Inferring Privacy Information from Social Networks[⋆]

Jianming He[1], Wesley W. Chu[1], and Zhenyu (Victor) Liu[2]

[1] Computer Science Department UCLA, Los Angeles, CA 90095, USA
[2] Google Inc. USA

Abstract. Since privacy information can be inferred via social relations, the privacy confidentiality problem becomes increasingly challenging as online social network services are more popular. Using a Bayesian network approach to model the causal relations among people in social networks, we study the impact of prior probability, influence strength, and society openness to the inference accuracy on a real online social network. Our experimental results reveal that personal attributes can be inferred with high accuracy especially when people are connected with strong relationships. Further, even in a society where most people hide their attributes, it is still possible to infer privacy information.

1 Introduction

With the increasing popularity of Social Network Services (SNS), more and more online societies such as Friendster, Livejournal, Blogger and Orkurt have emerged. Unlike traditional personal homepages, people in these societies publish not only their personal attributes (e.g., age, gender, and interests), but also their relationships with friends. As social networks grow rapidly, many interesting research topics [3, 6, 13] arise. Unfortunately, among these topics, privacy has not been fully addressed yet. Given the huge amount of personal data and social relations available in online social networks (for example, Friendster owns over 24 million personal profiles), it is foreseeable that privacy may be compromised if people are not careful in releasing their personal information.

Information privacy has become one of the most urgent research issues in building next-generation information systems. A great deal of research effort has been devoted to protecting people's privacy. Aside from recent developments in cryptography and security protocols that provide secure data transfer capabilities, there has been work on enforcing industry standards (e.g., P3P [12]) and government policies (e.g., the HIPAA Privacy Rule [11]) to grant individuals control over their own privacy. These existing techniques and policies aim to effectively block *direct* disclosure of sensitive personal information. However, to the best of our knowledge, none of the existing techniques handle *indirect* disclosure which can often be achieved by intelligently combining pieces of seemingly innocuous or unrelated information. Specifically, in scenarios like social networks,

[⋆] This research is in part supported by NSF grant # IIS-03113283.

S. Mehrotra et al. (Eds.): ISI 2006, LNCS 3975, pp. 154–165, 2006.

we realize that individuals connected in social networks often share common attributes. For instance, in a dance club, people come together due to their common interest; in an office, people connect to each other because of similar professions. Therefore, it is possible that one may be able to infer someone's attribute from the attributes of his/her friends. In such cases, privacy is indirectly disclosed by their social relations rather than from the owner directly.

In this paper, we study the privacy disclosure in social networks. We want to analyze under what conditions and to what extent privacy might be disclosed by social relations. In order to perform privacy inference, we propose an approach to map Bayesian networks to social networks. We discuss prior probability, influence strength and society openness which might affect the inference, and conduct extensive experiments on a real online social network structure.

The paper is organized as follows. In Section 2, we briefly introduce the background and related work. In Section 3, we explain the target scenarios, propose an approach to model social networks with Bayesian networks and perform Bayesian inference on personal attributes. In Section 4, we present three key characteristics of social networks and conduct experiments to investigate their impact on privacy inference. In Section 5, we discuss the issue of society openness and explain why Bayesian inference performs well even with little evidence of friends' attributes. Finally, we summarize this paper.

2 Background and Related Work

2.1 Social Networks

Social network analysis has been conducted in many areas. Milgram's classic paper [8] in 1967 estimates that every person in the world is only six hops away from each other. The recent success of the Google search engine [2], which applies social network ideas to the Internet, draws great attention on social network analysis again. For instance, Newman [10] reviews the relationship between graph structure and dynamical behavior of large networks. The ReferralWeb project mined social networks from a wide variety of public-available information [6]. A work similar to ours is [3], which realizes that one's decision to buy products may be influenced by his/her friends, and they model social network as a Markov random field to find the customers' network value. In contrast, we believe a person's attribute can be reflected from his/her friends' attributes, and we view a social network as a Bayesian network.

