上海交通大学自动化系
Department of Automation
Shanghai Jiao Tong University

系统控制与信息处理教育部重点实验室
Key Laboratory of System Control and Information Processing, Ministry of Education

学术报告会

时间：2023年4月25日 10:00-11:00
地点：电信群楼2-410会议室

Privacy-preserving decentralized federated learning over time-varying communication graph

路洋

Lecturer (Assistant Professor) , Lancaster University

摘要:

Establishing how a set of learners can provide privacy-preserving federated learning in a fully decentralized (peer-to-peer, no coordinator) manner is an open problem. We propose the first privacy-preserving consensus-based algorithm for the distributed learners to achieve decentralized global model aggregation in an environment of high mobility, where participating learners and the communication graph between them may vary during the learning process. In particular, whenever the communication graph changes, the Metropolis-Hastings method is applied to update the weighted adjacency matrix based on the current communication topology. In addition, the Shamir's secret sharing scheme is integrated to facilitate privacy in reaching consensus of the global model. The correctness and privacy properties of the proposed algorithm are theoretically analyzed. The computational efficiency is evaluated by a simulation built on a federated learning framework with a real-world dataset.

简介:

Yang Lu is a Lecturer (Assistant Professor) of the Systems Security Group in the School of Computing and Communications at the Lancaster University. He received Ph.D. degree in Electrical Engineering from the Pennsylvania State University (PSU) in 2020, B.E. and M.E. degrees in Electrical Engineering from Shanghai Jiao Tong University in 2010 and 2013, respectively, and M.S. degree in Electrical Engineering from the Georgia Institute of Technology, in 2013. From September 2020 to August 2021, he worked as a postdoctoral scholar in the School of Electrical Engineering and Computer Science at PSU. From January 2019 to May 2019, he worked as a Ph.D. intern at the Pacific Northwest National Laboratory. From March 2013 to June 2014, he worked as a visiting scholar in the School of Electrical and Computer Engineering at the Georgia Institute of Technology. His research interests mainly focus on cyber-physical privacy and security, distributed control and optimization of multi-agent networks, and machine learning. He is a recipient of the Dr. Nirmal K. Bose Dissertation Excellence Award at PSU in 2019, and a winner of Best Paper Award of MSN 2022 (The 18th International Conference on Mobility, Sensing and Networking).