Applying mix de-anonymisation techniques for good

Steven Murdoch
University College London

Wi-Fi data collection

We collect Wi-Fi connection data at this station to better understand journey patterns and improve your services.

We will not identify individuals.

You can opt out by turning off your device's Wi-Fi.

TfL monitor wifi MAC addresses to track mobility

Steven Murdoch @sjmurdoch · Jul 15

My issues are that the poster implies there's an opt-out when it isn't really and also there would be privacy-preserving ways to achieve the same goal

1 1

Kate Bevan 🙄🙄

@katebevan

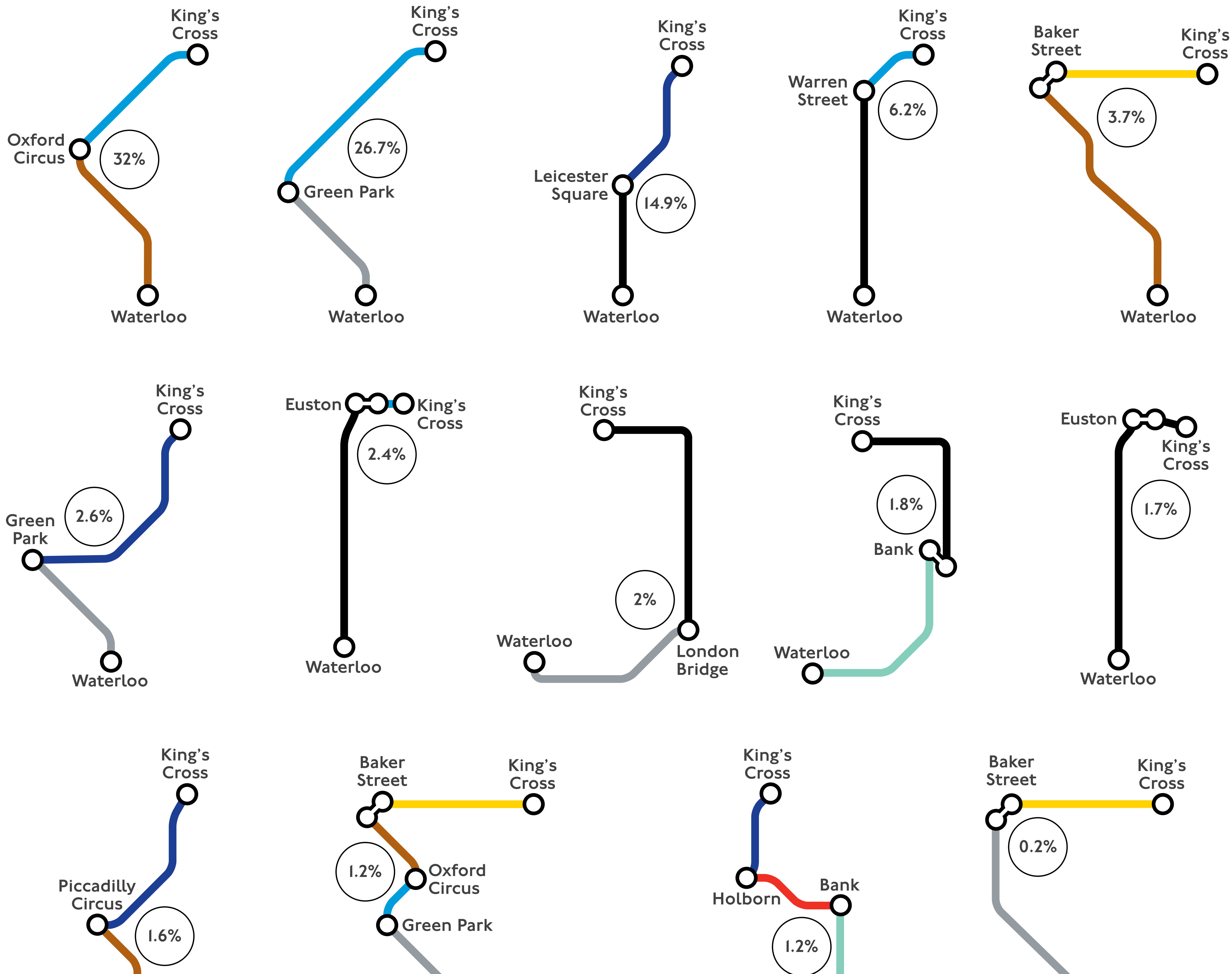
Follow

Replying to @sjmurdoch @futureidentity and 5 others

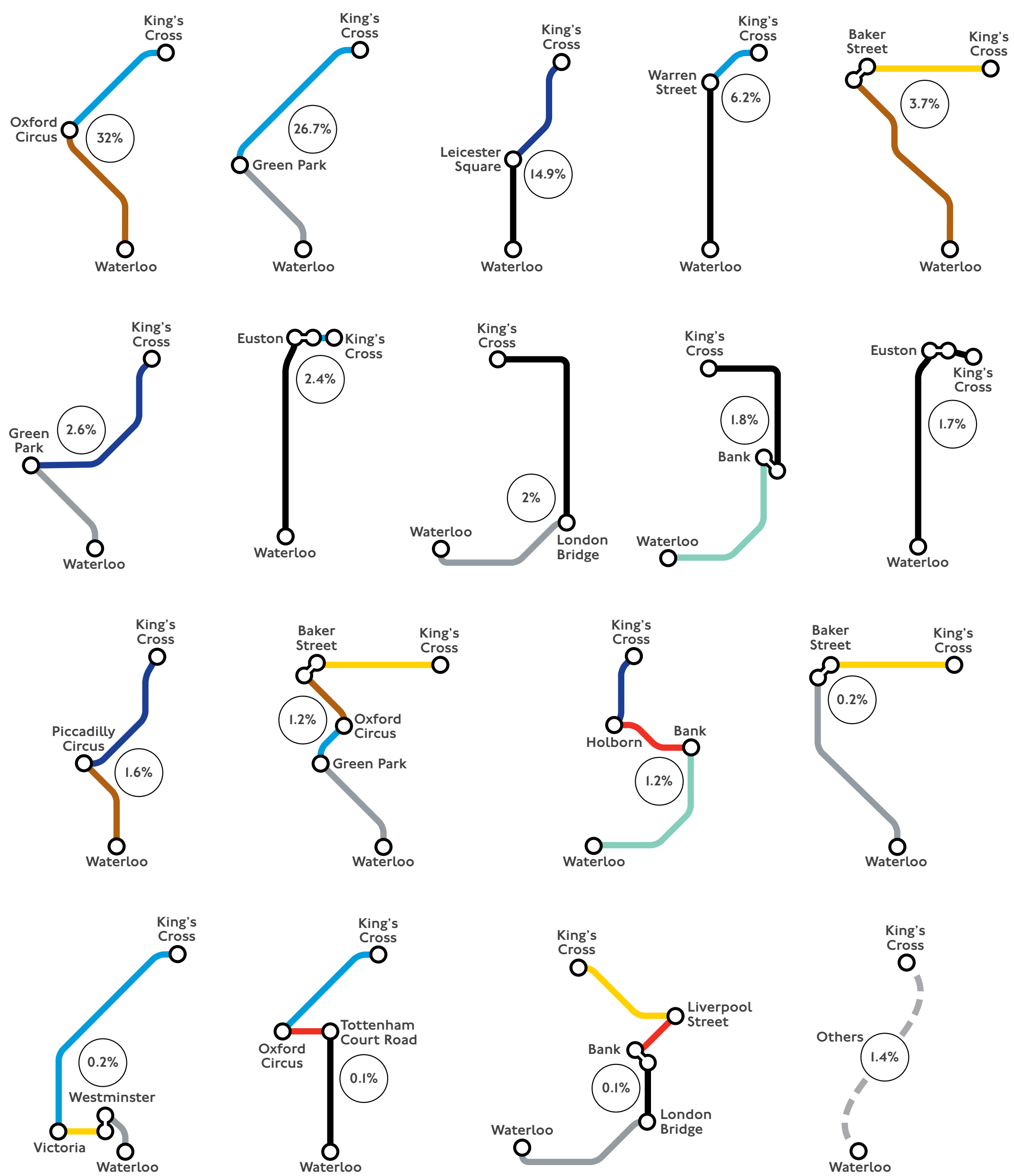
You can turn off your WiFi, though as Michael points out, it's less quick if you've got a laptop in your bag. But seriously, this is a good project. It's less perfectly implemented than some might like, but it's data for good. Not all data collection is terrible.

