Inference Attack Prevention of Private Information on Social Networks

Kaloge T.B.[1]&Nandwalkar B.R.[2]

[1,2]*(Comp. Engg. Dept., GNS COENashik, SPP Univ., Pune(MS), India)*

Abstract :*Online social networks, such as Facebook, LinkedIn are increasingly use by many people. These networks allow users to give details about themselves and allow connecting to their friends. Some of the information visible inside these networks is meant to be private. It is possible to use learning algorithms on released data to predict private information. We explore how to launch inference attacks using released social networking data to predict private information. We devise three possible sanitization techniques that could be used in various situations. Then, we define the effectiveness of these techniques and attempt to use methods of collective inference to discover sensitive attributes of the data set. We also show that we can decrease the effectiveness of both local and relational classification algorithms by using the sanitization methods we described.*

Keywords -*Social network analysis, data mining, social network privacy, genetic algorithm.*

1. INTRODUCTION

Social networks are online applications that allow their users to connect by means of various link types. These networks allow people to list details about themselves that are relevant to the nature of the network. In general-use social network individual users list their favorite activities, books, and movies. LinkedIn is a professional network; because of this users will specify details which are related to their professional life (i.e., reference letters, previous employment, and so on.) Because these sites gather extensive personal information of users, social network application providers have a rare opportunity: direct use of this information could be useful to advertisers for direct marketing. In practice, privacy concerns can prevent these efforts. This conflict between the desired use of data and individual privacy presents an opportunity for privacy preserving social network data mining that is the discovery of information and relationships from social network data without violating privacy. Privacy concerns of individuals in a social network can be classified into two categories privacy after data release and private information leakage. The Instances of privacy after data release involve the identification of specific individuals in a data set subsequent to its release to the general public or to paying customers for a specific usage.

Private information leakage is related to details about an individual that are not explicitly stated, but, they are inferred through other details released and relationships to individuals who may express that detail. An example of this type of information leakage is a scenario where a user, says Arnold, does not enter his political affiliation because of privacy concerns. But, it is publicly available that he is a member of the “legalize the same sex marriage.” By using these type of available information publicly available regarding a general Group membership, it is easily guessable what Arnold’s political affiliation is somewhat less obvious is the favorite movie “The End of the Spear” We note that this is an issue which is related to both in live data and in any released data.

2. LITERATURE SURVEY

He et al. Consider ways to infer private information via friendship links by creating a Bayesian network from the links inside a social network. While they will crawl a real social network, they use hypothetical attributes to analyze their learning algorithm, but they have not considered collective inference techniques for possible inference attack [4].

Zheleva and Getoor propose several methods of Social graph anonymization and focusing mainly on the idea that by anonymizing both the nodes in the group and the link structure, that one thereby anonymizes the graph[5].

Gross et al. examine specific usage instances at Carnegie Mellon. They note potential attacks, such as node re identification , that easily accessible data on Facebook could assist. They further note that while privacy controls may exist on the user's end of the social networking site but many individuals do not take advantage of this tool. This finding coincides well with the amount of data that we were able to crawl using a very simple crawler on a Facebook network. We will extend on their work by experimentally examining the accuracy of some types of the demographic re identification that they propose before and after sanitization [6].

Jones and Soltrencrawl Facebook's data and analyze usage trends among Facebook users will employing bothprofile postings and survey information. Their paper focuses mostly on faults inside the Facebook platform.

They do not discuss attempting to learn unrevealed details of Facebook users and do no analysis of the details of Facebook users. Their crawl consist of around 70,000 Facebook accounts [7].Sen and Getoor was compare various methods of link-based classification including loopy belief propagation, mean field relaxation labeling, and iterative classification [8].Tasker et al. present an alternative classification method where they build on Markov networks. None of these papers consider ways to combat their classification methods [9]. Zheleva and Getoor attempt to predict the private attributes of users in four real-world data sets Facebook, Flickr, Dogster and BibSonomy. They do not attempt to actually anonymized or sanitize any graph data. but their focus is on how specific types of data namely that of declared and inferred group membership, may be used as a way to boost the local and relational classification accuracy. Their define method of group based (as opposed to details-based or link-based) classification is an inherent part of our details-based classification, as we will treat the group membership data as another detail , as we do favorite books or movies [11].