2.2 Bayesian Networks

A Bayesian network [4, 5, 9] is a graphic representation of the joint probability distribution over a set of variables. It consists of a network structure and a collection of *conditional probability tables* (CPT). The network structure is represented as a *Directed Acyclic Graph* (DAG) in which each node corresponds to a random variable and each edge indicates a dependent relationship between connected variables. In addition, each variable (node) in a Bayesian network is associated with a CPT, which enumerates the conditional probabilities for this variable, given all the combinations of its parents' value. Thus, for a Bayesian network, the DAG captures causal relationships among random variables, and CPTs quantify these relationships.

Bayesian networks have been extensively applied to fields such as medicine, image processing, and decision support systems. Since Bayesian networks include the consideration of network structure, we use them as our inference model. Individuals in a social network can be represented as nodes and the relations between individuals can be modelled as edges in Bayesian networks.

3 Bayesian Inference Via Social Relations

3.1 Problem Statement

Intuitively, friends often share common attributes (e.g., hobbies and professions); thus, it is possible to predict someone's attributes by looking at the types of friends he/she has. In this paper, we want to investigate the effect of social relations on privacy inference. However, in the real world, people are acquainted with each other via all types of relations, and a personal attribute may only be sensitive to certain types of relations. For example, in order to predict someone's age, it is more appropriate to consider the ages of his/her classmates rather than officemates. Therefore, to infer people's privacy from social relations, one must be able to filter out other types of relations between two connected people. To simplify this problem, we investigate privacy inference in *homogeneous societies* where individuals are connected by a single type of social relations (referred to as "friendship") and the impact of every person on his/her friends is the same. Homogenous societies reflect small closely related groups (such as offices, classes or clubs), where people are connected by a relatively pure relationship. Real social networks can be regarded as the combinations of many homogeneous societies.

To perform inference, we use Bayesian networks to model the causal relations among people in social networks. Specifically, if we want to infer the value of attribute A for a person (referred to as *query node* X), we first construct a Bayesian network from X's social network, and then analyze the Bayesian network to obtain the probability that X has attribute A. In Section 3.2, we start from a simple case in which privacy inference only involves the direct friends of the query node. In Section 3.3, we treat the more complex case where attribute values from friends at multiple hops away are considered.

3.2 Single Hop Inference

Let us consider the case in which we know the attribute values for *all* the direct friends of the query node X. We define Y_{ij} as the jth friend of X at i hops away. If a friend can be reached via more than one route from X, we use the depth of the shortest path as the value of i. Let Y_i be the set of Y_{ij} $(1 \leq j \leq n_i)$, where n_i

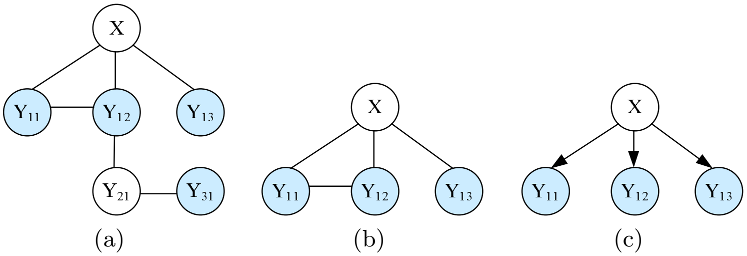

Fig. 1. Reduction of a social network (a) into a Bayesian network to infer X from his friends Y via Localization assumption (b) and via Naive Bayesian Assumption (c). The shaded nodes represent friends whose attribute values are known.

is the number of X's friends at i hops away. For instance, $Y_1 = \{Y_{11}, Y_{12}, ..., Y_{1n_1}\}$ is the set of X's direct friends which are one hop away.

An example of a social network with six friends is shown in Fig. 1(a). In this figure, Y_{11}, Y_{12} and Y_{13} are direct friends of X. Y_{21} and Y_{31} are the direct friends of Y_{12} and Y_{21} respectively. In this scenario, the attribute values of Y_{11}, Y_{12} and Y_{13} are known (represented as shaded nodes).

Bayesian Network Construction. To facilitate the construction of the Bayesian network, we make two assumptions.

