Abstract

Social networking sites are extensively useful for communicating with the real world. The conversation among these sites accomplishes an extreme amount of data in the network. These large amount of data contain vulnerable information that is sharing between social users through links or edges. A broad use of social network creates security and privacy issues of a network. Many of social users unguarded about the risks, which caused by extrovert their sensible data, make network bunch for identity, and link disclosure. Simply the privacy of users is preserve by removing the identified element of users but it is not enough for user's privacy through attacks, which have some prior knowledge about users. This paper mainly concerned with friendship and structural attack on user's privacy, which disclose user's identity and link information. Detailed analysis is done regarding k2-degree and k-automorphism methods for protecting the privacy from these attacks and the utility such as average shortest path and cluster coefficient were also calculated for these two method.

References
C. C. Aggarwal (Ed.), social network data analysis, DOI 10.
1007/978-1-4419-8462-3_10, @ Springer Science+Business Media, LLC 2011.

Index Terms

Computer Science Information Sciences

Keywords

Social network k2-degree k-automorphism Anonymization.