NATIONAL UNIVERSITY OF SINGAPORE

School of Computing

PH.D DEFENCE - PUBLIC SEMINAR

Title: ON THE PRIVACY AND UTILITY OF SOCIAL NETWORKS

Speaker:	Ms Song Yi
Date/Time:	19 September 2014, Friday, 04:00 PM to 05:30 PM
Venue:	Executive Classroom, COM2-04-02
Supervisor :	Dr Stephane Bressan, Associate Professor, School of Computing

Abstract:

The connectedness of social networks inspires the study of social networks for applications in various fields such as sociology, marketing and biology. Online Social Network Sites (SNSs) allow users to discover and share information about themselves and their peers. Data that is produced on a large scale from these networks brings challenges to the exploration of data utility, as well as the protection of data privacy.

We look into both problems from a graph perspective. In particular, we focus on community detection and graph anonymization. Graphs analyses facilitate the study of relationships or social interactions of online social networks modeled as graphs. Community detection constitutes an important tool for the analysis, by exploring the network structure and associated information. It provides insights into the network characteristics and structural properties, and thus, the social phenomena that take place. On the other hand, to protect data from private information disclosure, prevent malicious use and to ease the user concerns, graph anonymization approaches are in demand. Graph anonymization approaches perturb graphs under certain constraints such that the released data has a certain level of guaranteed privacy or data utility.

In this thesis, we discuss the concepts, related works and the problems of graph anonymization and community detection. We then design algorithms to solve the problems, respectively.

First, we study the problem of graph anonymization that protects the privacy of sensitive information in social network data. The target is to perturb the structures of naive anonymized graphs in such a way that, after anonymization, the graphs are capable of resisting attacks and preserving users' privacy. We study the shortcomings of an existing state-of-the-art algorithm and propose a heuristic algorithm that not only overcomes the shortcomings, but also improves the effectiveness and, most importantly, the efficiency of large graphs. Next, we propose a user-centric utility-driven paradigm, as opposed to the

commonly used privacy-driven paradigm, and an algorithm that anonymizes graphs with a utility guarantee, while certain graph properties are preserved. We aim to offer an informative view of the network for users while resisting certain structural attacks.

Second, we study the problem of community detection on a simple graph that explores beneficial knowledge, based on the graph structures underlying social networks. The target is to discover structural communities utilizing various graph properties. We propose three algorithms that detect communities based on a wide range of graph structural properties, including the degree and clustering coefficient, closeness among the vertices, and the physical forces among the vertices when simulating the whole graph as a physical system, respectively. Through a comprehensive experimental study on both the real world network and synthetic data sets, the proposed solutions are shown to be efficient and effective.