Intuitively, the direct friends of an individual have more influence on this person than friends who are two or more hops away. We assume that it is sufficient to consider only the attribute values of direct friends Y_1 to infer X's attribute. Once all the attribute values of Y_1 are known, knowing the attribute values of any other friends at multiple hops away provides no additional information for predicting X's attribute. Formally, we state this assumption as follows.

Localization Assumption. Given the attribute values of the direct friends Y_1 of the query node X, then friends at more than one hop away (i.e., Y_i for $i > 1$) are conditionally independent of X.

Based on this assumption, Y_{21} and Y_{31} in Fig. 1(a) can be pruned, and the inference of X only involves X, Y_{11}, Y_{12} and Y_{13} (Fig. 1(b)). Then the next question is how to decide a DAG linking the remaining nodes. If the resulting social network does not contain cycles, a Bayesian network can be obtained immediately. Otherwise, one must employ more sophisticated techniques to remove cycles, such as the use of auxiliary variables to capture non-causal constraints (*exact conversion*) and the deletion of edges with the weakest relations (*approximation conversion*). We adopt the latter approach and make a *Naive Bayesian* Assumption. That is, the attribute value of X influences that of Y_{1j} $(1 \leq j \leq n_1)$, and there is a direct link pointing from X to each Y_{1j}. By making this assumption, we consider the inference paths from X to Y_{1j} as the *primary* correlations, and disregard the correlations among the nodes in Y_1. Formally, we have:

Naive Bayesian Assumption. Given the attribute value of the query node X, the attribute values of direct friends Y_1 are conditionally independent of each other.

This Naive Bayesian model has been used in many classification/prediction applications including textual-document classification. Even though it simplifies the correlation among variables, this model has been shown to be quite effective [7]. Thus, we adopted this assumption in our study. In Fig. 1(c), we obtain a final DAG by removing the connection between Y_{11} and Y_{12} in Fig. 1(b).

Bayesian Inference. We use the Bayes Decision Rule to predict the attribute value of X. For a general Bayesian network with maximum depth i, let the value for X, $\bar{x}$, be the attribute value with the maximum conditional probability given the observed attribute values of other nodes in the network (i.e., the maximum posterior probability):

$$\bar{x} = \arg\max_{x} P(X = x \mid Y_1, Y_2, ..., Y_i) \qquad x \in \{t, f\}. \tag{1}$$

Since single hop inference involves only the direct friends Y_1 that are independent of each other, the posterior probability can be further reduced using the conditional independence encoded in the Bayesian network:

$$\begin{aligned} P(X = x \mid Y_1) &= P(X = x \mid Y_{11} = y_{11}, ..., Y_{1n_1} = y_{1n_1}) \\ &= \frac{P(X = x, Y_{11} = y_{11}, ..., Y_{1n_1} = y_{1n_1})}{P(Y_{11} = y_{11}, ..., Y_{1n_1} = y_{1n_1})} \\ &= \frac{P(X = x) \cdot P(Y_{11} = y_{11}, ..., Y_{1n_1} = y_{1n_1} \mid X = x)}{\sum_x [P(X = x) \cdot P(Y_{11} = y_{11}, ..., Y_{1n_1} = y_{1n_1} \mid X = x)]} \\ &= \frac{P(X = x) \cdot \prod_{i=1}^{n_1} P(Y_{1i} = y_{1i} \mid X = x)}{\sum_x [P(X = x) \cdot \prod_{i=1}^{n_1} P(Y_{1i} = y_{1i} \mid X = x)]}, \end{aligned} \tag{2}$$

where x and y_{1j} are the attribute values of X and Y_{1j} respectively ($1 \leq j \leq n_1$, $x, y_{1j} \in \{t, f\}$) and the value of y_{1j} is known.

