

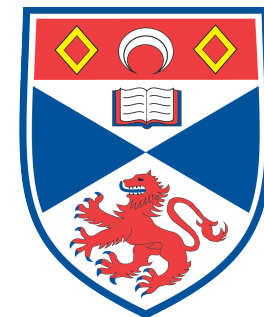
# The impact of location privacy on opportunistic networks

Iain Parris and Tristan Henderson

{isp3,tnhh}@st-andrews.ac.uk

<http://www.cs.st-andrews.ac.uk/~ip/>

<http://www.cs.st-andrews.ac.uk/~tristan/>



University  
of  
St Andrews

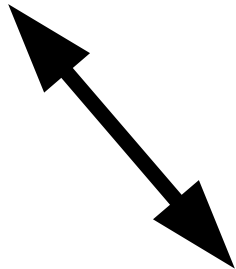
# Opportunistic networks



Can **directly exchange data** between the mobile devices that people already carry, when in proximity (e.g., **Bluetooth**).

If many such people cooperate, can form a **disconnected, store-carry-and-forward opportunistic network**.

“Hello, I am eating a pizza.”



Intersection of research problems:

- **Routing**
- **Privacy**

# Location privacy



## PLEASE ROB ME

### Raising awareness about over-sharing

Check out our [guest blog post](#) on the CDT website.

**Next step**

 We are satisfied with the attention we've gotten for an issue that we deeply care about. If you're interested, you might like to read these articles:

- [On Locational Privacy, and How to Avoid Losing it Forever](#)
- [Over-sharing and Location Awareness](#)

Currently we're looking through the emails we've received regarding the future of the website. As soon as we've thought of a suitable way to continue, you'll find it right here.

We're not showing the Twitter messages anymore, as they no longer add anything. If you don't want your information to show up everywhere, don't over-share ;-)

**More Info**

[Home](#)  
[Why](#)

**Made Possible By**

[Foursquare](#)  
[Twitter](#)  
[@boyvanamstel](#)  
[@frankgroeneveld](#)  
[@barryborsboom](#)

<http://pleaserobme.com/>

# Location privacy

Assumption: at times people may **switch off** their devices' opportunistic networking features:

- To become **invisible to the network.**
- And thus preserve their privacy.



# Location privacy & performance

How might we measure the impact on opportunistic network **performance** if people disable their devices in order to preserve their privacy?

Our approach:

- **User study** to collect **privacy preferences**.
- Extract general **privacy model**.
- Run **simulations** using privacy model, to model opportunistic network performance.

# Collecting privacy preferences



Location-sensing mobile phones.

