Título: Differentially Private Release of Count-Weighted Graphs

Data: 03/08/2023

Horário: 14:00h

Local: Sala de Seminários - Bloco 952

Resumo:

Many complex natural and technological systems are commonly modeled as count-weighted graphs, where nodes represent entities, edges model relationships between them and edge weights define some counting statistics associated with each relationship. As graph data usually contain sensitive information about entities, preserving privacy when releasing this type of data becomes an important issue. In this context, differential privacy (DP) has become the de facto standard for data release under strong privacy guarantees. When dealing with DP for weighted graphs, most state-of-the-art works assume that the graph topology is known. However, in several real- world applications, the privacy of the graph topology also needs to be ensured. In this paper, we aim to bridge the gap between DP and count-weighted graph data release, considering both graph structure and edge weights as private information. We first adapt the weighted graph DP definition to take into account the privacy of the graph structure. We then develop two novel approaches to privately releasing count-weighted graphs under the notions of global and local DP. We also leverage the post-processing property of DP to improve the accuracy of the proposed techniques considering graph domain constraints. Experiments using

real-world graph data demonstrate the superiority of our approaches in terms of utility over existing techniques, enabling subsequent computation of a variety of statistics on the released graph with high utility, in some cases comparable to the non-private results.

Banca:

- Prof. Dr. Javam de Castro Machado (MDCC/UFC - Orientador)
- Prof. Dr. César Lincoln Cavalcante Mattos (UFC)
- Profa. Dra. Mirella M. Moro (UFMG)
- Prof. Dr. Divesh Srivastava (AT&T Labs-Research - USA)
- Prof. Dr. Carlos Eduardo Santos Pires (UFCG)