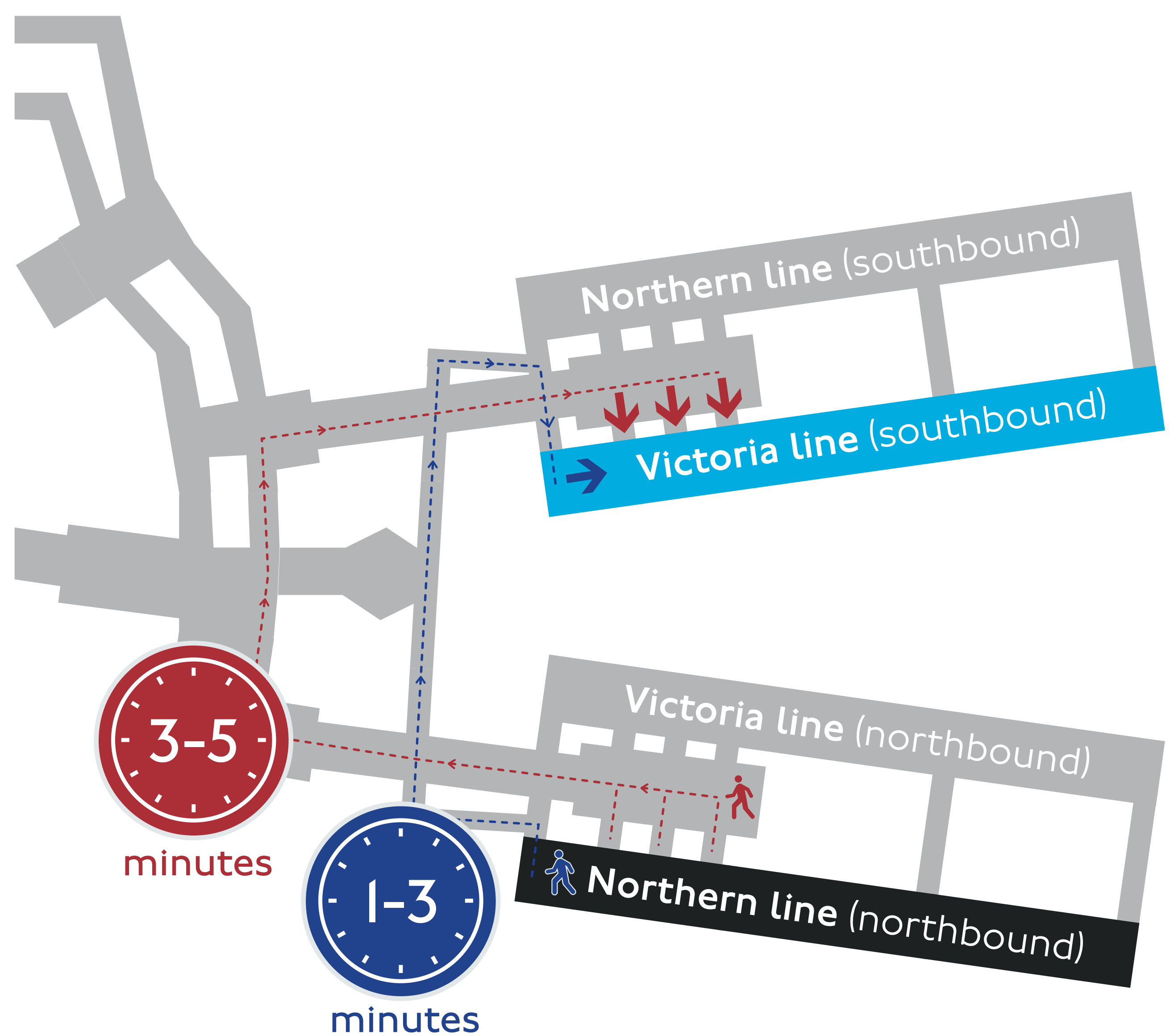
9:02 AM - 15 Jul 2019

4

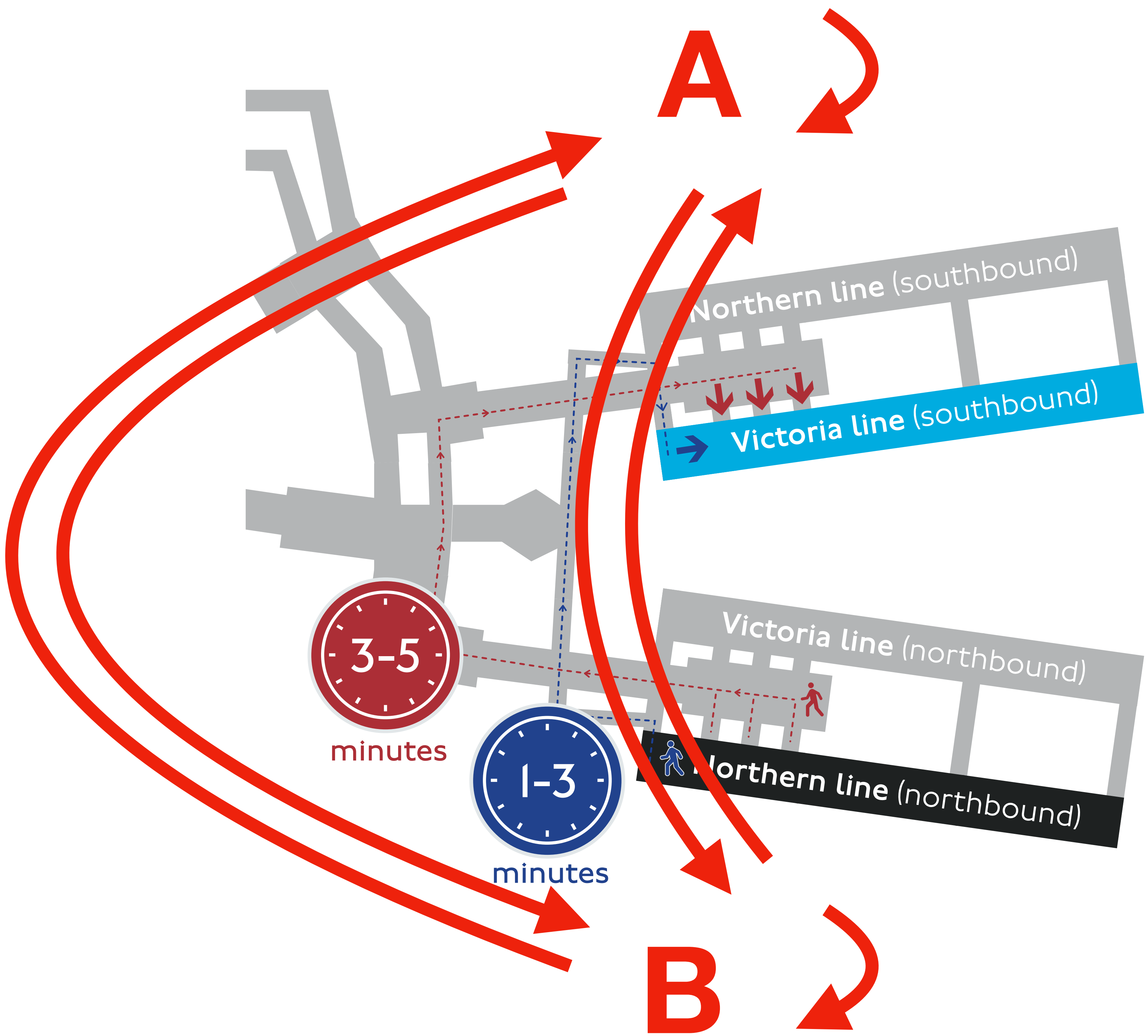

King's Cross
Oxford Circus
32%
Waterloo
King's Cross
26.7%
Green Park
Waterloo
King's Cross
Leicester Square
14.9%
Waterloo
King's Cross
Warren Street
6.2%
Waterloo
Baker Street
King's Cross
3.7%
Waterloo
King's Cross
Green Park
2.6%
Waterloo
Euston
King's Cross