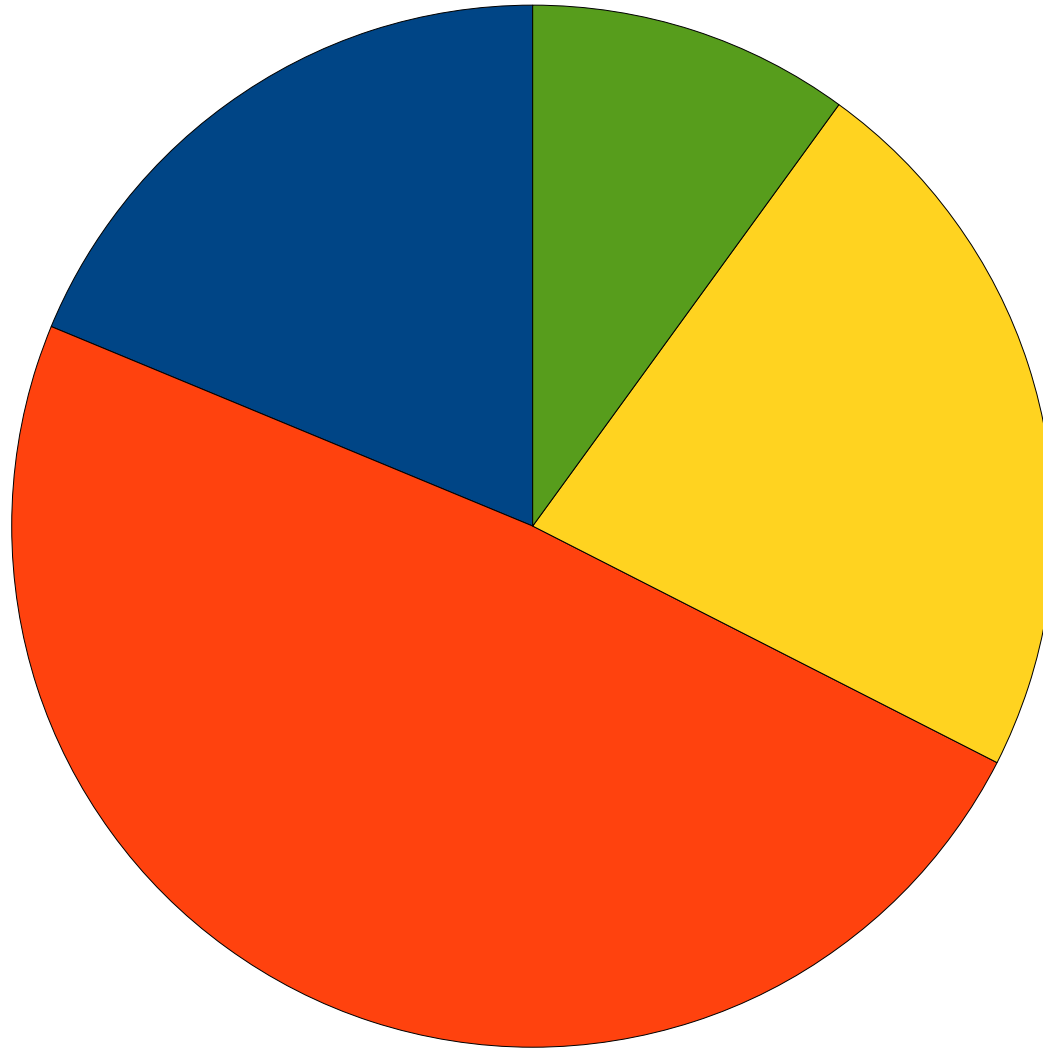
Phone asks about sharing current location.

- Experience sampling method (ESM).

80 students:

- Four runs of 20 students.
- St Andrews (2), London (2).

