Personalized Protection of Identifiers on Public Trajectories

Jeppe R. Thomsen

Aalborg University
Department of Computer Science

November 8, 2010
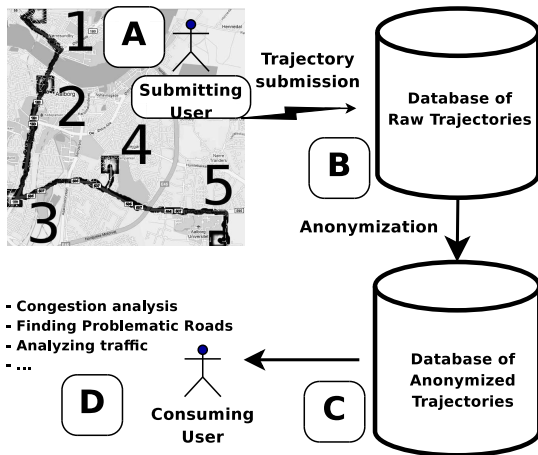
Overview

Problem Setting

Privacy Profile

t-anonymity

Conclusion

Introduction
Privacy Profile
Conclusion

Problem Setting
Goals
Related work

Problem Setting

A Privacy Aware User

B Trusted Server

C Public Untrusted Server

D Service Providers

Goals

At the service provider:

- Remove all user identifying information from trajectories.
- Preserve usability to users of public dataset

At the users side:

- Provide **Usability**. specifying privacy should be simple.
- Be **Practical**. No user interaction during normal operation.
- Be **Flexible**. Support several ways of defining privacy.

Related work

Protection of Trajectories

- Collapse trajectories and remove updates
- Only publish edges with k support.

- At each update compute MBR including k-1 updates
- Precompute regions before sending.

- Degrade public dataset so no sub-trajectory can be matched to it.

No work on spatial anonymity with time

Introduction
Privacy Profile
Conclusion

Settings
t-anonymity
Time Period

Privacy Profile

- Settings
- PSR - Potentially Sensitive Region
- Protection types and schemes
- t-anonymity

Introduction
Privacy Profile
Conclusion

Settings
t-anonymity
Time Period

Settings

Users Can

- Set both globally and locally
    - Temporal sensitivity
    - Spatial sensitivity
- Define a PSR
- Have multiple profiles.

Definition (Privacy Profile)

$(stime, etime, d_s, d_t, \{PSR\})$

Introduction
Privacy Profile
Conclusion

Settings
t-anonymity
Time Period

PSR

- A group of edges in a road network considered sensitive
- A value indicating spatial sensitivity
- A value indicating temporal sensitivity
- A general usage class

Definition (PSR)

A PSR p is a tuple $(p_{edges}, d_s, d_t, class)$ where p_{edges} is the set of tuples $\{(e, e_{from}, e_{to} | 0 \leq e_{from} < e_{to} \leq e_{length})\}$ which is sensitive. $e \in \mathbf{E}$ and $e_{from}, e_{to}, e_{length} \in \mathbb{R}$. e_{from}/e_{to} specifies on e the start-/end-location covered by p_{cover}. If e is fully included in p_{cover}, e_{from}/e_{to} is equal to $0/p_{length}$. $d_s, d_t, class \in \mathbb{N}$ is respectively the spatial sensitivity, the temporal sensitivity, and the PSR classification

Introduction
Privacy Profile
Conclusion

Settings
t-anonymity
Time Period

PSR Classes

Classification	Scheme
Public Service Point	AS
House	ASTI,RS
Route w. endpoints	AS, ASTI, RS
Route w/o endpoints	AS, ASTI, RS

Protection Schemes
- AS - Always Sensitive.
- ASTI - Always Sensitive within a time interval.
- RS - Rarely Sensitive.

Introduction
Privacy Profile
Conclusion

Settings
t-anonymity
Time Period

t-anonymity

Spatial k-anonymity

- Adapted for trajectories
- Argumented with time.

In a PSR:

- Spatial sensitivity decides t-1 trajectories to hide between
- Temporal sensitivity defines a time period shared with t-1 other trajectories.

Introduction
Privacy Profile
Conclusion

Settings
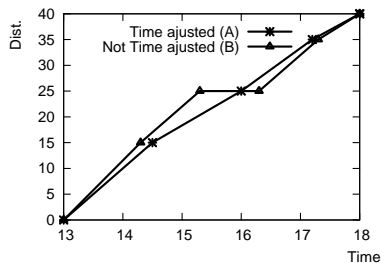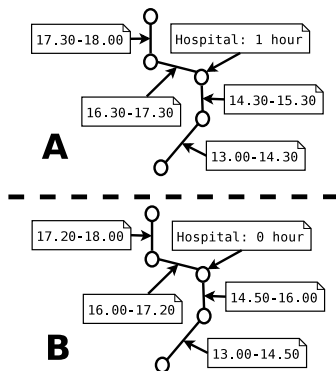**t-anonymity**
Time Period

Definition: t-anonymity

Definition (t-anonymity)

Given $\mathbf{T}$, the set of trajectories and p_{edges}, the set of edges covering a sensitive part of trajectory γ.

Let $\Gamma \subseteq \mathbf{T}$ be all trajectories which subtrajectories intersect with p_{edges}. $\Gamma' \subseteq \Gamma$ be all trajectories where, for edges intersecting with p_{edges}, at each timestamp of γ their timestamps lie within a time period TP symmetric around the timestamp of γ.

Γ' is said to satisfy t-anonymity with respect to TP and γ iff Γ' contains at least $t - 1$ other trajectories.

Introduction
Privacy Profile
Conclusion

Settings
t-anonymity
Time Period

Time Period

Conclusion

- Novel Privacy Profile to specify spatial-temporal sensitivity

- Introduced t-anonymity

- Introduced a way of temporally hiding users movements.

Future Work

- Performance study to determine a threshhold **D** for data integrety, to determine when data is no longer usable by data consumers.

End of Presentation

Thank You For Listening