2.4%
Waterloo
King's Cross
2%
Waterloo
London Bridge
King's Cross
1.8%
Bank
Waterloo
Euston
King's Cross
1.7%
Waterloo
King's Cross
Piccadilly Circus
1.6%
Baker Street
King's Cross
1.2%
Oxford Circus
Green Park
King's Cross
Holborn
Bank
1.2%
Baker Street
King's Cross
0.2%

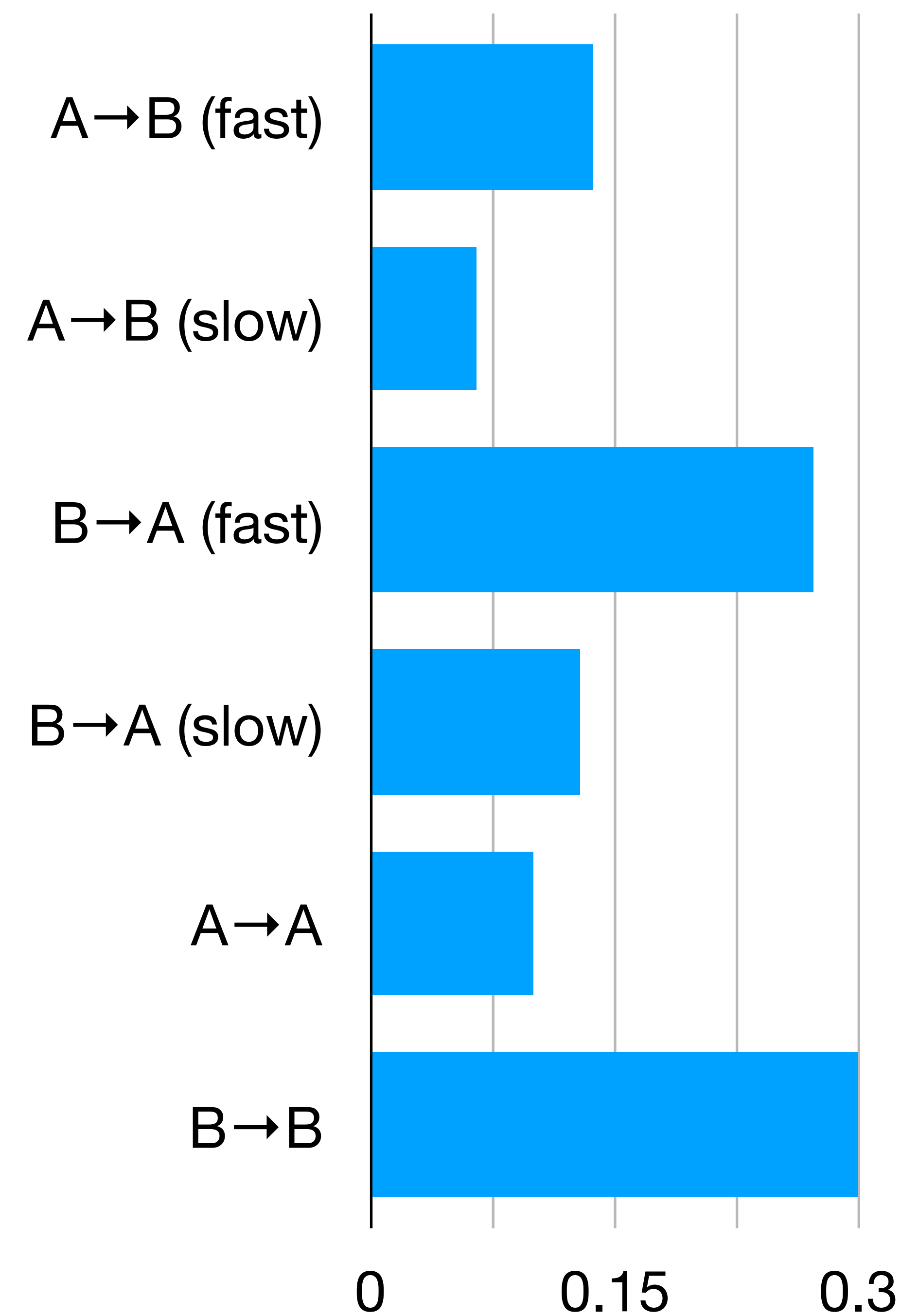
Ticketing data doesn't explain movements in stations