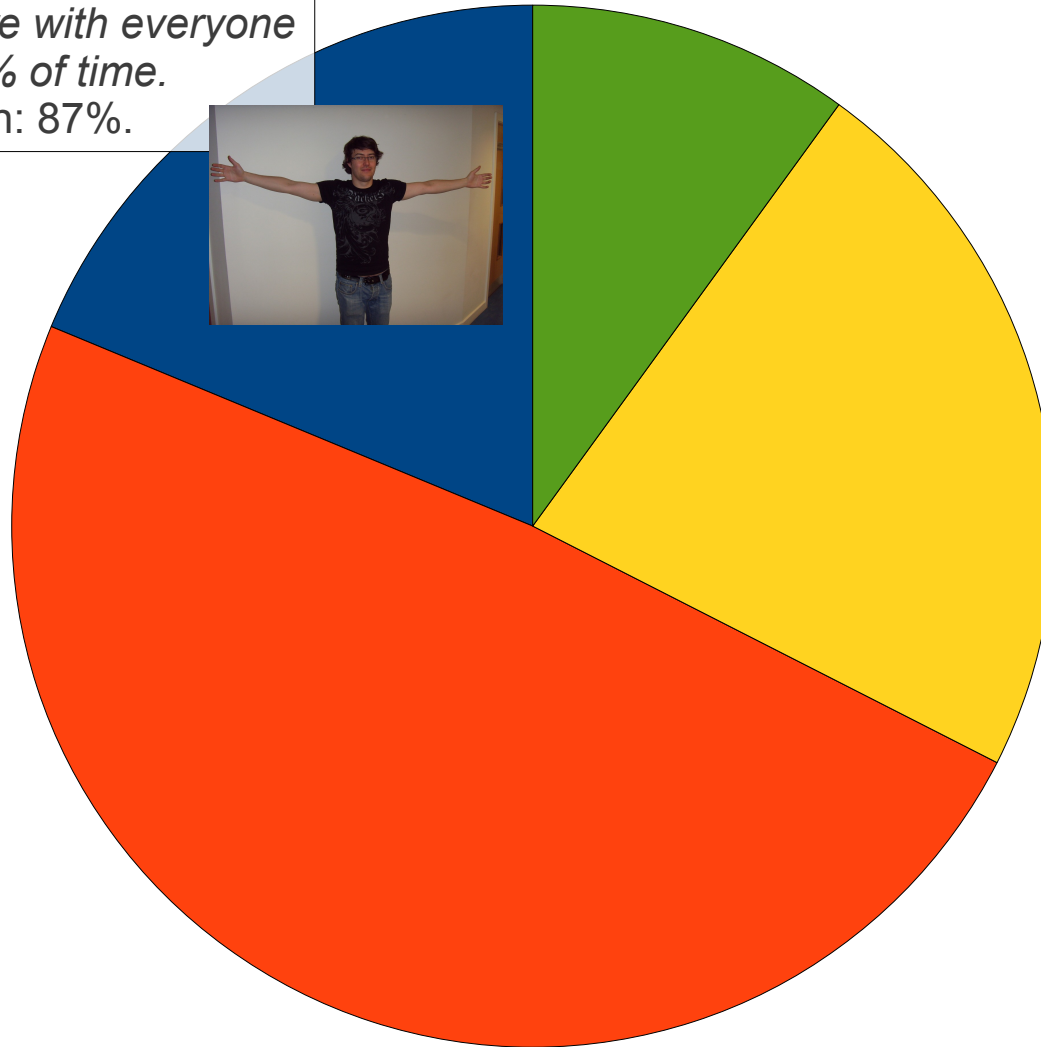
# Location privacy model



# Location privacy model

## Open

*Share with everyone*  
*>50% of time.*  
Mean: 87%.



