Privacy Preserving Bandits

Joint work with:
- Mohammad Malekzadeh (QMUL/Brave)
- Hamed Haddadi (ICL/Brave)
- Ben Livshits (ICL/Brave)

Dimitrios Athanasakis (Brave) • 02.03.2020
@dimmu
## Why this is an important topic

### Personalization is ubiquitous

- Many sites/apps offer personalized experiences
- Advertising (arguably the single biggest application of personalization) fuels the internet.

### Personalization is often invasive

- Tracking all over the internet
- Why is my being a fan of my little pony relevant to the pricing of my plane tickets?
- Some info gets REALLY personal
Real-time Ad bidding

No such thing as a free ad
How website advertisement auctions work

Sources: Brave; The Economist
Let’s learn everything locally

Great for privacy

- No data ever leaves the user’s device, therefore fewer things to worry from a privacy perspective.
- Eventually the local model will learn a very accurate model recommendation policy for the user.

Not so good for utility

- It may take a long time for the local model to learn a useful recommendation policy
- What happens when new personalization options appear
Online advertising and bandits

Learning

- What are the user’s interests?
- Should we display an ad for product X to user Y?
- Have the interests of the user changed?

Earning

- Given what we know about the user how can we maximise his engagement?
Problem Definition

Data tuple = \( (S = [S_0, S_1, ..., S_D], A \in \{1,2,...,K\}, R \in \{0,1\}) \)

Privacy first!
State? What state?

- “brave://histograms”

- Example:
  - Past 100 page visits? (%)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.25</td>
<td>0.15</td>
<td>0.05</td>
<td>0.20</td>
<td>0.35</td>
</tr>
</tbody>
</table>
How we can we enable an agent to know its user **faster** and **better**?
- Choose the best CBA
- **Warm start, instead of Cold!**
How can we use user data to initialize a warm model without violating a user’s privacy?
Can you recognize yourself by your own data?

Vanilla model inversion

VS

Model inversion on noised data
Can we quantify privacy?

**Differential Privacy:**

Definition 1: Differentially-Private Data Sharing. Given $\epsilon, \delta \geq 0$, we say a data sharing mechanism $\mathcal{M}$ satisfies $(\epsilon, \delta)$-differential privacy if for all pair of neighbor datasets of context vectors $X, X'$ differing in only one context vector $x$ and for all $R \subseteq \text{Range}(\mathcal{M})$,

$$Pr[\mathcal{M}(X) \in R] \leq e^\epsilon Pr[\mathcal{M}(X') \in R] + \delta$$

(Revised & Roth 2013)

**Crowd-blending**

Definition 2: Crowd-Blending Encoding. Given $l \geq 1$, we say an encoding mechanism $\mathcal{M}$ satisfies $(l, \bar{\epsilon} = 0)$-crowd-blending privacy if for every context vector $x$ and for every context dataset $X = X' \cup \{x\}$ we have

$$\left|\{y \in \mathcal{M}(X) : y = \mathcal{M}(\{x\})\}\right| \geq l \quad \text{or} \quad \mathcal{M}(X) = \mathcal{M}(X')$$

(Gehrke et al 2011)
Our approach: ESA + LinUCB
State Space

- **Histograms**
  - D-dimensional vector of real numbers
  - Its sum is 1
  - It’s rounded to F decimal points
- e.g. if we set D=10:
  - with F=1 we have ~100K possible states
  - with F=2 it is ~4T

\[
\left(10^F + D - 1\right) \choose {D - 1}
\]

Number of possible states is too large
Encoding

- e.g. $D=3$, $F=1$
- 66 possible states
- 6 cluster
  - Locality-sensitive hashing
- 3bits

This helps increasing the size of the crowd a user can blend in.

E.g. $D=10 \rightarrow 10$ bits : $4T \rightarrow 1K$
Shuffling

- **Anonymization**: Remove Meta-data (e.g. ip address) received from local agents.
- **Shuffling**: gather tuples received from different sources into batches and shuffle their order.
- **Thresholding**: remove tuples whose encoded context vector frequency in the batch is less than a defined threshold.
- Yes, that means throwing away potentially useful data for the sake of privacy.
- This happens in an sgx secure enclave.
Model updates

- **Updates** are performed using standard LinUCB update rules on the data the shuffler releases.
- Agents can then upload their local models according to the globally updated weights.
Privacy Model

- Crowd-Blending + Sampling $\Rightarrow$ Differential Privacy
  - iid random sampling with probability $p$

$$\varepsilon_{DP} = \ln \left( p \cdot \left( \frac{2 - p}{1 - p} \varepsilon_{CB} \right) + (1 - p) \right)$$
Evaluation

**Algorithm**
- Linear UCB

**Context**
- Histograms

**Environment**

- **Synthetic Datasets**
  - Linear and nonlinear randomly initialized mapping functions
    - Input: a histogram
    - Output: a stochastic preference model

- **Real Multi-Label Datasets**
  - Input: a binary vector (features)
  - Output: a binary vector (labels)

- **Criteo Ad Recommendation Dataset**
  - Input: Integer values (unknown features)
  - Output: a one-hot vector (product category)

Github:
https://github.com/mmalekzadeh/privacy-preserving-bandits
Results: Synthetic Data

- Left: effect of available actions on expected reward for varying numbers of users
- Bottom: effect of the dimensionality of the context on expected reward
Results: Multi-Label Classification

- MediaMill: $d=20$, $|A|=40$, $\sim 44000$ instances
- TextMining: $d=20$, $|A|=20$, $\sim 28,500$ instances
Results: Ad. Recommendation (Criteo)

- $k = 32$
- $k = 128$

$|A| = 40$, $d = 10$, $u = 3,000$ agents
Some Remarks

- The Criteo ad recommendation experiments are somewhat strange but surely interesting
- ESA is making a comeback (ESA Revisited)
- Also SMPC for bandits
- Feel free to play around with the notebooks. Also stickers, again

Personal Notes

- Mohammad will be looking for a job soon.
- Pleasantly surprised to see some remote presentations.

Github:
https://github.com/mmalekzadeh/privacy-preserving-bandits
Let’s keep in touch

1. Poster #15

2. Working on privacy? Let’s talk. Have experiences in the adtech ecosystem? We’d like to hear from you.

3. We’re always looking for great engineers:
   https://brave.com/careers/

Also @dimmu