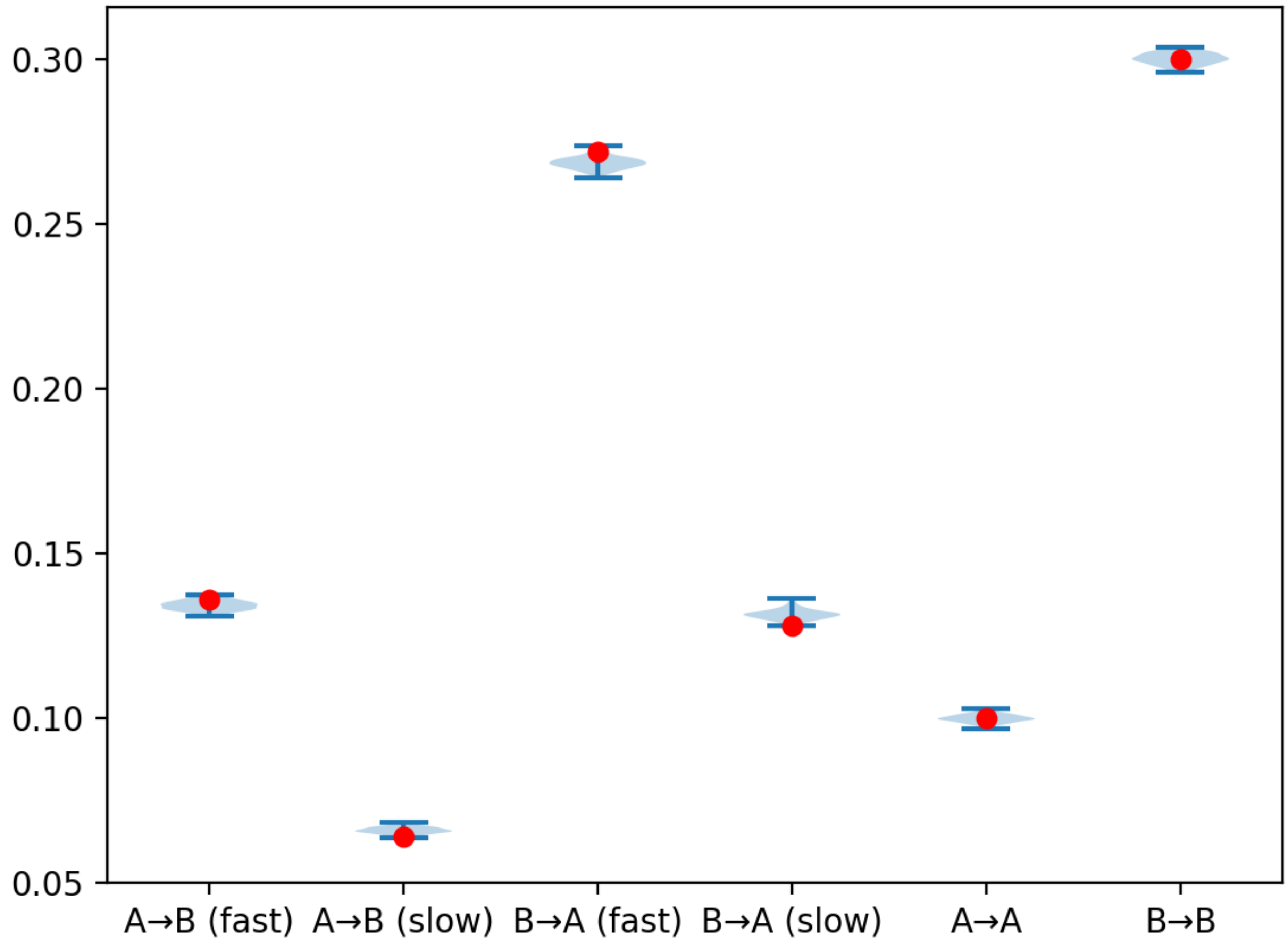
We can simulate wifi observations in a station based on user profiles