# Location privacy model

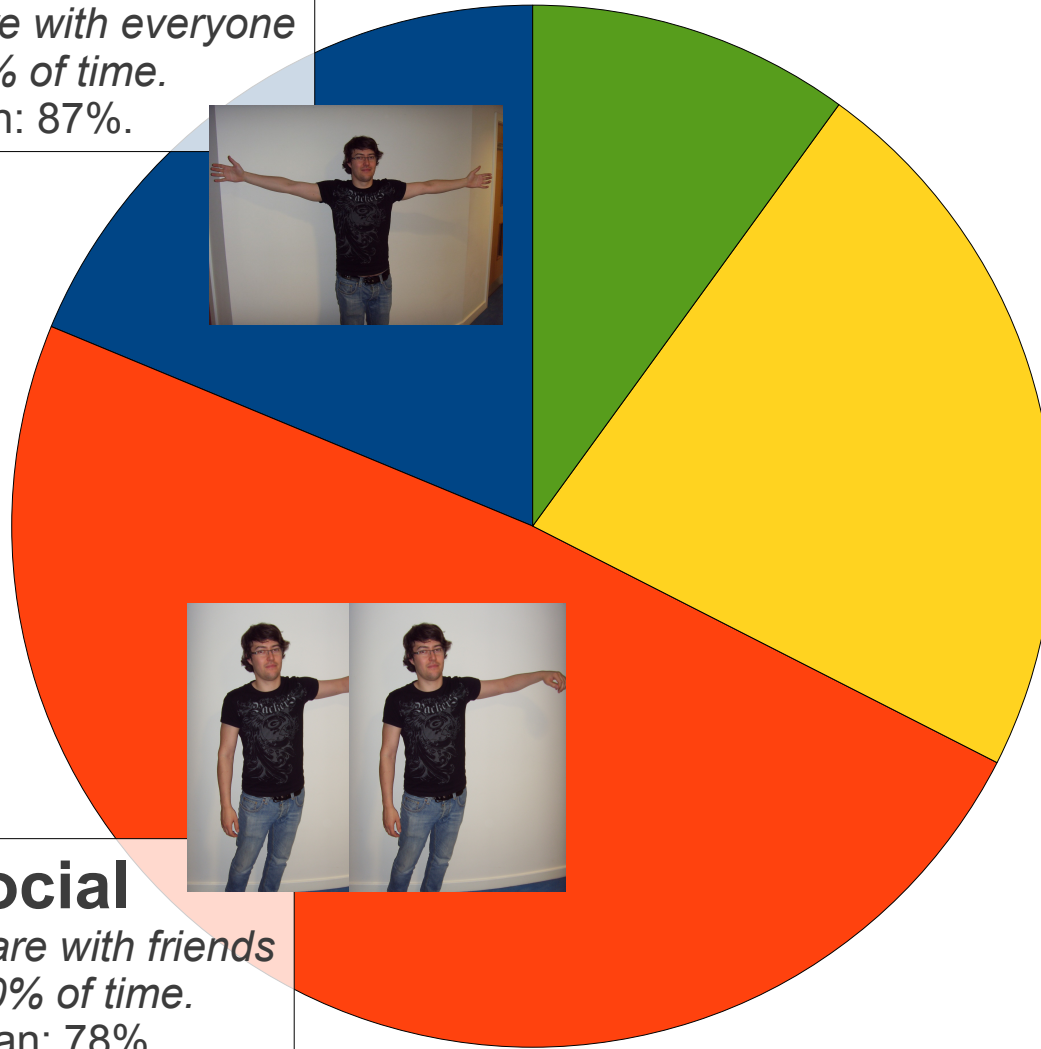
## Open

*Share with everyone*  
*>50% of time.*  
Mean: 87%.



## Social

*Share with friends*  
*>50% of time.*  
Mean: 78%.



# Location privacy model

## Open

*Share with everyone*  
>50% of time.  
Mean: 87%.



## Closed

*Share with nobody*  
>50% of time.  
Mean: 70%.

