Group Relational Privacy Protection on Time-constrained Point of Interests

Bo NING, Xiaonan Li, Fan YANG, Yunhao SUN, Guanyu LI, George Y. YUAN

Frontiers of Computer Science, DOI: 10.1007/s11704-022-2090-9

Model and Our Approach

- **$k^{m,n}$-Anonymity Model**: Given a time-constrained data set $D(U, I)$ of users, a $k^{m,n}$-anonymity is used to make the number of each vulnerable PoIs in D not less than k, where m and n denote the number of common PoIs of two-user and multi-user as the prior knowledge known by attackers, respectively.
- **Our Approach:** Anonymous Algorithm of User Relationship

Algorithm 1: Anonymous Algorithm of User Relationship

Input: time-constrained data set of user PoIs $D(U, I)$, prior knowledge m, n, k, distance matrix M
Output: anonymous data set $\mathcal{D}$

```
1  for u, u' ∈ U do
2      R^m_single ← R^m_single(u, u');
3  for u ∈ U and r ∈ R^m_single do
4      R^n_group ← R^n_group(u, u');
5      Tree ← Root(r) ∪ Node(u, r);
6  if m ≤ n then
7      anonymize R^m_single on D limited by M;
8  else
9      for r ∈ R^m_single do
10         anonymize r on D limited by M;
11         iteratively update and anonymize nodes in Tree(r)
             limited by M;
```

Algorithm Description: Algorithm 1 consists of two subroutines. The first subroutine is to construct the user relationships as a tree (Lines 1-5). The tree is rooted by the single-relationship R^m_{single} and takes the group-relationship R^n_{group} as node, where the branches denote a user linking single-relationship and group-relationship (Line 5). The second subroutine is to anonymize the user PoIs in time-constrained data set D (Lines 6-11). According to Section 3.2, the m prior knowledge is meaningless in group relationship if n is bigger than m.

Therefore, the user PoIs of single-relationship are only anonymized if $m \leq n$ (Lines 6-7), otherwise both user PoIs of single-relationship and group-relationship are anonymized (Lines 9- 11). The anonymous strategy is executed in a tree, iteratively (Line 11). If one node have been anonymized, its descendant nodes are verified whether there still exists group-relationship or not. If one descendant node still satisfie the group-relationship, the node is anonymized and verifies its descendant nodes.

Experimental Result and Conclusions

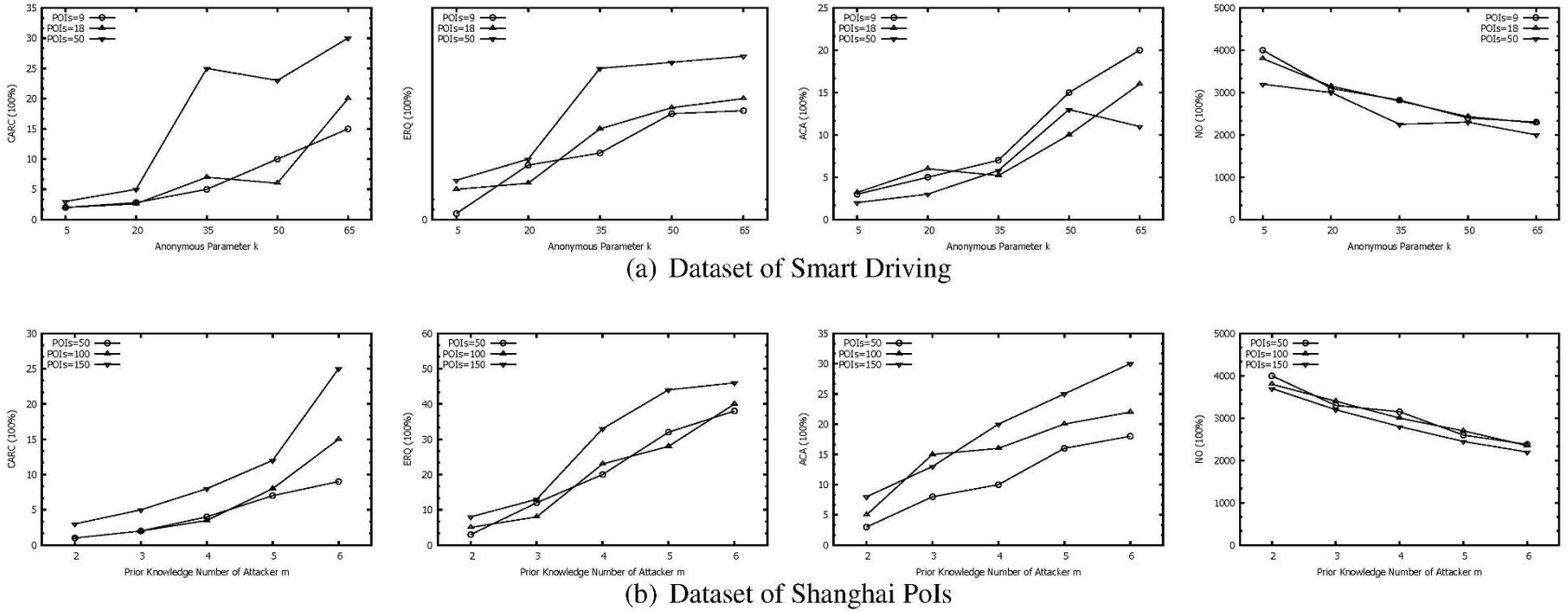

Fig.2: Experiments of CARC, ERQ, Average CA(ACA) and Number of changing PoIs

Experimental Result: Figure 2 shown that the values of CARC, ERQ and ACA appear an overall upward trend as the increase of m and the unmodified number of points of interest NO has been shown a downward trend. This upward trend mean that the anonymous data has a worse data and query availability and decreased number of NO refers to a more laborious anonymous operations. In general, the larger the value of m is, the worse the data availability of anonymous data is.

Conclusions: This paper designed an algorithm to protect the privacy relationship exposed by the user PoIs. Through the experimental evaluation, our method can protect the time-constrained PoIs under the hypothetical prior knowledge of attackers.