The Long Road to Trajectory Privacy

Erik Buchholz, Alsharif Abuadbba, Shuo Wang, Surya Nepal, and Salil S Kanhere

UNSW Sydney

UNSW Institute for Cyber Security

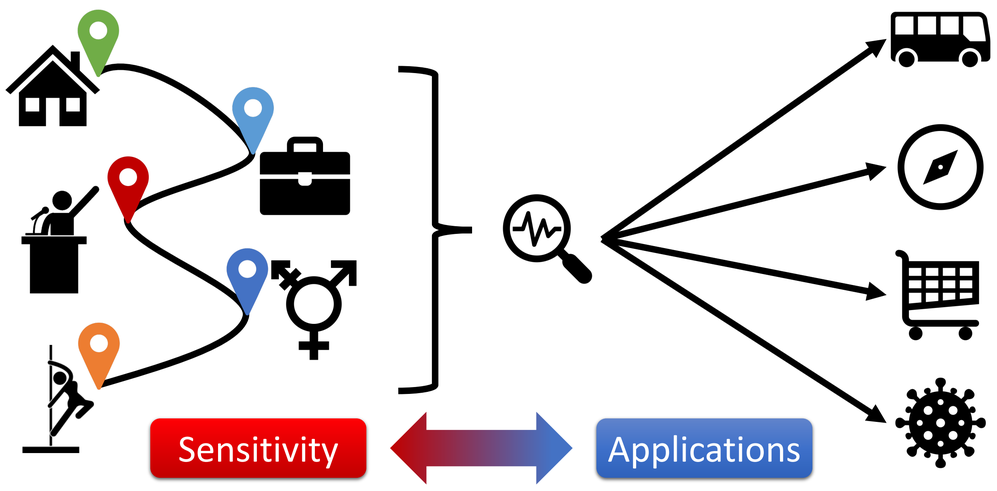
Motivation

Location trajectories are valuable for **many applications**:

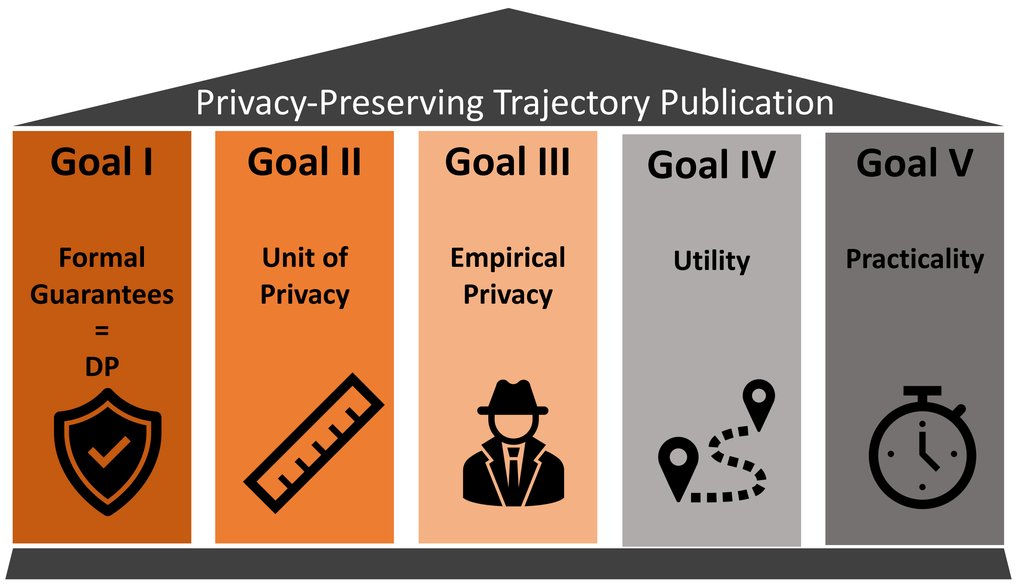
- Navigation, Targeted Marketing, City Planning, …

But: Trajectories reveal **sensitive information**:

- Sexual Orientation, Religious Beliefs, Political Opinions, …

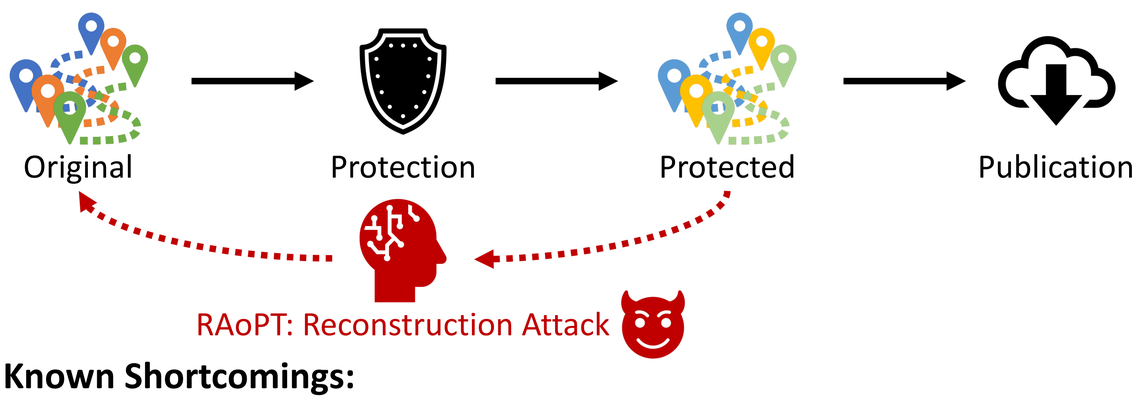


Proposed Framework



Traditional Approaches

Protect Dataset:



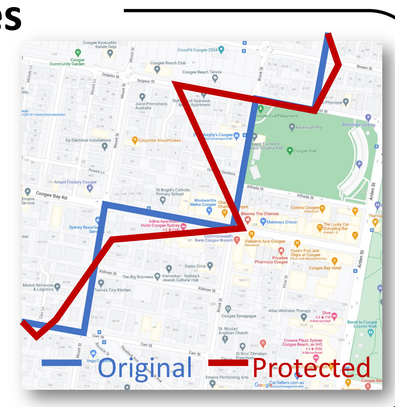
Known Shortcomings:

- **Broken DP Proofs:** Errors in Proofs
- **Grid Cells:** Reduced Granularity
- **Limited Domain:** Pre-Defined Locations
- **Aggregation:** Only Aggregated Results
- **Correlation:** Enables Attacks
- **Points Only:** Unconnected Loc. only

Structural Differences

Noise leads to **structural differences** between authentic and protected trajectories:

- Cars not following roads
- Ships passing over land



Contact

Paper

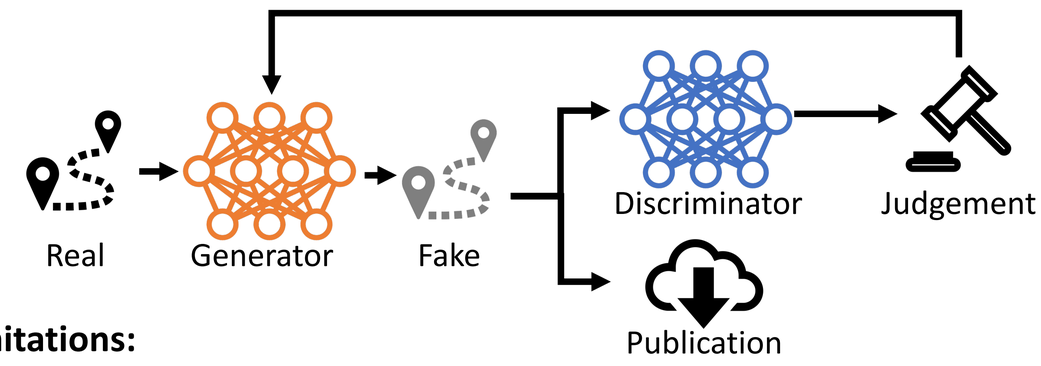
Artifacts

Author

Generative Models

Deep Learning-based Generative Models as Alternative?

LSTM-TrajGAN as the most common architecture:



Limitations:

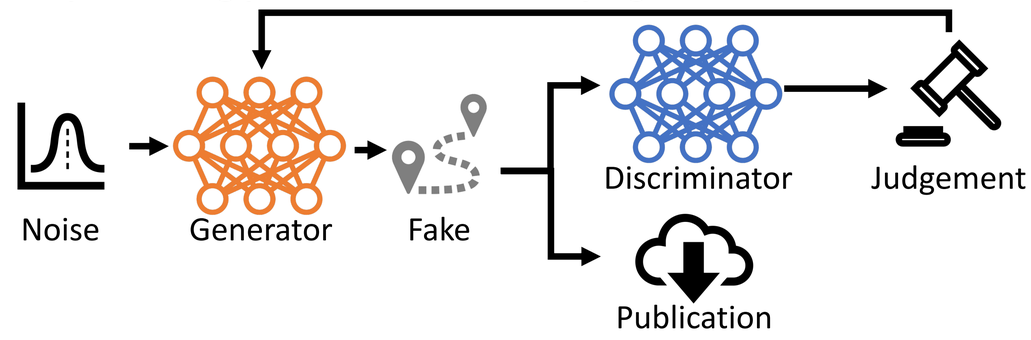
- No privacy **guarantees**
- Converges towards identity function → No privacy
- Vulnerable to reconstruction attacks (RAoPT)

Other Approaches:

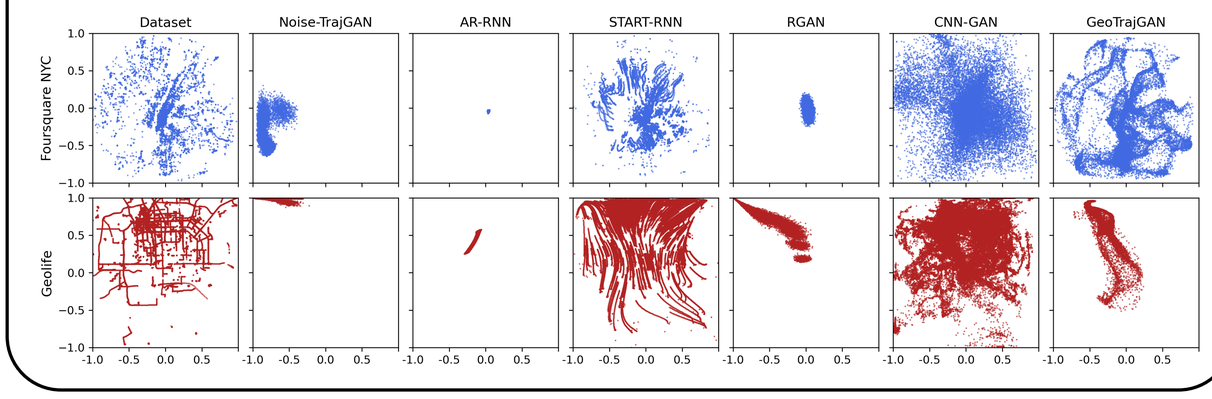
	Approach	UoP	G1	G2	G3	G4	G5	Main Shortcoming
1	LSTM-TrajGAN	Instance	✗	✓	✓ (TUL) / ✗ (RAoPT)	✓	✓	No guarantees
2	Shin2023	Instance	✗	✓	✓ (TUL)	✓	✓	No guarantees
3	Ozeki2023	Instance	✗	✓	○ (MIA)	✓	✓	No guarantees
4	Song2023	Instance	✗	✓	✓ (TUL)	✓	✓	No guarantees
5	Fontana2023	Instance	✗	✓	✓ (TUL)	✓	✓	No guarantees
6	LGAN-DP	Instance	✗	✓	–	○	✓	Flawed DP proof
7	DP-TrajGAN	Instance	✗	✓	–	○	✓	Flawed DP proof
8	Kim2022	Location		✗	–	○	✓	UoP; Grid-based
9	RNN-DP	Instance	✗	✓	–	✓	✓	Flawed DP proof
10	TSG	Instance	✗	✓	–	✓	✓	No guarantees
11	TS-TrajGEN	Instance	✗	✓	–	✓	✓	No guarantees
12	GeoPointGAN	Location		✗	–	✓	✓	Points only

GAN-based Architectures

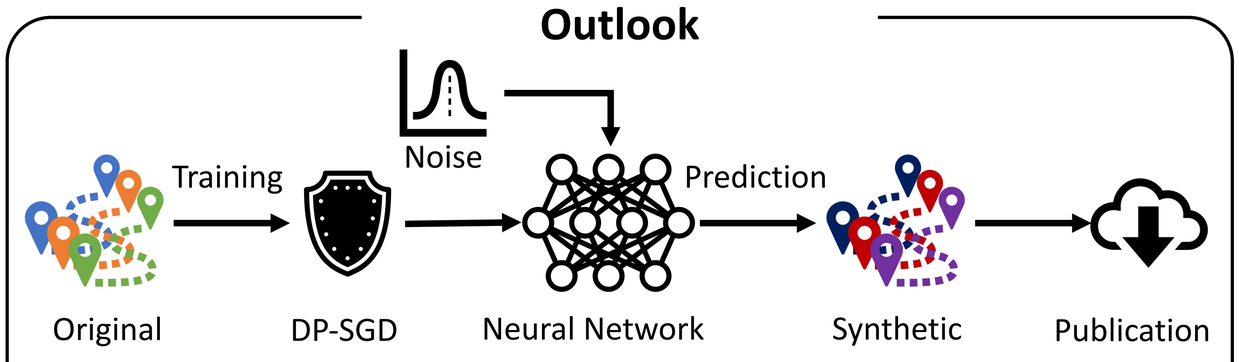
No input during prediction *"noise-only"* generation:



Did not observe sufficient utility on trajectory datasets:



Outlook



Goal: Generate Synthetic Trajectories with DP Guarantees

1. Develop a model without input during generation
2. Train the model with DP-SGD (to prevent memorization)
3. Explore DP-relaxations if required
4. Special-purpose solutions for certain applications

Conclusion: Further research on private trajectory generation required!

Acknowledgement

The authors would like to thank UNSW, the Commonwealth of Australia, and the Cybersecurity Cooperative Research Centre Limited for their support.