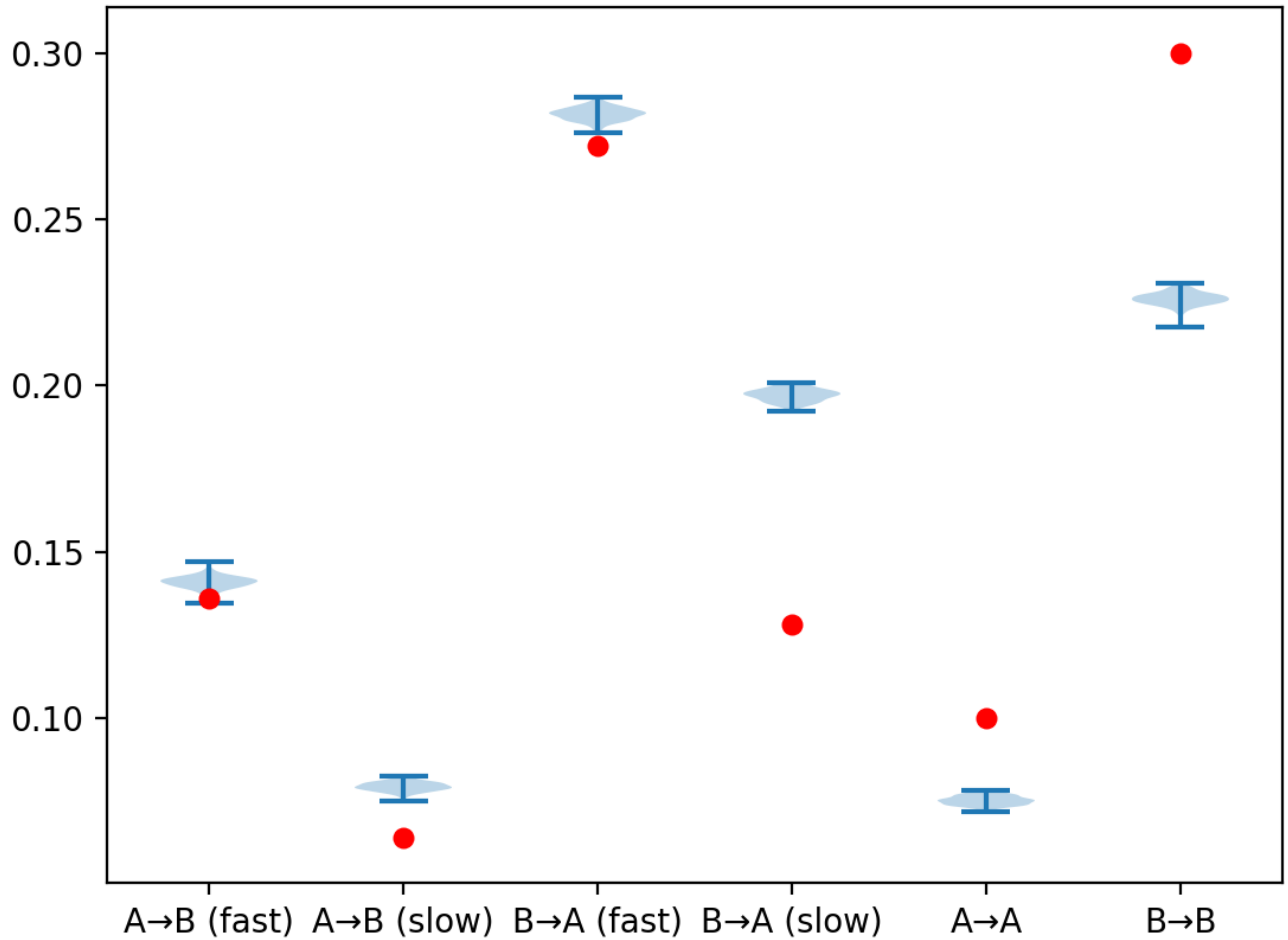
Analysis of 64 bit MAC addresses gives good results

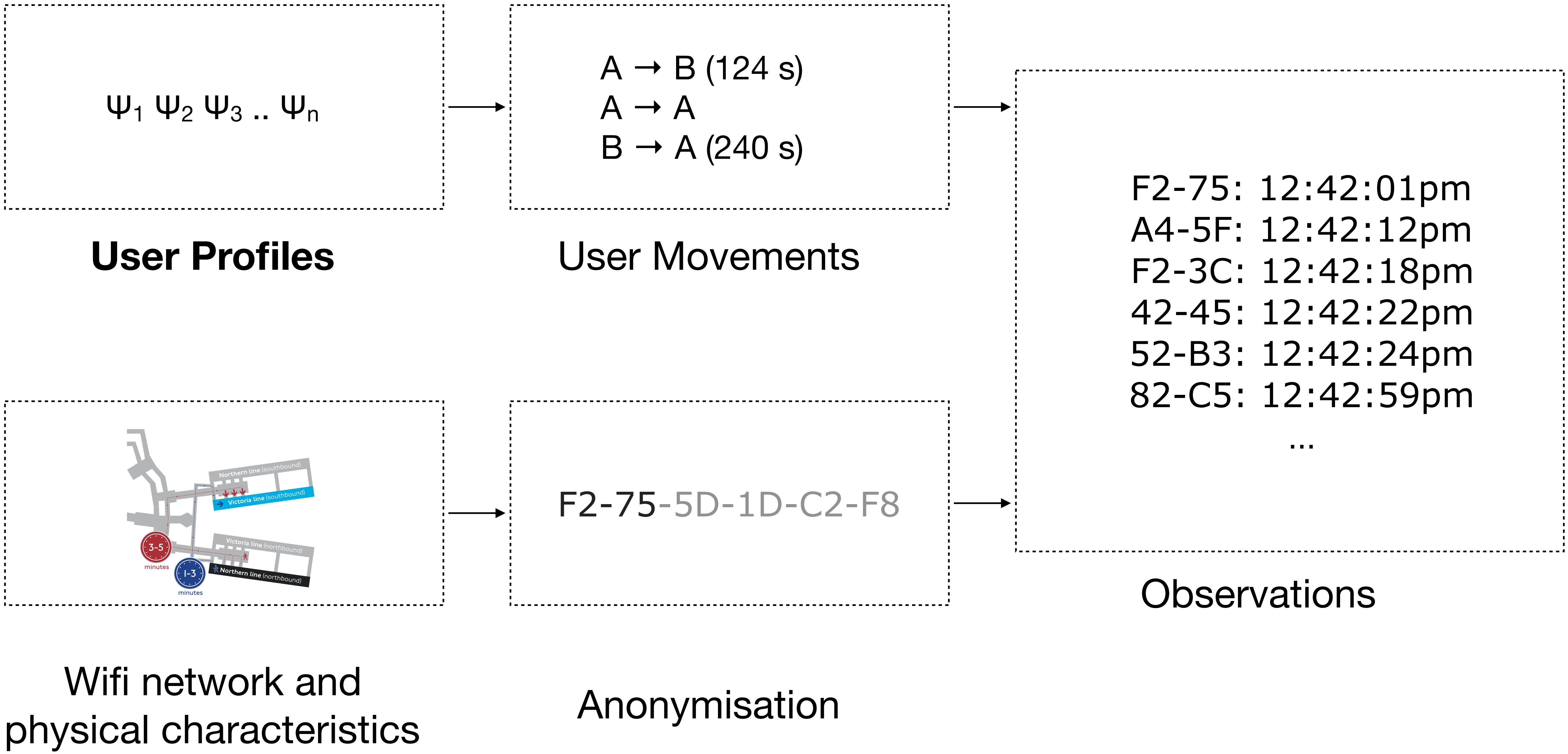
- Poisson arrival
  - λ = 1 per s
- Normal distribution for walking speed
  - σ = 30 s
- 100 simulations
  - Each 1 day