Since we assumed that the network is homogeneous, the CPT for each node is the same. Thus, we use $P(Y = y \mid X = x)$ to represent $P(Y_{1j} = y_{1j} \mid X = x)$. For this reason, direct friends of X are equivalent to each other, and the posterior probability now depends on N_{1t}, which is the number of friends with attribute value t, rather than the individual attribute value. Therefore, we rewrite the posterior probability $P(X = x \mid Y_1)$ as $P(X = x \mid N_{1t} = n_{1t})$. If $N_{1t} = n_{1t}$, we obtain:

$$P(X{=}x \mid N_{1t}{=}n_{1t}) {=} \frac{P(X = x) \cdot P(Y = t \mid X = x)^{n_{1t}} \cdot P(Y{=}f \mid X = x)^{n_1 - n_{1t}}}{\sum_x [P(X = x) \cdot P(Y{=}t \mid X = x)^{n_{1t}} \cdot P(Y = f \mid X = x)^{n_1 - n_{1t}}]}. \tag{3}$$

To compute (3), we need to further learn the conditional probability $P(Y = y \mid X = x)$. We apply the *parameter estimation* [9] technique and obtain:

$$P(Y = y \mid X = x) = \frac{\#\text{ of friendship links connecting people with } X = x \text{ and } Y = y}{\#\text{ of friendship links connecting a person with } X = x}. \tag{4}$$

Substituting (4) and (3) into (1) yields $\bar{x}$.

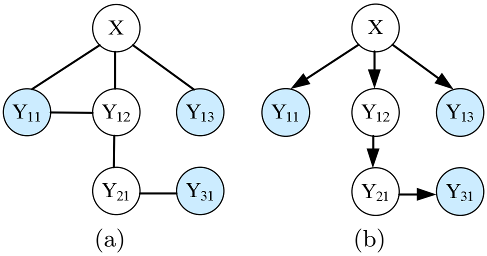

Fig. 2. Reduction of a social network (a) into a Bayesian network to infer X from his friends Y via Generalized Localization assumption (b). The shaded nodes represent friends whose attribute values are known.

3.3 Multiple Hops Inference

In real world, the attribute values of all the direct friends may not be observed because people may hide their sensitive information. Therefore, the Localization Assumption in Section 3.2 is no longer applicable. To incorporate more attribute information into our Bayesian network, we propose a *generalized localization assumption* as follows.

Generalized Localization Assumption. Given the attribute value of the jth friend of X at i hops away, Y_{ij} $(1 \leq j \leq n_i)$, the attribute of X is conditionally independent of the descendants of Y_{ij}.

This assumption states that if the attribute value for the X's direct friend, Y_{1j}, is unknown, then the attribute value of X is conditionally dependent on the attribute values for the direct friends of Y_{1j}. This process continues until we reach a descendent of Y_{1j} whose attribute value is known. For example, the network structure in Fig. 2(a) is the same as in Fig. 1(a), but the attribute value of Y_{12} is unknown. Based on the Generalized Localization Assumption, we extend the network by branching to Y_{12}'s direct child Y_{21}. Since Y_{21}'s attribute is unknown, we further branch to Y_{21}'s direct friend Y_{31}. The branch terminates here because the attribute of Y_{31} is known. Thus, the inference network for X includes all the nodes in the graph. After applying Naive Bayesian assumption, we obtain the DAG shown in Fig. 2(b). Similar to single hop inference, the resulting DAG in multiple hops inference is also a tree rooted at the query node X. One interpretation of this model is that when we predict the attribute value of X, we always treat him/her as an egocentric person who influences his/her friends but not vice versa. Thus, the attribute value of X can be reflected by those of his/her friends.

For multiple hops inference, we still apply the Bayes Decision Rule. Due to additional unknown attribute values such as Y_{12}, the calculation of the posterior probability becomes more complicated. One common technique to solve this equation is through variable elimination [14]. We adopt the same technique to derive the value of $\bar{x}$ in (1).

4 Experimental Study of Inference Accuracy

In this section, we define three characteristics of social networks that might affect Bayesian inference and evaluate their impact. The performance metric that we consider is *inference accuracy*, which is defined as the percentage of nodes predicted correctly by inference.

4.1 Characteristics of Social Networks

Prior Probability $P(X = t)$ is the probability that people in the social network have attribute A. When no additional information is provided, we could use prior probability to naively predict attribute values for the query nodes: if $P(X = t) \geq 0.5$, we predict that every query node has value t; otherwise, we predict that it has value f. We call this method *naive inference*. The average naive inference accuracy that can be obtained is $max(P(X = t), 1 - P(X = t))$. In our study, we use it as a reference to compare with our Bayesian inference approach.

