PriSTE: Protecting Spatiotemporal Event Privacy in Continuous LBS

Yang Cao*#, Yonghui Xiao&, Li Xiong#, Liquan Bai#, Masatoshi Yoshikawa*
* Kyoto University, # Emory University, & Google Inc.
contact: yang@i.kyoto-u.ac.jp

Motivation

- When a user's perturbed locations are released **continuously**, existing LPPMs may not protect users' **secrets about spatiotemporal activities**.
- The secrets could be "visited hospital in the last week" or "regularly commuting between Address 1 and Address 2 every morning and afternoon" (it is easy to infer that Addresses 1 and 2 may be home and office), which we call it **spatiotemporal event**.

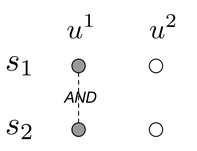
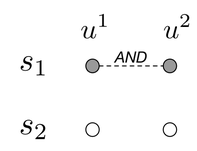
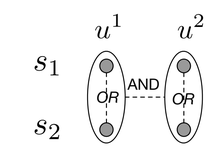
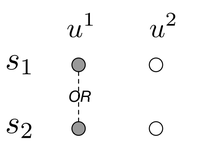
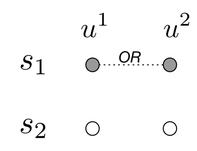
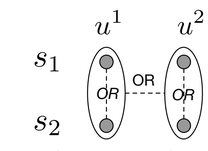
Spatial dimension	Temporal dimension	Spatial and Temporal
		
(a) $(u^1 = s_1) \wedge (u^1 = s_2)$	(c) $(u^1 = s_1) \wedge (u^2 = s_1)$	(e) $((u^1 = s_1) \vee (u^1 = s_2)) \wedge ((u^2 = s_1) \vee (u^2 = s_2))$
		
(b) $(u^1 = s_1) \vee (u^1 = s_2)$	(d) $(u^1 = s_1) \vee (u^2 = s_1)$	(f) $((u^1 = s_1) \vee (u^1 = s_2)) \vee ((u^2 = s_1) \vee (u^2 = s_2))$

Fig. 1: Six examples of spatiotemporal events.

Event (a) is always false.
Event (b) indicates a sensitive *region*.
Event (c) represents a sensitive *trajectory*.
Event (d) represents the *presence or not* in a sensitive location.
Event (e) indicates a *mobility pattern* passing through sensitive regions.
Event (f) indicates the *presence or not* in a sensitive region.

Spatiotemporal Event Privacy vs. Location Privacy

- Although the definition of spatiotemporal event is more general than a single location or a trajectory, the privacy metrics between spatiotemporal event privacy and location privacy can be **orthogonal.**

(a) indistinguishability-based Location Privacy (b) indistinguishability-based Trajectory Privacy (c) ε-Spatiotemporal Event Privacy

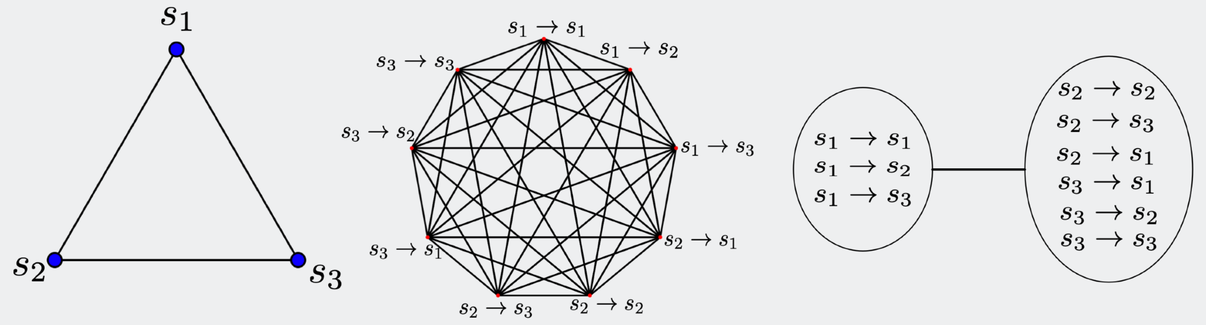


Fig.3 Illustration of indistinguishability-based privacy metrics.

- Given any Event(s) :

  ε-Spatiotemporal Event Privacy $\not\Rightarrow$ ε-Geo-Indistinguishability

  ε-Spatiotemporal Event Privacy $\not\Leftarrow$ ε-Geo-Indistinguishability

- The best of two worlds :
  - ✳ Location privacy = **general protection** against unknown risks when sharing location with the third parties,
  - ✳ spatiotemporal event privacy = **flexible and customizable protection** which may prevent against profiling attacks.