Talukder et al. propose a method of measuring the amount of information that a user reveals to the outside world and which automatically determines which information (on a per-user basis) should be removed to increase the privacy of an individual [12].We do preliminary work on the effectiveness of our Links, details and Average classifiers and examine their effectiveness after removing some details from the graph. We try to expand further by evaluating their effectiveness after removing details and links [13].

2.1. Naïve Bayesian classification

Determining an individual's political affiliation is an exercise in graph classification. Given a node ni with m details and p potential classification labels, C1,... ,Cp , the probability of ni being in class Cx, is given by the equation given below, where arg max1 ≤ x ≤ p represents the possible class label that maximizes the previous equation. This is difficult to calculate, P for any given value of x is unknown. Then by applying Bayes' theorem, we have equation

$$\underset{1\leq x\leq p}{\operatorname{argmax}}\left[\frac{P(C_x^i)\times P(D_i^1\ \dots\dots\dots\dots\dots..D_i^m\left|C_x^i\right.)}{P(D_i^1\ \dots\dots\dots\dots\dots..D_i^m)}\right](1)$$

Further, by assuming that all details are independent, we are left with the simplified equation [1].

$$\operatorname{argmax}_{1\leq x\leq p}\left[\frac{P(C_x^i)\times P(D_i^1|C_x^i)\times\dots\dots\dots\dots\dots\times P(D_i^m|C_x^i)}{P(D_i^1\dots\dots\dots\dots\dots D_i^m)}\right](2)$$

2.2. Naive Bayes on Friendship Links

Consider the problem of determining the class detail value of person ni given their friendship links using a naive Bayes model.

That is, of calculating P(Cix|Ni). Because there are relatively few people in the training set that have a friendship link to ni, the calculations for P(Cix|Fi,j) become extremely inaccurate. Instead, we choose to decompose this relationship. Rather than having a link from person ni to nj, we instead consider the probability of having a link from ni to someone with nj's details. Thus

$$\begin{aligned}P\left(C_x^i|F_{i,j}\right) &\approx P\left(C_x^i|L_1.L_2\ \dots\dots\dots\dots\dots.L_m\right)\\ &\approx \frac{P\left(C_x^i\right)\times P(L_1|C_x^i)\times\ \dots\dots\dots\dots\dots.P(L_m|C_x^i\right)}{P(L_1.L_2\ \dots\dots\dots\dots\dots.L_m)}(3)\end{aligned}$$

Where Ln represents a link to someone with detail Jn [1].

2.3. Weighing Friendships

There is one last stepto calculating P(Cix|Ni). In the specific case of social networks, two friends can be anythingfrom acquaintances to close friends or family members. Whilethere are many ways to weigh friendship links, the methodweused is very easy to calculate and is based on the assumption that the more public details two people share,themore private details they are likely to share. Thisgives thefollowing formula for Wi;j, which represents the weight of a friendship link from ni to node nj:

$$W_{i,j} = \frac{\left|\left(D_i^1 \ldots\ldots\ldots . D_i^n\right) \cap \left(D_j^1 \ldots\ldots\ldots . D_j^m\right)\right|}{|D_i|} \quad (4)$$

Equation (5) calculates the total number of details ni and nj share divided by the number of details of ni. Note that theweight of a friendshiplinkisnot the samefor both people on each side of a friendship link. In other words, Wj,i ≠ Wi,j. The final formula for person i becomes the following, where Z represents a normalization factor and P(Cix|Fi,j) is calculated by

$$p\left(C_x^i, N_i\right) = \frac{1}{Z} \sum_{n_i \in N_i} \left[P\left(C_x^i \middle| F_{i,j}\right) \times W_{i,j}\right] \quad (5)$$

The value p(Cix;Ni) is used as our approximation to P(Cix|Ni)

3. IMPLEMENTATION DETAILS

3.1. Platform: NetBeans IDE 6.7.1:

Netbeans IDE provides first class comprehensive support for the newest java technologies and latest java specification enhancements before other IDE. It is first free IDE providing support for JDK8 previews JDK7, JavaEE7 including its related HTML5 enhancements and javaFX2.

