A Survey of Security Aggregation

Sufang Zhou*, Mingzhe Liao*, Baojun Qiao*, Xiaobo Yang**

**School of Computer and Information Engineering, Henan University, Kaifeng 475004, China*

**China United Network Communication Corporation Henan Branch, Zhengzhou 450003, China

zsf@henu.edu.cn, 326995871@qq.com, qiaobaojun2009@163.com, yangxb72@chinaunicom.cn

Corresponding author: qiaobaojun2009@163.com

***Abstract*—Machine learning (ML) requires the collection of large amounts of data to train robust predictive models. Federated learning (FL) allows sensitive data to be kept on the client side to train a shared model, but shared models still pose privacy concerns. Secure aggregation is an important algorithm for securing federation learning by being able to compute the sum of client-side model updates without revealing information about individual client updates. In this study, we investigate the results of secure aggregation protocols in recent years and review the research results in the field of secure aggregation according to secret sharing, differential privacy, and homomorphic encryption mechanisms. On this basis, we compare and analyze the advantages and disadvantages of different mechanisms and then evaluate the security aggregation protocols in terms of security, dynamic user robustness, computational cost, and communication cost. Finally, we provide an outlook on the future development of secure aggregation protocols and give possible future research directions.**

***Keyword*—Federated Learning, Security Aggregation, Secret Sharing, Differential Privacy, Homomorphic Encryption**

Sufang Zhou received the B.S. degree in computer science from Henan Normal University in 2013, and the Ph.D. degree in computer software and theory from Shaanxi Normal University in 2019. She is currently a master supervisor within the School of Computer and Information Engineering, Henan University. Her research interests include secure multiparty computation, privacy-preserving machine learning.

Mingzhe Liao is currently an undergraduate student at Henan University. His research interests include secure multiparty computation and security aggregation.

Qiao Baojun, Professor, doctoral supervisor, Dean of School of computer and information engineering, Henan University. He obtained a doctoral degree in computer software and theory from Beijing University of technology in 2007. At present, his main research directions include spatial data analysis, software engineering and privacy-preserving distributed computing.

Xiaobo Yang received a master degree in computer software and theory from Shaanxi Normal University in 2016. He is currently a senior engineer within the China United Network Communication Corporation Henan Branch. Her research interests include network security, distributed computing.