejiang University of Technology, May 2014. (**invited lecture**)

(7) Jiajia Liu, “Device-to-Device Communication for Load Balancing and Coverage Extension in LTE-Advanced Networks,” A3 Annual Workshop on Next Generation Internet and Network Security, Busan, Korea, Feb. 2015. (**keynote**)

(8) Jiajia Liu, “Study on Fundamental Performance Analysis in Mobile Ad Hoc Networks,” Zhejiang University of Technology, Dec. 2014. (**invited lecture**)

(9) Jiajia Liu, “Performance Modeling and Analysis for Mobile Ad Hoc Networks,” Shaanxi Normal University, May 2014. (**invited lecture**)

(10) Jiajia Liu, “Delay and Capacity in Ad Hoc Mobile Networks with f-cast Relay Algorithms,” Tokyo Denki University, Feb. 2013. (**keynote**)