Truncated 16 bit MACs don't work as well

- Poisson arrival
  - λ = 1 per s
- Normal distribution for walking speed
  - σ = 30 s
- 100 simulations
  - Each 1 day




Ψ_1 Ψ_2 Ψ_3 .. Ψ_n
User Profiles
A → B (124 s)
A → A
B → A (240 s)
User Movements
F2-75: 12:42:01pm
A4-5F: 12:42:12pm
F2-3C: 12:42:18pm
42-45: 12:42:22pm
52-B3: 12:42:24pm
82-C5: 12:42:59pm
...
Observations
Northern line (southbound)
Victoria line (southbound)
Victoria line (northbound)
Northern line (northbound)
3-5
minutes
1-3
minutes
Wifi network and
physical characteristics
F2-75-5D-1D-C2-F8
Anonymisation

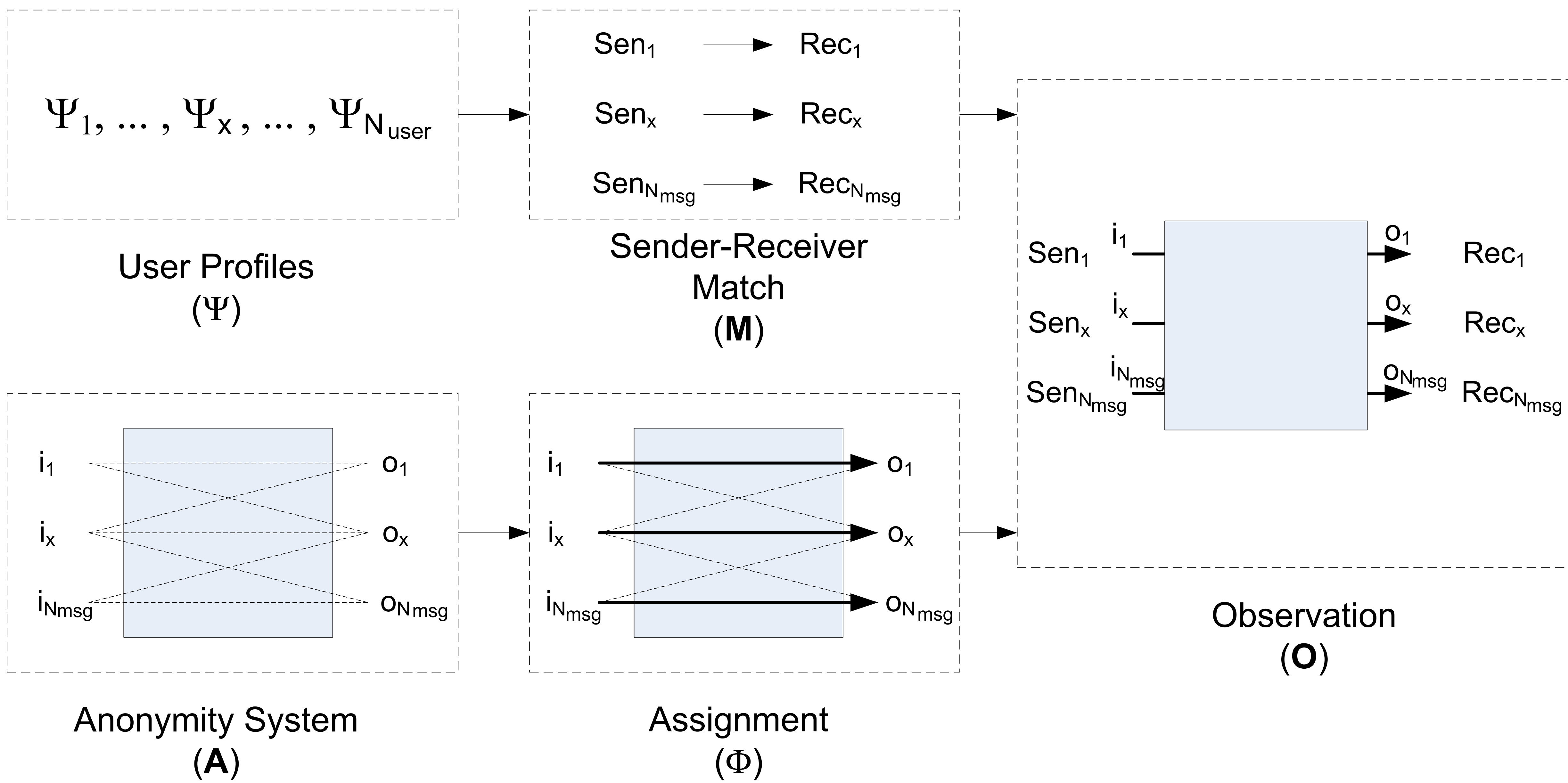


Fig. 1. The generative model used for Bayesian inference in anonymous communications.