Influence Strength $P(Y = t \mid X = t)$ is defined as the conditional probability that Y has attribute A given that its direct friend X has the same attribute. This conditional probability measures how X influence its friend Y. A higher influence strength implies that there is a higher probability that X and Y will have attribute A.[1]

Society Openness $O(A)$ is defined as the percentage of people in a society who release their values of attribute A. The more people release their attribute values, the higher the society openness is, and the more evidence about attribute A is observed.

4.2 Data Set

For the experiment, we collect $66,766$ personal profiles from an online weblog service provider Livejournal [1], which owns 2.6 million active members. For each member, Livejournal generates a personnel profile which specifies the member's personal information as well as the URLs for the profiles of this member's friends. Among the collected profiles, there are $4,031,348$ friend relations. The number of friends per member v.s. the number of members follows the power law distribution. About half of the population have less than 10 direct friends.

In order to evaluate the inference behaviors for a wide range of parameters, we use a hypothetical attribute and synthesize the attribute values: for each member, we assign a CPT and determine the actual attribute value based on the parent's value and the assigned CPT. The attribute assignment starts from the set of nodes whose in-degree is 0 and explores the rest of the network following

[1] There is another type of influence strength $P(Y = t \mid X = f)$, which is the conditional probability that two friends have opposite values of attribute A. In an equilibrium state, the value of $P(Y = t \mid X = f)$ can be derived from $P(X = t)$ and $P(Y = t \mid X = t)$, so we do not introduce it as an additional characteristic.

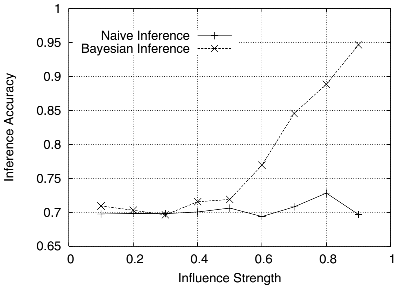

Fig. 3. Inference accuracy of Bayesian vs. naive inference when $P(X = t) = 0.3$

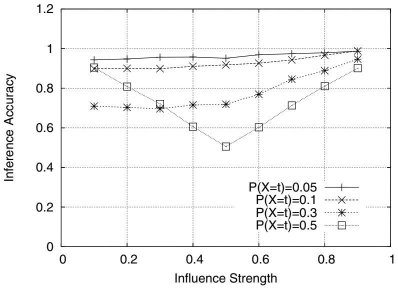

Fig. 4. Inference accuracy of Bayesian inference for different prior probabilities

friendship links. Since we are investigating homogeneous societies, all the members are assigned with the same CPT. We evaluate the inference performance by using different CPTs.

After the attribute assignment, we obtain a social network. To infer each individual, we built a corresponding Bayesian network, and then conducted Bayesian inference as described in Section 3.

4.3 Experimental Results

Comparison of Bayesian and Naive Inference. In the first set of experiments, we compare the performance of Bayesian inference with naive inference. We want to study whether we can utilize the social relations to improve inference accuracy. We fix the prior probability to 0.3 and vary the influence strength from 0.1 to 0.9. Fig. 3 shows the inference accuracy of the two methods. It is clear that Bayesian inference outperforms naive inference. The curve for naive inference fluctuates around 70%, because with the prior probability being 0.3, the average accuracy we can achieve is 70%. The performance of Bayesian inference varies with influence strength. We achieve a very high accuracy, especially at high influence strength. The accuracy even reaches 95% for the influence strength 0.9, which is much higher than the 70% accuracy of the naive inference. We observed the same trend for other prior probabilities as well.