Formalize Spatiotemporal Event Privacy

Define Spatiotemporal Event

- We call $u^t = s_i$ **location-time predicate**, whose value can be *true* or *false* depending on the ground truth of u^t.
- A **spatiotemporal event** is defined as a Boolean expression of the location-time predicates using the AND, OR, NOT operators, denoted by $\wedge$, $\vee$, $\neg$, respectively.

Spatiotemporal Event	Boolean Expression
single location event	$u^t = s_i$
PRESENCE at a single location	$(u^1 = s_i) \vee (u^2 = s_i) \vee \cdots \vee (u^T = s_i)$
region event	$(u^t = s_i) \vee (u^t = s_j) \vee \cdots, \vee (u^t = s_k)$
single trajectory event	$(u^1 = s_i) \wedge (u^2 = s_j) \wedge \cdots, \wedge (u^n = s_k)$
PATTERN of trajectories	$((u^1 = s_i) \vee (u^1 = s_j) \vee \cdots, \vee (u^1 = s_k)) \wedge \cdots \wedge ((u^n = s_l) \vee (u^n = s_m) \vee \cdots, (u^n = s_n))$

Fig. 2: Examples of Spatiotemporal Events.

ε-Spatiotemporal Event Privacy

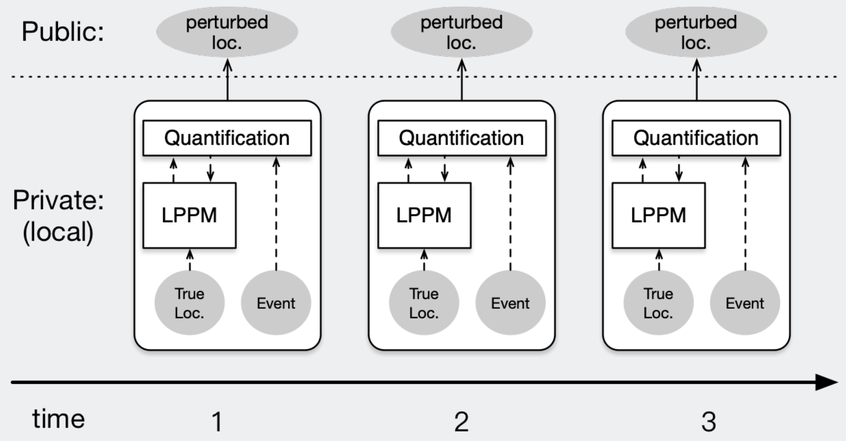
- A mechanism preserves -Spatiotemporal Event Privacy for a spatiotemporal event if at any timestamp t in {1, · · · , T} given any observations {o_1 , · · · , o_t }

$$\Pr(o_1, \cdots, o_t \mid Event) \leq e^{\epsilon} \Pr(o_1, \cdots, o_t \mid \neg Event)$$

where ***Event*** is a logic variable about the user-specified spatiotemporal event and ¬***Event*** denotes its negation.

PriSTE framework

- PriSTE (Private Spatiotemporal Event)
  - ✳ employ existing LPPM (e.g., Planar Laplace M. for Geo-I)
  - ✳ quantification algorithms
  - ✳ calibrate ε of PLM for ε-Spatiotemporal Event Privacy.



Experiments

- A **stricter LPPM** satisfies a certain level of spatiotemporal event privacy without any change.
- a **more loose LPPM** may need to reduce its privacy budget significantly for protecting the same event..

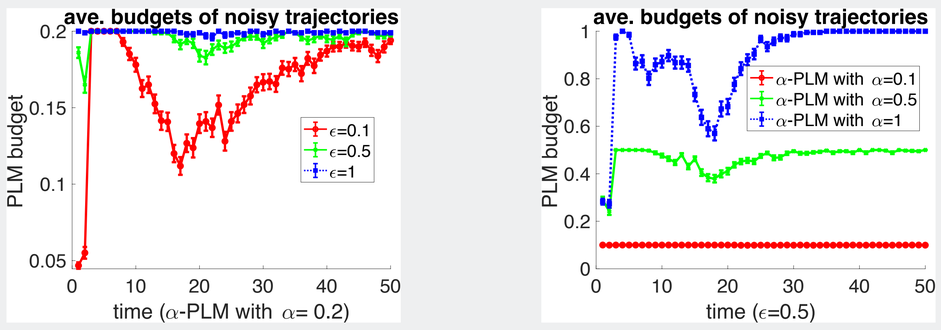


Fig.4 PRESENCE(S = {1 : 10}, T = {16 : 20})

See more details in a long version of our paper: https://arxiv.org/abs/1810.09152

Kyoto University & Emory University
This work is supported by NSF under grant No. 1618932, the AFOSR DDDAS program under grant FA9550-121-0240,
the Japan Society for the Promotion of Science (JSPS) Grant-in-Aid for Scientific Research (S) No. 17H06099 and (A) No. 18H04093.