A Unified View of Frequency Estimation and their Attacks on Local Differential Privacy

Al Mehdi Saadat Chowdhury, Dhaval Pankaj Tanna, Deepak Vellanki, Chirag Manjeshwar
School of Computing and Augmented Intelligence
Arizona State University

Outline

Introduction:
- Differential Privacy
- Local Differential Privacy
- Frequency Estimation and Pure LDP
- Attack Problem

Frequency Estimation Techniques:
- K Randomized Response (kRR)
- Optimized Unary Encoding (OUE)
- Optimized Local Hashing (OLH)

Attacks:
- Attack Types
- Attacking kRR
- Attacking OUE
- Attacking OLH

Defenses:
- ?
- ?
- ?

Evaluation:
- Comparison between Estimators
- Gain from Attacks
- Impacts of Parameters on Attacks

Conclusion

Introductory Concepts

Differential Privacy

Local Differential Privacy

Frequency Estimation Problem

Pure Local Differential Privacy

Attack – Problem Formulation

Frequency Estimation Techniques

K Randomized Response

Optimized Unary Encoding

Optimized Local Hashing

Attacks on Frequency Estimators

Attack Types

Attacking kRR

Attacking OUE

Attacking OLH

Evaluation

Comparison between Estimators

Gain from Attacks

Impacts of Parameters on Attacks

Conclusion

Summary

Open Problems

Thank You