To Protect Sensitive Labels in Social Network Data Anonymization

Miss Pradnya L. Sangade
PG Student, Computer Department, JSMP's BSIOTR,Wagholi,Pune

Prof. Nitin Shivale
Assistant Professor, Computer Department, JSMP's BSIOTR,Wagholi,Pune

***Abstract-*: Privacy is very important thing when publishing and sharing large amount of data. Researchers have developed various privacy models, but these privacy models does not protect sensitive labels, these privacy models are enforced, an attacker may still be able to infer one's private information if a group of nodes largely share the same sensitive labels. The label-node relationship is not well protected. This paper define k-degree-l-diversity anonymity model that consist of protection of structural information as well as sensitive labels. Here purpose a novel anonymization methodology based on adding noise nodes. We develop a new algorithm by adding noise nodes into the original graph with the consideration of introducing the least distortion to graph properties.**

***Index Terms*- privacy, sensitive labels, anonymization, and social network**

I. INTRODUCTION

The publication of social network data entails a privacy threat for their users. Sensitive information about users of the social networks should be protected. The challenge is to devise methods to publish social network data in a form that affords utility without compromising privacy. Previous research has proposed various privacy models with corresponding protection mechanisms that prevent both inadvertent private information leakage and attacks by malicious adversaries. These early privacy models are mostly concerned with identity and link disclosure. The social networks are modeled as graphs in which users are nodes and social connections are edges. This paper is motivated by to protect the sensitive label.

Users entrust social networks such as Facebook and LinkedIn with a wealth of personal information such as their age ,address, current location or political orientation. We refer to these details and messages as features in the user's profiles .An individual user can select which features of her profile she wishes to conceal.

II. SURVEY ON ANONYMIZATION TECHNIQUES

An anonymization technique prevents node replication attacks. The goal is to publish a social graph, in order to protect privacy. Recent approaches for protecting social graph privacy are edge editing and clustering method. Edge-editing method keep the nodes unchanged and by increasing or decreasing or by swapping edges of original graph. The edge editing method substantially changes the distance of node properties by linking faraway nodes together or breaking the bridge link of two communities. Clustering method which often merges a sub graphs to super nodes. Otherwise grouping of "similar" nodes as super nodes. The super node represents a "cluster". Then linking between nodes are refers as the edges in between super nodes called "super edges." Each super edge describes more edges in the original graph.

The framework presentation for analyzing privacy preservation develops a new reidentification algorithm for target of various anonymized social network graphs. Our Deanonymization algorithm is based on network topology, does not contain creation of more number of dummy "Sybil" nodes. Existing defenses works between the overlapping of target network and adversary's information. A generic reidentification algorithm showed that it can successfully monitors and de-anonymize lot of users in anonymous social network graph. Since human names has not unique identity, this algorithm having overlap problem in memberships.

Random link attacks performs multiple false identities and creates interactions among various users profiles to attack regular users profiles to attack regular users of social networks. We have showed that RLA attackers can be splitted by their special collaborative attack. The malicious user has complete control by breaking nodes and captures then to attack a more number of randomly chosen victim nodes. Our spectrum detection approach works when hackers choose random victims or by attacking few victims while performing their collaborative attacks.

The state of anonymization of privacy protection in social network graphs describes effective anonymization attacks to protect from hackers. In this paper, starclique, a minimal graph required k-anonymity, whrere user is identified for all possible contributions of data objects. The identification of social intersection attack can compromise users to identify shared objects relying on social graph topology.

III. SYSTEM MODULE AND PROPOSED WORK

A. System Module

1. USER MODULE:-In this module, users are having authentication and security to access the detail which is presented in the ontology system. Before accessing or searching the details user should have the account in that otherwise they should register first.

2. INFORMATION LOSS:-We aim to information loss low. Information loss in this case contains both structure information loss. There are some non sensitive data's are loss due to privacy making so we can't send out full information to the public.

3. SENSITIVE LABEL PRIVACY PROTECTION:-There are who post the image to the online social network if allow the people for showing the image it will display to his requesters it make as the sensitive to that user.

B. Proposed Work

Finally in our proposed approach, we are developing KDLD sequence for target node creation of social network graphs. Given a graph G and its degree sequence consists of triplet namely node position, degree and sensitive labels.