3.2. Genetic Algorithm:

In a genetic algorithm approach, a solution (i.e., a point in the search space) is called a “chromosome” or string. A GA approach requires a population of chromosomes (strings) rep-resenting a combination of features from the solution set, and requires a cost function (called an evaluation or fitness function). This function calculates the fitness of each chromosome. The algorithm manipulates a finite set of chromosomes (the population), based loosely on the mechanism of evolution. In each generation, chromosomes are subjected to certain operators, such as crossover, inversion and mutation, which are analogous to processes which occur in natural reproduction. Crossover of two chromosomes produces a pair of offspring chromosomes which are synthesis of the traits of their parents. Inversion in a chromosome produces a mirror-image reflection of a subset of the features on the chromosome. Mutation of a chromosome produces a nearly identical chromosome with only local alternations of some regions of the chromosome.

By using Genetic Algorithm we will increase the accuracy and set privileges for friends, family friends and business friends to access the private information publish in social network.

Algorithm:

1. start
2. Consider a graph having nodes and edges of datasets
3. Select individual nodes.
4. Perform crossover i.e. find probability values of details, links and weights.
5. Store probability values in fitness function.
6. According to probability values set privileges.
7. Stop.

Module Architecture:

1. Learning method of social network module

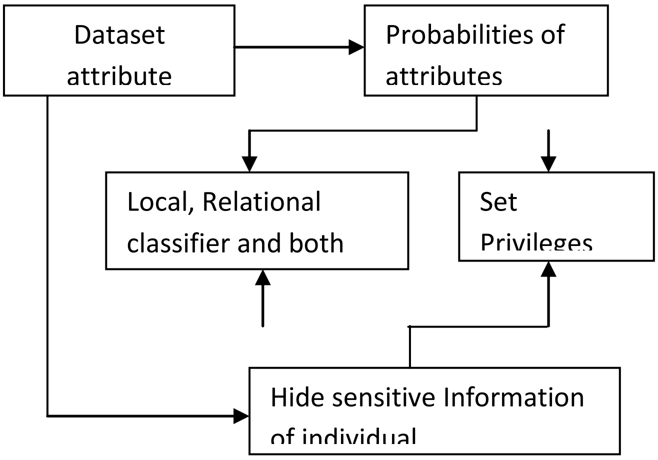
Input: In this module we consider the graph nodes in the datasets as input, in which nodes represent the details, link represent the friendship link.

Algorithm: Genetic algorithm

Output: Probability values of the attributes which we want to protect from inference attack.

2. Network Classification module
   Input: Probability values as calculated in first module
   Algorithm: Local Classifier, Relational Classifier, collective inference method.
   Output: According to probability values we remove details, link or both in order to protect private information.

3. Private information hiding module
   In this module we set the privileges for friends, business friends and family friends so that the private information is hide and protected.


Dataset attribute
Probabilities of attributes
Local, Relational classifier and both
Set Privileges
Hide sensitive Information of individual

3.3. Network classification

Collective inference is a method of classifying social network data using a combination of node details and connecting links in the social graph. Each of this classifiers consists of three components: a relational classifier, a local classifier, and a collective inference algorithm.

Local Classifier: Local classifiers are a type of learning method that is applied in the initial step of collective inference. It is a classification technique that examines details of a node and constructs a classification scheme based on the details that it finds there. The naive Bayes classifier we discussed previously is a standard example of Bayes classification. The classifier builds a model based on the details of nodes in the training set. Then applies this model to nodes in the testing set to classify them.

