Obfuscating Web User Search Queries via Generative Adversarial Privacy

ang Zhang, Zhongxuan Ruan, Mengwei Yang

EE 599 Final Project

Jiang Zhang, Zhongxuan Ruan, Mengwei Yang

2020.4.xx

Content

- Introduction
- Related work
- Approach
- Evaluation
- Conclusion

Introduction

Related work

Approach: SeqGAN with multiple objectives

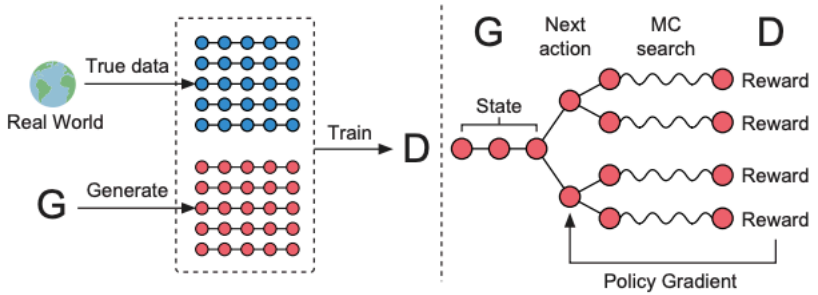

Figure 1: The illustration of SeqGAN. Left: D is trained over the real data and the generated data by G. Right: G is trained by policy gradient where the final reward signal is provided by D and is passed back to the intermediate action value via Monte Carlo search.

Fig. 1. Original SeqGAN (single objective).

* Discriminator: predict where a query is real, to make the obfuscated query meaningful.

* Adversary: predict the category of a query, to enhance the privacy of user query.

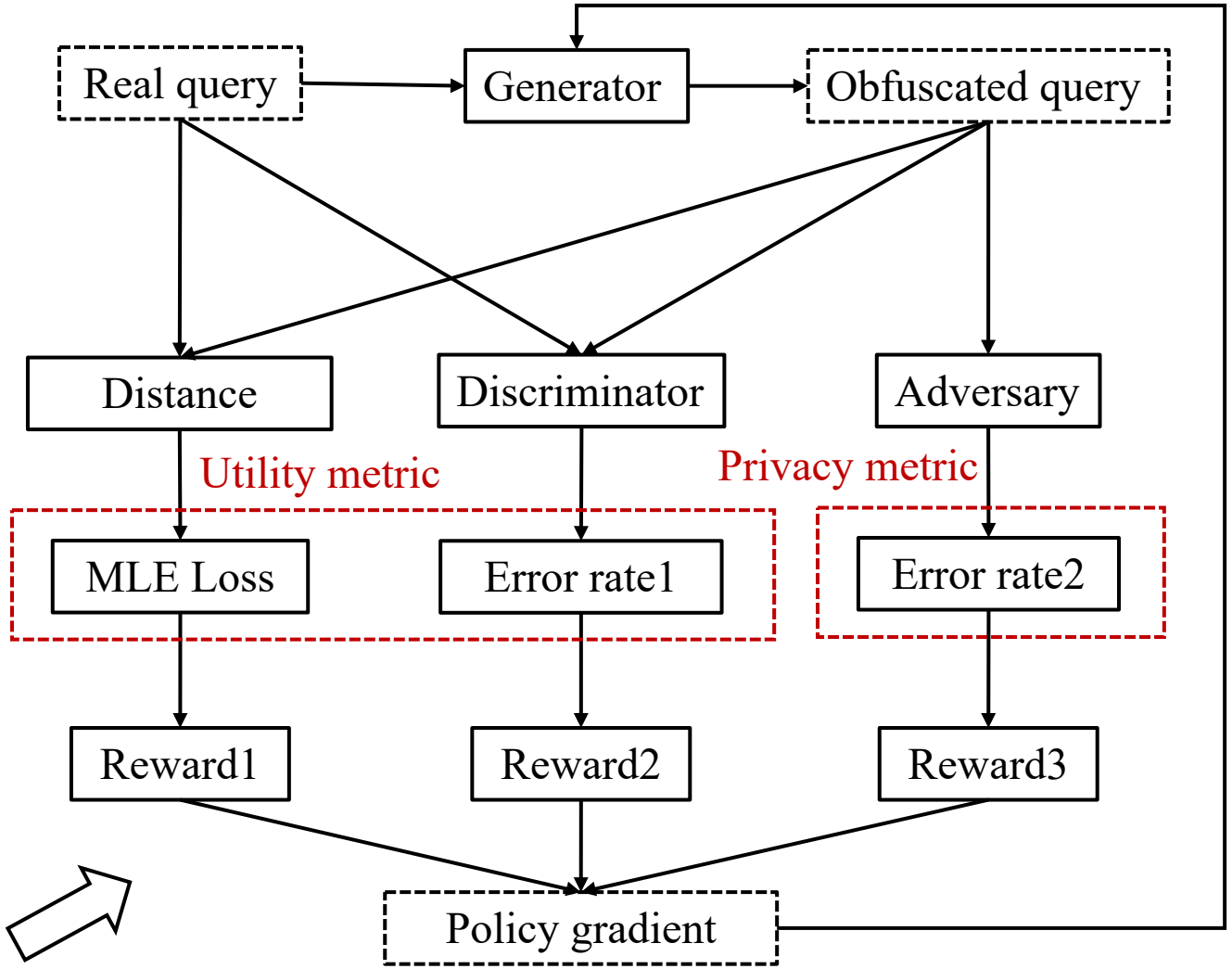

Fig. 2. Our SeqGAN with multiple objectives.

Evaluation

Conclusion