# Neighbourhood-Pair Attack in Social Network Data Publishing

Mohd Izuan Hafez Ninggal(✉) and Jemal H. Abawajy

Parallel and Distributed Computing Lab School of Information Technology, Deakin University, Victoria, Australia
{mninggal, jemal}@deakin.edu.au

**Abstract.** Vertex re-identification is one of the significant and challenging problems in social network. In this paper, we show a new type of vertex re-identification attack called neighbourhood-pair attack. This attack utilizes the neighbourhood topologies of two connected vertices. We show both theoretically and empirically that this attack is possible on anonymized social network and has higher re-identification rate than the existing structural attacks.

## 1 Introduction

Data publishing agencies, such as healthcare providers and public services, face fundamental challenges in how to release data to the public without violating the confidentiality of personal information. This problem has recently received considerable traction as more and more social network data has been released publicly to enable social network data analysis [1]. Currently, the privacy of individuals and the confidentiality of data in social network data publishing are protected through variety anonymization techniques. Some of these techniques include removing vertices labels such as the name or other personally identifiable information, the *k*-anonymity and *l*-diversity approaches for privacy [11] to conceal the identity of the individuals.

Privacy preservation in publishing social networks data is a challenging problem [2]. This is because a social network data has numerous types of structural information which could be manipulated by an adversary to re-identify individuals and breach their privacy. For example, the degree attack [3] manipulates the number of links of the targeted vertex. Similarly, the neighbourhood attack [2, 4] manipulates the link patterns among the direct neighbours of the targeted vertex in a social network.

In this paper, we present a new type of privacy attack called neighbourhood-pair attack in a social network. This attack utilizes the neighbourhood structure of a pair of connected vertices as the background knowledge of an adversary to query and re-identify targeted victims in a released social network data. Since neighbourhood pair structure consists of a large size of sub-graph, we identify a technique of how the structure of the neighbourhood-pair could be represented and show its practicality to facilitate the vertex re-identification.

The rest of the paper is structured as follows. In Sect. 2, the models used in the paper are discussed. The proposed attack and its analysis are discussed in Sect. 3 and 4 respectively. The conclusion is given in Sect. 5.


I. Stojmenovic et al. (Eds.): MOBIQUITOUS 2013, LNICST 131, pp. 726–731, 2014.
DOI: 10.1007/978-3-319-11569-6_61

## 2 Models

We model a social network data as a graph characterized as $G(V, E)$ where $V = \{v_1, v_2, \ldots, v_n\}$ is a set of $n$ unlabeled vertices representing individuals in the social network. We represent the social links between individuals via unlabelled undirected edges $E \subseteq V \times V$. We assume that the data publisher releases useful social network data in a way that satisfies the data users need while at the same time preserving private information about the individuals in the data. To this end, we assume that the social network data graph $G(V, E)$ is sanitized into $\bar{G}(\bar{V}, \bar{E})$ before publishing using $k$-anonymization mechanism with $k = 2$.

An adversary $\mathcal{A}$ is interested in deriving private information such as the identity of an individual or an attribute value from $\bar{v} \in \bar{V}$. The outcome of structural attack depends on the background knowledge that an adversary $\mathcal{A}$ has. In [2, 5, 6], it is assumed that the adversary knows large set of structural information regarding the target vertex in a social network. In contrast, we assume that $\mathcal{A}$ knows the neighbourhood-pair information (shown in Fig. 1d) of $\bar{v} \in \bar{V}$ and $\bar{v} \in \bar{V}$ where $\bar{u}$ is an adjacent vertex of a vertex $\bar{v}$ such that $\bar{v} \neq \bar{u}$.

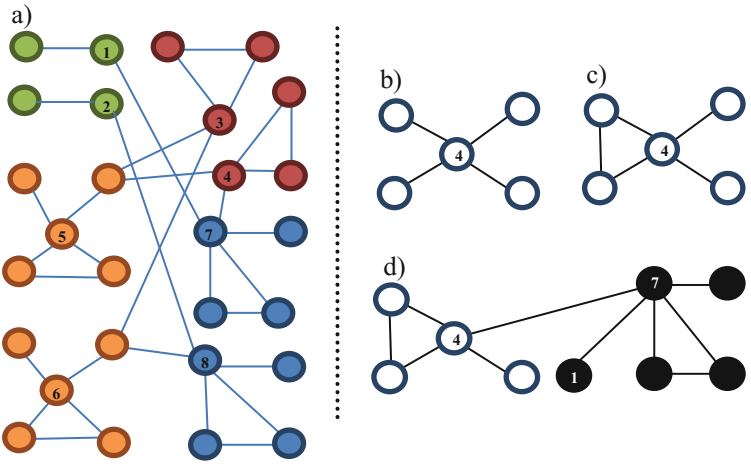


**Fig. 1.** An anonymized graph $\bar{G}(\bar{V}, \bar{E})$ (left) and structural knowledge (right).

## 3 Neighbourhood-Pair Attack

In this section, we present a new type of privacy attack called neighbourhood-pair attack in a social network. We will first define some background information needed to carry out the attack.