We start by proposing a 'forward' generative model describing how messages are generated and sent through the anonymity system. We then use Bayes rule

- **De-anonymisation techniques can improve user privacy!**
- It is possible to **infer customer mobility profiles from observations of anonymised MAC addresses**
- Model wifi network and MAC address anonymization as a mix network
- Take into account reasonable prior beliefs of mobility patterns

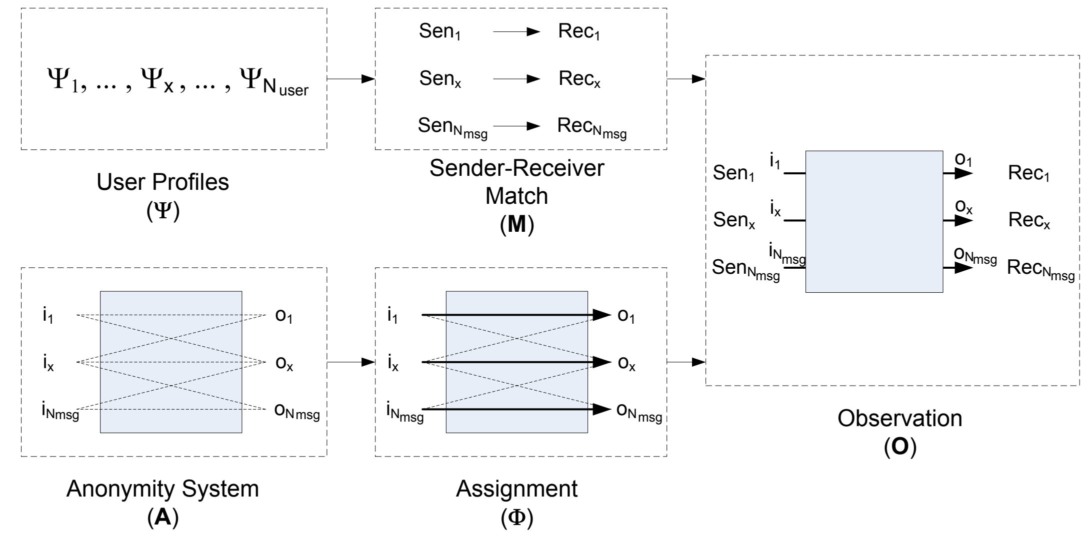


Fig. 1. The generative model used for Bayesian inference in anonymous communications.

We start by proposing a 'forward' generative model describing how messages are generated and sent through the anonymity system. We then use Bayes rule to 'invert' the problem and perform inference on the unknown quantities. The broad outline of the generative model is depicted in Figure 1.

An anonymity system is abstracted as containing N_{user} users that send N_{msg} messages to each other. Each user is associated with a sending profile Ψ_x describing how they select their correspondents when sending a message. We assume, in this work, that those profiles are simple multinomial distributions, that are sampled independently when a message is to be sent to determine the receiver. We denote the collection of all sending profiles by $\Psi = \{\Psi_x | x = 1 \ldots N_{\text{user}}\}$.

A given sequence of N_{msg} senders out of the N_{user} users of the system, denoted by $\text{Sen}_1, \ldots, \text{Sen}_{N_{\text{msg}}}$, send a message while we observe the system. Using their sending profiles a corresponding sequence of receivers $\text{Rec}_1, \ldots, \text{Rec}_{N_{\text{msg}}}$ is selected to receive their messages. The probability of any receiver sequence is easy to compute. We denote this matching between senders and receivers as $\mathcal{M}$:

$$\Pr[\mathcal{M}|\Psi] = \prod_{x \in [1, N_{\text{msg}}]} \Pr[\text{Sen}_x \rightarrow \text{Rec}_x | \Psi_x].$$

In parallel with the matching process where users choose their communication partners, an anonymity system $\mathcal{A}$ is used. This anonymity system is abstracted as a bipartite graph linking input messages i_x with potential output messages o_y, regardless of the identity of their senders and receivers. We note that completeness of the bipartite graph is not required by the model. The edges of the bipartite graph are weighted with w_{xy} that is simply the probability of the input message i_x being output as o_y: $w_{xy} = \Pr[i_x \rightarrow o_y | \mathcal{A}]$.

This anonymity system $\mathcal{A}$ is used to determine a particular assignment of messages according to the weights w_{xy}. A single perfect matching on the bipartite

UCL InfoSec are hiring!

Post-docs, PhD students, …

New UK cybersecurity centre for doctoral training (CDT) – **55+ PhD studentships** over the next 8 years between Computer Science, Crime Science and Public Policy

www.benthamsgaze.org