STEVENS
INSTITUTE OF TECHNOLOGY
1870

Ph.D. DISSERTATION DEFENSE

Candidate: Xiuling Wang
Degree: Doctor of Philosophy
School/Department: Charles V. Schaefer, Jr. School of Engineering and Science, Department of Computer Science
Date: Tuesday, May 7th, 2024
Time/Location: 10:30 AM EDT
Gateway North 303

Title: Trustworthy Graph Learning

Chairperson: Dr. Wendy Hui Wang, Department of Computer Science, Stevens Institute of Technology

Committee Members: Dr. Yue Ning, Department of Computer Science, Stevens Institute of Technology
Dr. Tian Han, Department of Computer Science, Stevens Institute of Technology
Dr. Violet Chen, School of Business, Stevens Institute of Technology

ABSTRACT

Graph learning is a rapidly growing field in machine learning. Despite its success, there are several concerns about the trustworthiness of graph learning models. In my research, I focus on two important issues in trustworthy graph learning: fairness and privacy. Fairness aims to mitigate bias introduced or amplified during the learning process. Privacy requires that the privacy of the data and model parameters, which are regarded as confidential information belonging to their owners, should be protected.

In terms of fairness, we focus on fairness in social network analysis and deep recommender systems. For social network analysis, we formalize the definition of bias in link prediction by providing quantitative measurements of accuracy disparity. And we design the methods to mitigate the bias based on the unfairness definition. For deep recommender systems, we define a new notion of individual fairness from the perspective of items to deal with item popularity bias in recommendations. We design two bias mitigation methods, namely embedding-based re-ranking and greedy substitution, that can achieve individual fairness on deep recommender systems.

Regarding privacy, we propose three types of attacks, property inference attacks against GNNs by which the attacker can infer the sensitive properties of nodes and links in the training graph, link membership inference attacks against unsupervised graph learning and graph contrastive learning models, in which the attacker aims to infer the presence of a particular edge in the training graph, subgraph membership inference attack against GNNs that the attacker attempts to infer whether a given node set corresponds to a k-clique or (k-1)-hop path or neither in the training graph. Furthermore, we design new defense mechanisms to defend against these attacks.