KDLD SEQUENCE GENERATION: Given the sensitive degree sequence P and two integers k and l, computes a KDLD sequence. To obtain a new KDLD sequence, same group nodes are needed to be modified for next graph construction process. We further employ two algorithms:

1. K-L BASED
2. L-K BASED

The algorithms keeping the nodes of similar degrees to same group to reduce node reidentification process. Algorithm K-L-BASED chooses firstly K elements in original social graph and by monitoring the next element into current group until L-diversity constraint is satisfied.

Cnew: The cost of developing a new group for the next element

Cmerge: The cost of merging the next element into the current group.

In this way, target node generation can be created and after that graph construction process is to generated as follows.

Graph construction:

Neighborhood_Edge_Editing(): Neighborhood operation describes by adding or by deleting the nodes and edges in the KDLD sequence generation. By doing this modification sensitive labels are being protected from hackers.

Adding_Node_Decrease_Degree(): If the node degree is larger than target KDLD sequence generation node, we need to decrease the degree of node by breaking the links between two hop neighbours and by making a direct links to noise nodes.

Adding_Node_Increase_Degree(): If the node degree is smaller than target KDLD sequence generation node, we need to degree of node by concerning the links between two hop neighbors and by breaking a direct links to noise nodes.

New_Node_Degree_Setting(): This operation describes by assigning degrees to noise nodes. Suppose whose noise node degree is an even number, we select an even degree or if it is odd degree we have to assign odd degree for target nodes.

New_Node_Label_Setting(): The final step is to assign labels to newly modified social network graphs. By doing this it is more helpful for preserving distances between labels and remaining labels in social network graphs.

IV. CONCLUSION

We purpose k-degree-l-diversity model for privacy preserving social network data publishing. We implement both distinct l-diversity and recursive diversity. In order to achieve of k-degree-l-diversity, we design a noise node adding algorithm to construct a new graph from the original graph with the constraint of introducing fewer distortions to the original graph. Our extensive experimental results demonstrate that the noise nodes adding algorithms can achieve a better result than the previous work using edge editing only. It is interesting direction to study clever algorithms which can reduce the number of noise nodes if the noise nodes contribute to both anonymization and diversity. It is another interesting direction is to consider how to implement this protection model in a distributed environment, where different publishers publish their data independently and their data are overlapping.

REFERENCES

[1] L. Sweeney , "K-Anonymity. Anonymity. A Model for Protecting Privacy," Int'l J. Uncertain. Fuzziness Knowledge-Based Systems, vol. 10, pp.557-570, 2002.

[2] B. Zhou and J. Pei, "The K-Anonymity and L-Diversity Approaches for Privacy Preservation in Social Networks against Neighborhood Attacks," Knowledge and Information Systems, vol.28,pp. 47-77,2011.

[3] S. Das, O. Egecioglu, and A.E. Abbadi, "Privacy Preserving in Weighted Social Network, "Proc. Int'l Conf. Data Eng.(ICDE'10), pp. 904-907,2010.

[4] A-L. Baraba si and R. Albert, "Emergence of Scaling in Random Networks, " Science, vol. 286, pp. 509-512,1999.

[5] J.Cheng A.W.-c, Fu , and J. Liu, "K-Isomorphism: Privacy Preserving Network Publication against Structural Attacks, "Proc. Int'l Conf.Management Of Data, pp, 459-470, 2010.

[6] G. Cormode, D. Srivastava, T. Yu, and Q. Zhang, "Anonymizing Bipartite Graph Data Using Safe Groupings," Proc. VLDB Endowment, vol. 1, pp. 833-844, 2008.

[7]G, Ghinita P. Karras, P. Kalnis, and N. Mamoulis, "A Framework for efficient Data Anonymization Under Privacy and accuracy Constraint, "ACM Trans. Database System,vol.34, pp.9:1-9:47,July 2009.

[8]A. Campan and T.M.Truta. A Clustering approach for data and structural anonymity in social network data.

[9]K. Liu and E. Terzi. Towards identity anonymization on graphs.

[10] S.Bhagat, G. Cormode, B. Krishnamurthy, and D. Srivastava, "Class-Based Graph Anonymization for Social Network Data, "Proc. VLDB Endownment, vol. 2,pp. 766-777, 2009.

AUTHORS

First Author – Miss Pradnya Sangade, PG Student, Computer Department, JSMP's BSIOTR,Wagholi,Pune
Second Author – Prof. Nitin Shivale, Assistant Professor, Computer Department, JSMP's BSIOTR,Wagholi,Pune.