Privacy and Security in Distributed Graph Analytics: Secure Distributed k-Core Decomposition

Bin Guo*

Department of Computing & Information Systems
Trent University, Ontario, Canada, K9L 0G2
binguo@trentu.ca

Abstract

As one of the most well-studied cohesive subgraph models, the k-core is widely used to find graph nodes that are "central" or "important" in many applications, such as biological networks, social networks, ecological networks, and financial networks. For distributed networks, e.g., Decentralized Online Social Networks (DOSNs) such that each vertex is a client as a single computing unit, the distributed k-core decomposition algorithms are already proposed. However, traditional distributed approaches do not adequately protect privacy and security. In today's data-driven world, data privacy and security have attracted more and more attention, e.g., DOSNs are proposed to protect privacy by storing user information locally without using a single centralized server. In this work, we are the first to propose the secure version of the distributed k-core decomposition.

1 Introduction

The k-core is the maximal subgraph in which each vertex has a degree of at least k; and the core number of each vertex is the maximum value of k contained in the k-core [2]. Due to its linear running time [2], the k-core has many applications. For distributed networks, e.g., Decentralized Online Social Networks (DOSNs) [3] such that each vertex is a client as a single computing unit, the distributed k-core decomposition is proposed to calculate the core numbers of vertices.

However, traditional distributed approaches [4] do not adequately protect privacy and security [5]; for example, each client can leak privacy to neighbors, and the centralized server can collect all clients' information. In today's data-driven world, data privacy and security have attracted more and more attention, e.g., DOSNs are proposed to protect privacy by storing user information locally without using a single centralized server. In this work, we are the first to propose the secure distributed k-core decomposition.

*This talk is based on the joint work with Emil Sekerinski and Lingyang Chu at McMaster University

2 Contributions

We have three main contributions:

- For each vertex, Homomorphic Encryption (HE) [1] is applied to *compare the core numbers* with neighbors without leaking the specific values of the core numbers.
- A decentralized approach is applied for the *termination detection* of distributed decomposition without collecting all vertices' information.
- When releasing the result of all vertices' core numbers after termination, we only calculate the *distribution of vertices* (based on the core numbers and labels), without releasing the specific values of the core numbers and labels for any vertices, since most applications only require the statistical analysis of core numbers.

The methodology can be applied to distributed k-core maintenance algorithms to enhance privacy and security. Additionally, it can be extended to distributed k-truss decomposition and maintenance algorithms.

References

[1] Abbas Acar, Hidayet Aksu, A Selcuk Uluagac, and Mauro Conti. A survey on homomorphic encryption schemes: Theory and implementation. *ACM Computing Surveys (Csur)*, 51(4):1–35, 2018.

[2] Vladimir Batagelj and Matjaz Zaversnik. An o(m) algorithm for cores decomposition of networks. *CoRR*, cs.DS/0310049, 2003.

[3] Giuliano Mega, Alberto Montresor, and Gian Pietro Picco. Efficient dissemination in decentralized social networks. In *2011 IEEE International Conference on Peer-to-Peer Computing*, pages 338–347. IEEE, 2011.

[4] Alberto Montresor, Francesco De Pellegrini, and Daniele Miorandi. Distributed k-core decomposition. *IEEE Transactions on Parallel and Distributed Systems*, 24(2):288–300, 2013.

[5] Merav Parter and Eylon Yogev. Distributed algorithms made secure: A graph theoretic approach. In *Proceedings of the Thirtieth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1693–1710. SIAM, 2019.