Relational Classifiers: The relational classifier is a separate type of learning algorithm that looks at the link structure of the graph and uses the labels of nodes in the training set to develop a model which it uses to classify the nodes in the test set. Specifically, in [14], Macskassy and Provost examine four relational classifiers: class-distribution relational neighbor (cdRN), weighted-vote relational neighbor (wvRN), network-only Bayes classifier (nBC), and network-only link-based classification (nLB). The cdRN classifier begins by determining a reference vector for each class. That is for each class, cdRN,Cxdevelops a vector RVx which is a descriptionof what a nodethat is of type Cx tends to connect to Specifically, RVx(a) isan average value for how often a node of class Cx has a link toa node of class Ca. To classify node ni, the algorithm builds a class vector, CVi, where CVi(a) iscount of h a ow often nihasa link to a node of class Ca. The class probabilities arecalculated by comparing CVi to RVx for all classes Cx.ThenBC classifier uses Bayes theorem to classify basedonly on the link structure of a node. That is, it defines

$$P(C_x^i|N_i) = \frac{P(N_i|C_x^i) \times P(C_x^i)}{P(N_i)} \qquad (6)$$

$$\prod_{n_j \in N_i} \frac{P\left(C_a^j | C_x^i\right) \times P\left(C_x^i\right)}{P\left(n_j\right)} (7)$$

where Ni are the neighbours of ni, and then uses theseprobabilities to classify ni.ThenLB classifier collects the labels of the neighbouringnodes and by means of logistic regression, uses thesevectors to build a model.In the wvRN relational classifier, to classify a node nieach of its neighbours, nj, is given a weight.

The probabilityofni being in class Cx is the weighted mean of the classprobabilities of ni's neighbours. That is

$$P\left(C_x^i | N_i\right) = \frac{P\left(N_i | C_x^i\right) \times P\left(C_x^i\right)}{P\left(N_i\right)} \qquad (8)$$

Collective Inference Methods: Unfortunately, there are issues with each of the methods described above. Local classifiers consider only the details of the node it is classifying. Conversely, relational classifiers consider only the link structure of a node.

Specifically, a major problem with relational classifiers is that while we may cleverly divide fully labelled test sets so that we ensure every node is connected to at least one node in the training set, real world data will may not satisfy this strict requirement. If this type of requirement is not met, then relational classification will unable to classify nodes which have no neighbors in the training set. The collective inference attempts to make up for these deficiencies by using both local and relational classifiers in a precise manner to attempt to increase the classification accuracy of nodes in the network and by using a local classifier in the first iteration, the collective inference ensures that every node will have an initial probabilistic classification will referred to as a prior and the algorithm then uses a relational classifier to reclassify nodes. At each of these steps i> 2, the relational classifier uses the fully labelled graph from step i 1 to classify each node in the graph.

The collective inference method also controls the length of time the algorithm runs. in Some algorithms specify a number of iterations to run, while others are converge after a general length of time.

We choose to use relaxation labelling as described in [14]: a method that retains the uncertainty of our classified labels each of these classifiers, including a relaxation labelling implementation is included in the NetKit-SRL.3

As such, after we will perform our sanitization techniques, we will allow NetKit to classify the nodes to examine the effectiveness of our approaches.