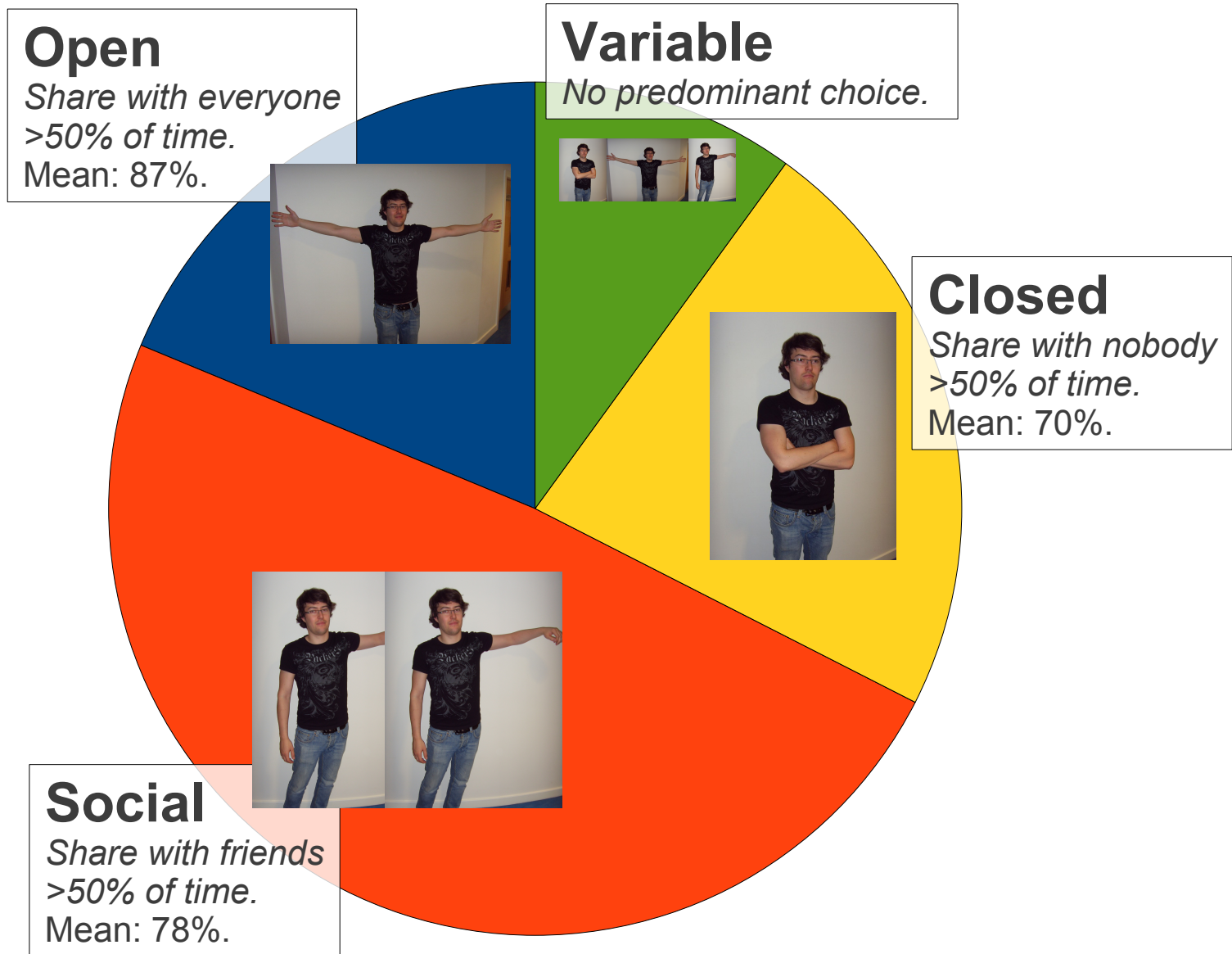


## Social

*Share with friends*  
>50% of time.  
Mean: 78%.



# Location privacy model



# Routing

## Epidemic routing (*Epid*)

- Flood all links with messages.
- Will find shortest path.
- But drains batteries.



## Simple social network routing (*SSNR*)

- From previous work.
- Social network information informs routing decisions.
- No global knowledge needed.
- At each hop, forward message to any person who is in the sender's social network.

# Using the privacy model

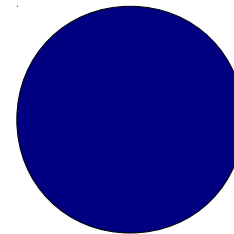
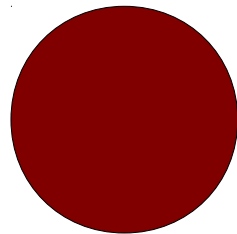
## Privacy modes

- **Default (*D*)**: Ignore privacy preferences: ground truth.
- **Friendly (*F*)**: Public, private or friends.
- **PubPriv (*PP*)**: All-or-nothing: public or private.

# Using the privacy model

## Privacy modes

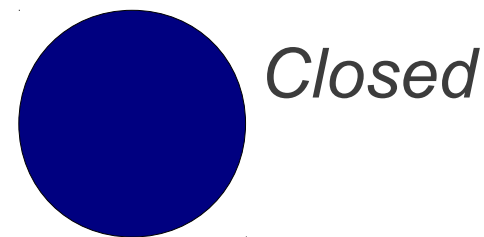
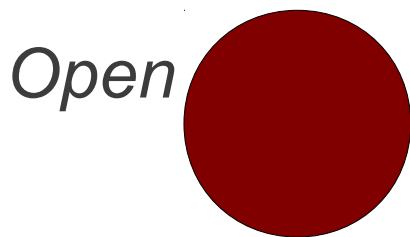
- **Default (*D*)**: Ignore privacy preferences: ground truth.
- **Friendly (*F*)**: Public, private or friends.
- **PubPriv (*PP*)**: All-or-nothing: public or private.



# Using the privacy model

## Privacy modes

- **Default (*D*)**: Ignore privacy preferences: ground truth.
- **Friendly (*F*)**: Public, private or friends.
- **PubPriv (*PP*)**: All-or-nothing: public or private.



