Location Privacy Protection on Social Networks

JUSTIN ZHAN AND XING FANG

PRESENTED BY MATTHEW GRUNERT

Problem

- Location information is considered private
- Little effort has been made to address this problem
- Location information can be used to track a person's movements

Prior Work

Amoli et al.

- 2PLoc (Preserve Privacy in Location based services) aimed to provide anonymity of location based on onetime tickets regardless of the existence of any trusted third party.
- The protocol satisfies the requirement of accurate location use, as well as the ability of revoking anonymity on the ticket double spending.
- The user, location-based service provider, and the ticket issuer are the three untrusted parties in 2PLoc.
- 2PLoc is based on a special designed ticket that disconnects the relation between the location of the mobile user and its identity

Prior Work

Kamat et al. & Taheri et al.

- ANDOR
  - Suggests using route pseudonyms instead of node IDs during the routing process
  - Street names vs. Location coordinates
- ARM
  - Two nodes share a secret key
- RDIS
  - Destination location privacy protection

Prior Work

Lipford et al. & Ho et al.

- Lipford's New Privacy Setting Interface
  - Based on Facebook that makes significantly improved understanding on the settings as well as better performance.
  - The interface enables a set of HTML tabs, each providing a different browser's view of Facebook users' account information.
- Ho's Problems with Privacy
  - Users are not notified by social networks when their personal information is at privacy risks.
  - Existing privacy protection tools in social networks are not flexible enough.
  - users cannot prevent information that may reveal the privacy of themselves from being uploaded by any other users

Contributions

Algorithm 1. The Encryption Approach

Input: m
Output: $En(m)$
1: **for** every m **do**
2: $T(m) = LocationTag(m)$
3: **end for**
4: **if** $(T(m) \in \emptyset \; or \; T(m) \not\subseteq T(u))$ **then**
5: **return** $null$
6: **else if** (Encrypt = =1$and \; PK \notin \emptyset$) **then**
7: $En(m) = \{m\}_{PK}$
8: **else**
9: **return** $null$
10:**end if**

Contributions

Algorithm 3. The k-anonymize algorithm

Input: $m, T(m)$
Output: $k_{anon}(m)$
1:**for** every $T(m) \in m$ **do**
2: **if** $(|T(m) \in DB| \geq 2)$ **then**
3: **return** $T(m)$
4: **else** $T(m) \leftarrow *$
5: **return** $T(m)$
6: **end if**
7: **end for**
8: $k_{anon}(m) \leftarrow T(m)$
9: **return** $k_{anon}(m)$

Contributions

Algorithm 5. The Noise-Inject algorithm

Input: $m, T(m)$
Output: $Noise_{injected}(m)$

if $(citylevel == 1)$ **then**
  for every $T(m) \in \{city\} \in DB$ **do**
    $T(m) \leftarrow T(m) \cup \{T_{noise}(city, zip\ code)\}$
  end for
else if $(statelevel == 1)$ **then**
  for every $T(m) \in \{city\} \cup \{zip\ code\} \in DB$ **do**
    $T(m) \leftarrow *$
  end for
  for every $T(m) \in \{state\} \in DB$ **do**
    $T(m) \leftarrow T(m) \cup \{T_{noise}(state)\}$
  end for
else return $null$
end if
$Noise_{injected}(m) \leftarrow T(m)$
return $Noise_{injected}(m)$

Conclusions and Onward

- Only collected city level geo-locations in United States.
- Expand database to include geo-location information lower than city level.
- Grants users flexibilities for selecting protection techniques.
- Imposes burdens such as the understanding of protection techniques to users.
- Integrate linguistic analysis to allow system to automatically select the best protection technique for each user