*DEFINITION 1 (**Structural Query**): Given a social network $G(V, E)$ and a target individual $t \in V$, a structural query $q$ returns a set of vertices $\dot{v} \subset V$ based on the structural properties of $t \in V$.*

In the proposed neighbourhood-pair attack, an adversary $\mathcal{A}$ utilizes the neighbourhood structure of a pair of connected vertices as the background knowledge to re-identify targeted victims in an anonymised social network data. Specifically, let $t \in V$ and $u \in V$ be adjacent vertices in $G$ such that $t \in V$ represents the target vertex where $t \neq u$. To utilise neighbourhood-pair information, the first step is to query the target vertex $t \in V$ by using the degree information. Assume the query returns a set of matching vertices $x \subset V$. The smaller the cardinality of matching vertices (i.e., $x$) is the higher the probability that the target victim $t \in V$ could be re-identified. To filter out $x$ in order to find $t$, the adversary then compares the link structure among every neighbours of $x$. By this, the adversary has manipulated the neighbourhood information for the query. We denote the set of matching vertices from the previous step as $y$. Assume the return set $y > 1$. The adversary then uses the neighbourhood information of $u$ to find $t$ in $y$. The target victim could be definitely re-identified if and only if the cardinality of matching vertices is 1.

We now illustrate the neighbourhood-pair attack. Figure 1a is a sample of an anonymized social network graph. In fact, the social network graph is resistant to the degree attack [3] and the neighbourhood attack [2, 4]. By referring to Fig. 1a, assume the target victim is John who in the graph has been anonymized as vertex #4. When the adversary tries to query John using degree (Fig. 1b) and neighbourhood information (Fig. 1c), the matching vertices give ¼ probabilities because the query returns at least four equivalent vertices. However, if the adversary knows that one of the individuals, who John is linked to, is connected to other five persons (including John) and that two of these five persons are directly connected, then John could still be uniquely re-identified as vertex 4.

Since neighbourhood pair structure consists of a large size of sub-graph, we identify a technique of how the structure of the neighbourhood-pair could be represented and how it can be used to facilitate the vertex re-identification. Essentially, the proposed technique transforms a given set of neighborhood information into a coefficient form. The goal is to simplify the information yet comprehensive enough to represent the neighborhood set of a given vertex. First, we define the Neighbourhood Coefficient as follows:

*DEFINITION 2 (**Neighbourhood Coefficient**): Given a set of vertices that comprise a neighbourhood of vertex v, the neighbourhood coefficient **(NC)** is calculated by:*

$$NC = \frac{\gamma(v)}{\delta(v)} + d(v) \tag{1}$$

where $d(v)$ is the degree of vertex $v$; $\gamma(v) = \{e_{ij} : v_i, v_j \in N, e_{ij} \in E\}$ is the existing links between the direct neighbours of $v$; $\delta(v)$ is the maximum number of links that could possibly exist between the direct neighbours of $v$ and defined by $\frac{[|N|.[|N|-1]]}{2}$.

For example, in the neighbourhood sub-graph in Fig. 1c, the vertex #4 has four neighbours and two of them are connected together. To transform this information into the NC, we first count the neighbours of vertex #4 which happens to be 4. Then we calculate the links that exist among the 4 neighbours of vertex #4. We find there is only 1 link connection that exists among the neighbours out of the maximum possible connections. We then calculate the maximum links that could possibly exist among

these four neighbours by $\frac{[|4|.[|4|-1]]}{2} = 6$. The denominator is 2 because the graph considered here is undirected. Having that, the neighbourhood coefficient is $\frac{1}{6} + 4 = 4.167$. We include the degree information in the calculation because we want to differentiate between the fractions with common denominator. For instance, between $\frac{1}{3}$ and $\frac{2}{6}$. To use NC for query, all the vertices in the graph must be transformed into neighbourhood coefficient. Having the neighbourhood coefficient list, the adversary can then perform mapping using the particular neighbourhood-pair coefficient of the target victim that he already have in hand. The neighbourhood-pair is transcribed as:

$$NP = [NC_t, NC_u] \tag{2}$$

where $NP$ is neighbourhood-pair, $NC$ is the Neighbourhood Coefficient defined in (1), $v$ is the targeted victim and $u$ is one of the neighbours of $v$.

## 4 Performance Analysis

In this section, we analyses the performance of the proposed attack and compare it with the degree attack [3] and the neighbourhood attack [2, 4].

PROPOSITION 1: Neighbourhood-Pair attack has higher re-identification rate than degree and neighbourhood attack.