# Using the privacy model

## Privacy modes

- **Default (*D*)**: Ignore privacy preferences: ground truth.
- **Friendly (*F*)**: Public, private or friends.
- **PubPriv (*PP*)**: All-or-nothing: public or private.



# Using the privacy model

## Privacy modes

- **Default (*D*)**: Ignore privacy preferences: ground truth.
- **Friendly (*F*)**: Public, private or friends.
- **PubPriv (*PP*)**: All-or-nothing: public or private.



# Performance evaluation

## Trace-driven simulation, two datasets:

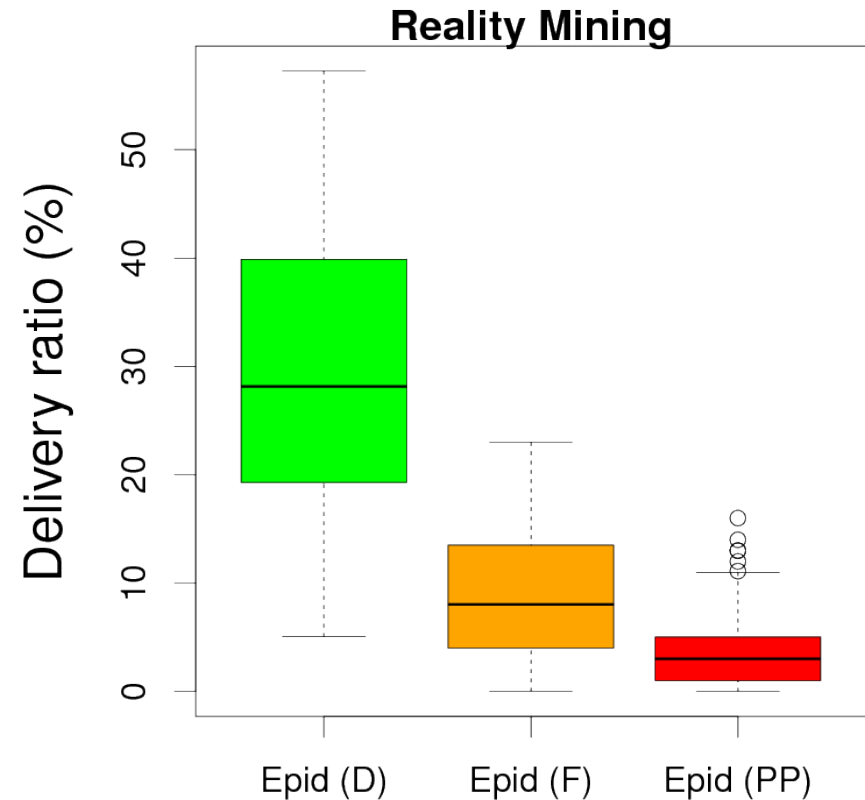
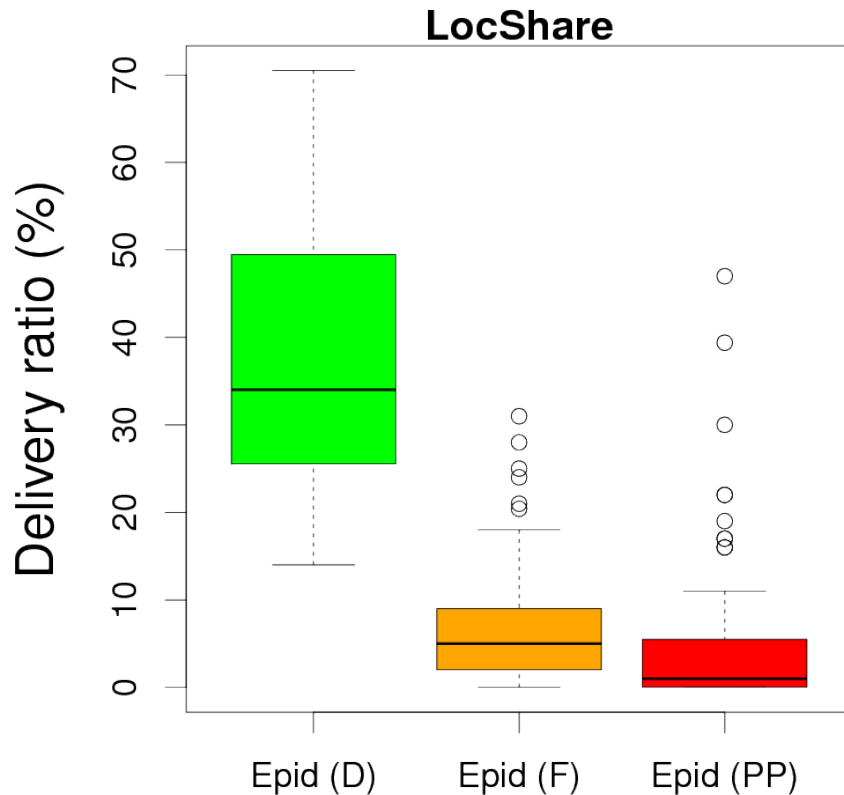
- **LocShare** – Collected in **St Andrews & London, UK**
  - Encounters: Proximity, within 10m.
  - Social network information: Facebook.
  - 80 participants.
- **Reality Mining** – Well-known dataset from **MIT, USA**
  - Encounters: Bluetooth.
  - Social network information: Address books.
  - 52 participants (not all ~100 had social network info).