Effect of Influence Strength and Prior Probability. Fig. 4 shows the inference accuracy of Bayesian inference when the prior probability is 0.05, 0.1, 0.3 and 0.5, and the influence strength varies from 0.1 to 0.9. As the prior probability varies, the inference accuracy yields different trends with the influence strength. The lowest inference accuracy always occurs when the influence strength is equal to the prior probability. For example, the lowest inference accuracy (approximately 70%) at the prior probability 0.3 is achieved when the influence strength is 0.3. This is because when the influence strength is equal to the prior probability, knowing friend relations provide no more information than just knowing the prior probability; thus, people in the network are actually independent of each other. Furthermore, the higher the difference between the influence strength and the prior probability, the stronger the influence (no

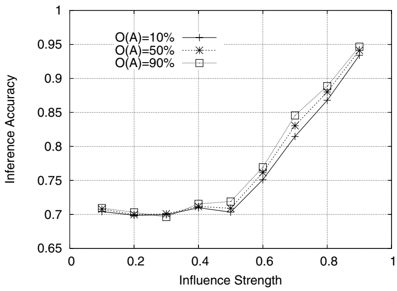

Fig. 5. Inference accuracy of Bayesian inference for different society openness.

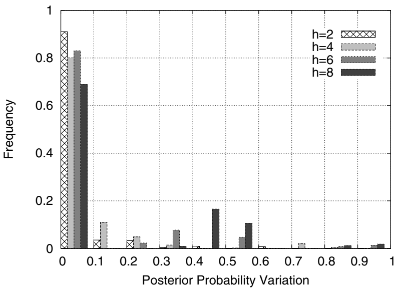

Fig. 6. Frequency of posterior probability variation for single hop inference.

matter positive or negative) of parent on children, and the better the Bayesian inference performs.

Society Openness. In the previous experiments, we assume the society openness is 100%. That is, all the friends' attribute values of the query node are known. In this set of experiments, we study the inference behavior at different levels of society openness. We randomly hide the attributes of a certain percentage of members, ranging from 10% to 90%, and then perform Bayesian inference on those nodes.

Fig. 5 shows the experimental results for the prior probability $P(X = t) = 0.3$ and the society openness $O(A) = 10\%, 50\%$ and 90%. The inference accuracy decreases as more members hide their attributes. For instance, at influence strength 0.7, when the openness is decreased from 90% to 10%, the accuracy reduces from 84.6% to 81.5%. However, the reduction in inference accuracy is relatively small (on average less than 5%). We also observe similar trends for other prior probabilities. This phenomenon is quite counterintuitive. Generally, when the society openness is small, the observed evidence on friends' attributes is low and the inference accuracy should drop drastically. To better understand the impact of openness, we perform some analysis in the next section.

5 Discussions on Society Openness

In this section, we want to obtain some insight about the impact that society openness has on the inference accuracy through analysis and simulations in simple regular social network structures. We consider single hop inference in two-level trees and multiple hops inference in complete k-ary trees.

5.1 Single Hop Inference

As mentioned earlier, the Bayesian network for single hop inference is a two-level tree. Given a general two-level tree with the query node X as the root and n_1 direct friends Y_{11}, ..., Y_{1n_1} as leaves, we want to derive the probability distribution of the posterior probability variation due to the change of openness, i.e., the difference of the posterior probability and the probability that this difference occurs. We change the openness by randomly hiding a certain percentage of friends' attributes.

Let random variables N_{1t} and N'_{1t} be the number of friends having attribute value t before and after hiding the attribute values of h friends, where $0 \leq h \leq n_1$ and $max(0, N_{1t} - h) \leq N'_{1t} \leq min(N_{1t}, n_1 - h)$. If $N_{1t} = n_{1t}$ and $N'_{1t} = n'_{1t}$, we can compute the posterior probabilities $P(X = t \mid N_{1t} = n_{1t})$ and $P(X = t \mid N'_{1t} = n'_{1t})$ from (3) respectively. Note that for Bayesian inference, hiding friends' attribute values in a two-level tree has the same effect as removing these nodes. Therefore, the posterior probability variation caused by hiding h attribute values is:

$$\varDelta P(X = t \mid N_{1t} = n_{1t}, N'_{1t} = n'_{1t}) = |P(X = t \mid N_{1t} = n_{1t}) - P(X = t \mid N'_{1t} = n'_{1t})|. \tag{5}$$