PROOF. Let $v_j$ be a set of vertices, $u_k$ be another set of vertices that are directly connected to $v_j$ where $u_k \neq v_j$. Given $D(v_j)$ is the number of neighbours for vertex $v_j$ called degree and $N(v_j)$ as the information about the links between $u_k$ called neighbourhood. We denote $D(v_j) \subset N(v_j)$ as to show that the information about the neighbourhood does also include the information about the degree. Given $NP\{N(v_j), N(v_l)\}$ as the pair of neighbourhood for vertex $v_j$ and $v_l$, then we denote $N(v_j) \subset NP[N(v_j), N(v_l)]$ to show that the neighbourhood-pair structure also does include neighbourhood information. Thus, we get $NP\{N(v_j), N(v_l)\} \supset N(v_j) \supset D(v_j)$ which means the neighbourhood-pair information has higher structural characteristic

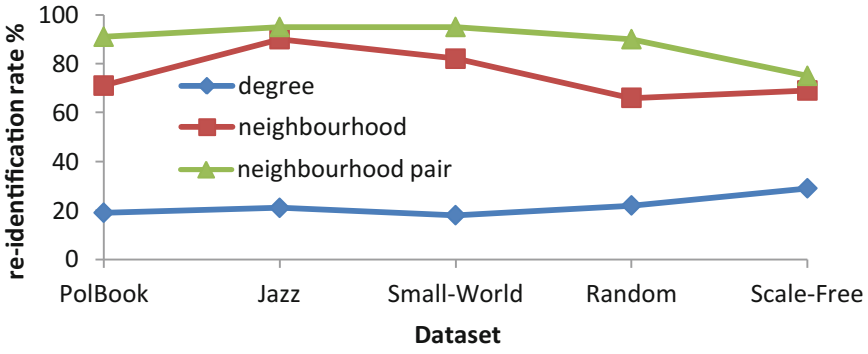


**Fig. 2.** The re-identification rate comparison graph

than the degree and neighbourhood information. Hence, using neighbourhood-pair to query target victim increases the chance of re-identification. ■

The graph in Fig. 2 compares the re-identification rate among the three types of structural information over the five different datasets (i.e., **PolBooks**: a network of books sold by an online store where the edges between books represent the purchase frequency of the same buyers; **Jazz Musician Network**: a network of jazz musicians who collaborate in different bands. The vertices represent the band and edges represent the musicians in common; **Scale-Free**: a synthetic network with a power-law vertex degree distribution; **Random:** a synthetic random network where the vertices in this network are randomly connected based on probability $p$; and **Small-World:** a type of graph in which most vertices can be reached from every other vertex by a small number of hops).

The percentage represents the amount of vertex that is the dataset that are exposed to re-identification attack using the three types of graph structural information. The graph only covers unique matching vertices from the structural query that we performed. We ignore the vertices match that has 50 % probability. Therefore, this graph only shows the rate of vertices that definitely re-identified. The degree attack has set 20–30 % of the users to be definitely re-identified over all datasets that we tested. Even though this rate gives significant percentage in terms of the number of users who are in risk, the neighbourhood structural information gives more than double of the re-identification risk. Through all the datasets, more than 60 % of the users are definitely re-identified using neighbourhood information. However, it is evident that the re-identification rate using the neighbourhood-pair scored the highest in all five datasets.

## 5 Conclusion

In this paper, we identified a new type of attack called neighbourhood-pair attack to distinguish people in a dataset. We also proposed the neighbourhood coefficient to transform neighbourhood information into more simple form for query. We have shown theoretically and empirically that using the neighbourhood-pair structural information, the adversary has higher chances to successfully re-identify targeted victim.

## References

1. Arnaboldi,V., et al.: Analysis of ego network structure in online social networks. In: Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom), pp. 31–40 (2012)
2. Zhou, B., Pei, J.: Preserving privacy in social networks against neighborhood attacks. In: IEEE 24th International Conference on Data Engineering, ICDE 2008, pp. 506–515. IEEE (2008)
3. Liu, K., Terzi, E.: Towards identity anonymization on graphs. In: Presented at the Proceedings of the 2008 ACM SIGMOD International Conference on Management of Data, Vancouver, Canada (2008)
4. Zhou, B., Pei, J.: The k-anonymity and l-diversity approaches for privacy preservation in social networks against neighborhood attacks. Knowledge and Information Syst. 1–31 (2010)

5. Zou, L., et al.: K-automorphism: A general framework for privacy preserving network publication. In: Proceedings of the VLDB Endowment, vol. 2, pp. 946–957 (2009)
6. Cheng, J., et al.: K-isomorphism: privacy preserving network publication against structural attacks. In: Proceedings of the 2010 ACM SIGMOD International Conference on Management of data, pp. 459–470 (2010)