4. RESULTS

3.1. Datasets

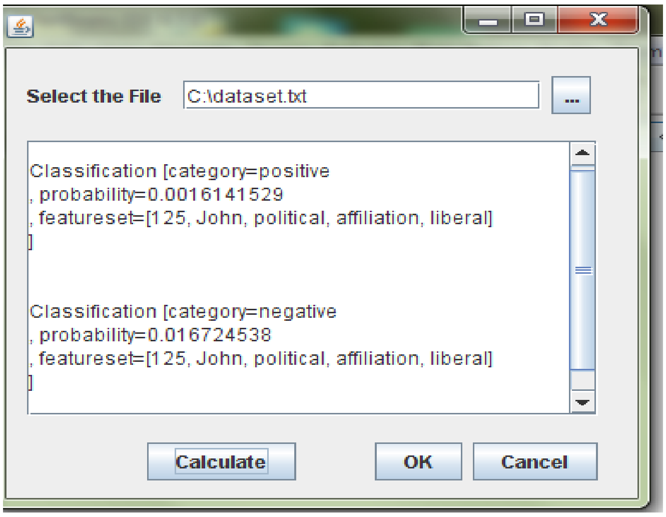
WebKB: This data is based on the WebKB Project. It consists of sets of web pages from four computer science departments, with each page manually labeled into 7 categories: course, department, faculty, project, staff, student, or other. We do not include the 'other' pages in the graph, but use them to generate edges.

This data file contains eight different graphs (two per university). For each university, we have the graph using direct hyperlinks and another graph using co-citation links. To create co-citation edges, we do allow an 'other' page as an intermediary although the final graph does not include the 'other' pages. To weight the link between x and y, we sum the number of hyperlinks from x to z and separately the number from y to z, and multiply these two quantities.These attributes we have consider as an input in module 1 We can use the datasets IMDB,CORA and SEC filings.

CORA: This data set is based on the coradata set, which comprises computer science research papers.

It includes the full citation graph as well as labels for the topic of each paper. There are seven possible labels.The file contains two data sets, one using only citation links and one using both citation and shared-author links. The edge weights are added: one per shared author and one for a citation (two if the papers cite each other).

3.2. Results



Select the File C:\dataset.txt

```
Classification [category=positive
, probability=0.0016141529
, featureset=[125, John, political, affiliation, liberal]
]


Classification [category=negative
, probability=0.016724538
, featureset=[125, John, political, affiliation, liberal]
]
```

5. CONCLUSION AND FUTURE SCOPE

We addressed various issues related to private information leakage in social networks. We show that using both friendship links and details together gives better predict-ability than details alone. In addition, we will explored the effect of removing details and links in preventing sensitive information leakage. In this process, we discovered situations in which collective inferencing does not improve on using a simple local classification method to identify the nodes. When we combine the results from the collective inference implications with the individual results, then we begin to see that removing details and friendship links together is the best way to reduce classifier accuracy. Then this is probably infeasible in maintaining the use of social networks. We also show that by removing only details, and then we greatly reduce the accuracy of local classifiers, it will give us the maximum accuracy that we were able to achieve through any combination of classifiers.

In future work we will identify the key node of the graph if it will remove or alter due to this node we can decrease and provide information leakage and give limited access to private information we want to protect.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my guide, Prof. B. R. Nandwalkar, for his guidance and support. I will forever remain grateful for the constant support and guidance extended by guide, in making this report. Through our many discussions, he helped me to form and solidify ideas. The invaluable discussions I had with him, the penetrating questions he has put to me and the constant motivation, has all led to the development of this project.

I wish to express my sincere thanks to the Head of department, Prof. N. R. Wankhade also grateful thanks to M. E. coordinator Prof. Ms. J. V. Shinde and the departmental staff members for their support.

REFERENCES

[1] R. Heatherly, M. Kantarcioglu, and B. Thuraisingham, Fellow “Preventing Private Information Inference Attacks on Social Networks" IEEE transactions on knowledge and data engineering ,VOL. 25, NO. 8, august, 2013.

[2] M. Hay, G. Miklau, D. Jensen, P. Weis, and S. Srivastava, “Anonymizing Social Networks,” Technical Report 07-19,Univ. of Massachusetts Amherst, 2007.

[3] K. Liu and E. Terzi, “Towards Identity Anonymization on Graphs,” Proc. ACM SIGMOD Int’l Conf. Management of Data (SIGMOD ’08), pp. 93-106, 2008.