Now we want to derive the probability that each possible value of $\varDelta P(X = t \mid N_{1t} = n_{1t}, N'_{1t} = n'_{1t})$ occurs. In other words, we want to compute the probability of the joint event $N_{1t} = n_{1t}$ and $N'_{1t} = n'_{1t}$ (before and after hiding nodes), which is equal to:

$$P(N_{1t} = n_{1t}, N'_{1t} = n'_{1t}) = P(N_{1t} = n_{1t}) \cdot P(N'_{1t} = n'_{1t} \mid N_{1t} = n_{1t}). \tag{6}$$

Thus, we need to compute the two terms on the right-hand side of the equation.

Initially, if we know X's attribute value is x ($x \in \{t, f\}$), the probability that $N_{1t} = n_{1t}$ follows the Binomial distribution:

$$P(N_{1t} = n_{1t} \mid X = x) = \binom{n_1}{n_{1t}} \cdot P(Y = t \mid X = x)^{n_{1t}} \cdot P(Y = f \mid X = x)^{n_1 - n_{1t}}. \tag{7}$$

By unconditioning on X, we obtain:

$$P(N_{1t} = n_{1t}) = P(X = t) \cdot P(N_{1t} = n_{1t} \mid X = t) + P(X = f) \cdot P(N_{1t} = n_{1t} \mid X = f). \tag{8}$$

We define h_t and h_f as the numbers of hidden nodes with attribute t and f, respectively ($h_t = n_{1t} - n'_{1t}$ and $h_f = h - h_t$). Then we can compute the conditional probability that $N'_{1t} = n'_{1t}$ given $N_{1t} = n_{1t}$ as:

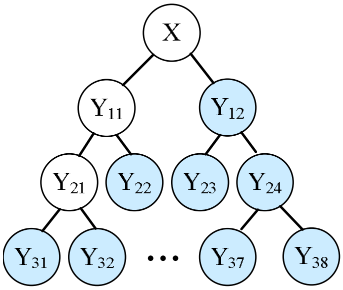

Fig. 7. An example for multiple hops inference when k=2 and d=2

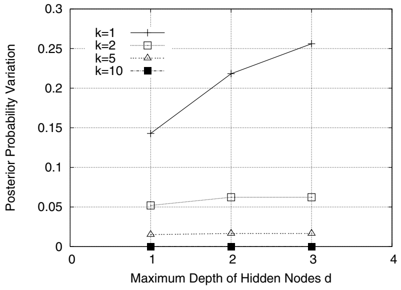

Fig. 8. Posterior probability variation for multiple hops inference

$$P(N'_{1t} = n'_{1t} \mid N_{1t} = n_{1t}) = \frac{\binom{n_{1t}}{h_t} \cdot \binom{n_1 - n_{1t}}{h_f}}{\binom{n_1}{h}}. \tag{9}$$

In this equation, the numerator represents the number of ways to hide h_t friends with value t and h_f friends with value f, and the denominator represents the number of combinations to choose any h nodes from a total of n_1 nodes. Substituting (8) and (9) into (6), we obtain $P(N_{1t} = n_{1t}, N'_{1t} = n'_{1t})$.

In the simulation study, we fix n_1 to be 10. To obtain the posterior probability variation $\varDelta P(X = t \mid N_{1t} = n_{1t}, N'_{1t} = n'_{1t})$ and its corresponding probability for each possible combination of n_{1t} and n'_{1t}, we vary h from 2 to 8. We plot the histogram of the posterior probability variation as follows. We divide the range of posterior probability variation into 10 equal width intervals. Then we compute the probability that the posterior probability variation falls in each interval.

Fig. 6 shows the histogram of the posterior probability variation when the prior probability is 0.3 and the influence strength is 0.7. The x axis represents the intervals and the y axis represents the frequency of the posterior probability variation within the interval. We observe that for 70% to 90% of the cases, the variation is less than 0.1. Thus, in single hop inference, the posterior probability is unlikely to be varied greatly due to hiding nodes randomly.

