Abstract

31% of global population use online social networks. These people can be from any class or may be very powerful, or may be world famous personnel, who are very likely to be stalked for inferring private information or people exploiting their privacy. For a better revenue, when any social networking sites sell these huge volume of data for either data mining or analysis to any third party organizations, the privacy of the users are put in danger. Naive anonymization is not effective enough to prevent most of the strategic attacks. Structural attack is kind of strategic attack. Here, using the structural knowledge available to the adversary, he can identify or infer some useful information about individual from a published anonymized social network graph. The available anonymization algorithms to prevent the structural attack are either insufficient or they degrades the data mining quality of the graph. So we consider preserving the data mining quality of the graph while eliminating most vulnerable edges under attack. We develop a privacy preserving strategy based on ant colony optimization which is a type of swarm robot intelligence algorithm. We test this algorithm in some publicly available social graphs for checking the quality of the graph before and after anonymization using some known parameter of graphs.
References


Index Terms

Computer Science

Algorithms

Keywords
Social Network Graph; Perturb Graph; Anonymization; Structural Attack; Ant Colony Optimization.