[4] J. He, W. Chu, and V. Liu, “Inferring Privacy Information from Social Networks,” Proc. Intelligence and Security Informatics, 2006.

[5] E. Zheleva and L. Getoor, “Preserving the Privacy of Sensitive Relationships in Graph Data,” Proc. First ACM SIGKDD Int’l Conf. Privacy, Security, and Trust in KDD, pp. 153-171, 2008.

[6] R. Gross, A. Acquisti, and J.H. Heinz, “Information Revelation and Privacy in Online Social Networks,” Proc. ACM Workshop Privacy in the Electronic Soc. (WPES ’05), pp.71-80,http://.doi.org/10.1145/1102199.1102214, 2005.

[7] H. Jones and J.H. Soltren, “Facebook: Threats to Privacy,”technical report, Massachusetts Inst. of Technology, 2005.

[8] P. Sen and L. Getoor, “Link-Based Classification,” Technical Report CS-TR-4858, Univ. of Maryland, Feb. 2007

[9] B. Tasker, P. Abbeel, and K. Daphne, “Discriminative Probabilistic Models for Relational Data,” Proc. 18th Ann. Conf. Uncertainty in Artificial Intelligence (UAI ’02), pp. 485-492, 2002.

[10] Menon and C. Elkan, “Predicting Labels for Dyadic Data,” Data Mining and Knowledge Discovery, vol. 21, pp. 327-343, 2010.

[11] E. Zheleva and L. Getoor, “To Join or Not to Join: The Illusion of Privacy in Social Networks with Mixed Public and Private user Profiles,” Technical Report CS-TR-4926, Univ. of Maryland, College Park, July 2008.

[12] N. Talukder, M. Ouzzani, A.K. Elmagarmid, H. Elmeleegy, and M. Yakout, “Privometer: Privacy Protection in Social Networks,” Proc. IEEE 26th Int’l Conf. Data Eng. Workshops (ICDE ’10), pp. 266-269, 2010.

[13] J. Lindamood, R. Heatherly, M. Kantarcioglu, and B. Thuraising-ham, “Inferring Private Information Using Social Network Data,” Proc. 18th Int’l Conf. World Wide Web (WWW), 2009.

[14] S.A. Macskassy and F. Provost, “Classification in Networked Data: A Toolkit and a Univariate Case Study,” J. Machine Learning Research, vol. 8, pp. 935-983, 2007.

[15] L. Sweeney, “k-Anonymity: A Model for Protecting Privacy,” Int’l J. Uncertainty, Fuzziness and Knowledge-based Systems, pp. 557-570, 2002.

[16] Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubrama-niam, “L-Diversity: Privacy Beyond K-Anonymity,” ACM Trans. Knowledge Discovery from Data, vol. 1, no. 1, p. 3, 2007.

[17] Dwork, “Differential Privacy,” Automa ta, L anguages and Programming, M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener, eds., vol. 4052, pp. 1-12, Springer, 2006.

[18] Friedman and A. Schuster, “Data Mining with Differential Privacy,” Proc. 16th ACM SIGKDD Int’l Conf. Knowledge Discovery and Data Mining, pp. 493-502, 2010..

[19] K. Fukunaga and D.M. Hummels, “Bayes Error Estimation Using Parzen and K-nn Procedures,” IEEE Trans. Pattern Analysis and Machine Intelligence, vol. PAMI-9, no. 5, pp. 634-643,http:// portal.acm.org/citation.cfm?id=28809.28814, Sept. 1987.

[20] Clifton, “Using Sample Size to Limit Exposure to Data Mining,” J. Computer Security, vol. 8, pp. 281-307, citation.cfm?id=371090.371092,

[21] K. Tumer and J. Ghosh, “Bayes Error Rate Estimation Using Classifier Ensembles,” Int’l J. Smart Eng. System Design, vol. 5, no. 2, pp. 95-110, 2003.