5.2 Multiple Hops Inference

For multiple hops inference, we use complete k-ary trees, in which all the internal nodes have k children. We hide a node with all of its ancestors in the tree, and check how the posterior probability varies with k and the maximum depth of the hidden nodes d. Fig. 7 depicts an example of when $k = 2$ and $d = 2$. The attribute values of Y_{11} and Y_{21} are hidden.

Fig. 8 plots the posterior probability variation when we vary k and d in a k-ary tree. The prior probability is 0.3 and the influence strength is 0.7. As k increases, the posterior probability variation before and after hiding nodes decreases, because there are increasingly more direct friends and the inference result will depend less on the hidden nodes. Moreover, when $k = 1$, the posterior probability varies more significantly when the maximum depth of hidden nodes is larger. For $k > 1$, the posterior probability does not vary much with the depth. These two observations show that, if there are many closer friends to the query node, a friend that is further away has little impact on the posterior probability. For our experiments in Section 4, the majority of the nodes have multiple direct friends. For example, about half of the population have more than 10 direct friends. As a result, openness in such an environment yields small variations of posterior probability which result in small changes in inference accuracy.

6 Conclusions

In this paper, we investigated the problem of privacy inference in social networks. Using Bayesian networks to model the causal relations among people in social networks, we performed a series of experiments on the real social network structures. We showed that privacy may be indirectly released via social relations, and the inference accuracy of privacy information is closely related to the inference strength between friends. Further, we observed that even in a society where people hide their attributes, privacy still could be inferred from Bayesian inference.

To protect privacy disclosure in social networks, we could either hide our friendship relations or ask our friends to hide their attributes. However, our analysis showed that randomly hiding friends' attributes and hiding people's attributes at multiple hops away have a small impact on privacy inference. Therefore, effective privacy protection should selectively hide friendship relations or friends' attributes. To achieve this, we should take both social network structures and influence strength of social relations into consideration. We plan to investigate this issue in our future work.

References

1. *Livejournal.* http://www.livejournal.com.
2. S. Brin and L. Page. The anatomy of a large-scale hypertextual Web search engine. In *Proceedings of the Seventh International World Wide Web Conference*, 1998.
3. P. Domingos and M. Richardson. Mining the network value of customers. In *Proceedings of the 7th International Conference on Knowledge Discovery and Data Mining*, 2001.
4. D. Heckerman. A Tutorial on Learning Bayesian Networks. Technical Report MSR-TR-95-06, March 1995.
5. D. Heckerman, D. Geiger, and D. M. Chickering. Learning bayesian networks: The combination of knowledge and statistical data. In *KDD Workshop*, pages 85–96, 1994.
6. H. Kautz, B. Selman, and M. Shah. Referral Web: Combining social networks and collaborative filtering. *Communications of the ACM*, 40(3):63–65, 1997.
7. D. Lowd and P. Domingos. Naive bayes models for probability estimation. In *Proceedings of the Twenty-Second International Conference on Machine Learning (ICML)*, Bonn, Germany, 2005. ACM Press.
8. S. Milgram. The small world problem. *Psychology Today*, 1967.
9. D. K. A. P. N. Friedman, L. Getoor. Learning probabilistic relational models. In *Proceedings of the 16th International Joint Conference on Artificial Intelligence (IJCAI)*, Stockholm, Sweden, August 1999.
10. M. Newman. The structure and function of complex networks. *SIAM Review*, 45(2):167–256, 2003.
11. U. D. of Health and O. for Civil Rights Human Services. *Standards for Privacy of Individually Identifiable Health Information*, 2003. http://www.hhs.gov/ocr/combinedregtext.pdf.
12. W. W. W. C. (W3C). *The platform for privacy preferences 1.1 (P3P1.1)*, 2004. http://www.w3.org/TR/P3P11/.
13. D. J. Watts and S. H. Strogatz. Collective dynamics of "small-world" networks. *Nature*, 1998.
14. N. L. Zhang and D. Poole. Exploiting causal independence in bayesian network inference. *Journal of Artificial Intelligence Research*, 5:301–328, 1996.