# Performance evaluation

## Simulation parameters

- **100 runs** per data point.
- **100 messages** per run.
- Unicast messages, from sender to a friend.
- TTL of messages: **1 day**.
- **One week** per simulation.
- Infinite buffers.

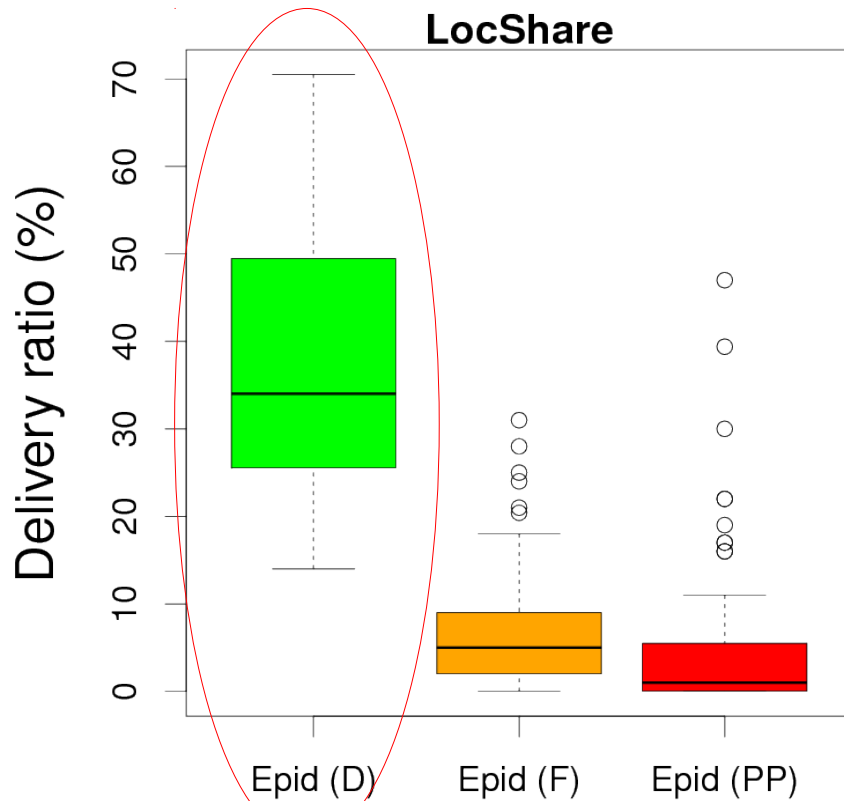
# Results – Delivery Ratio (Epid)



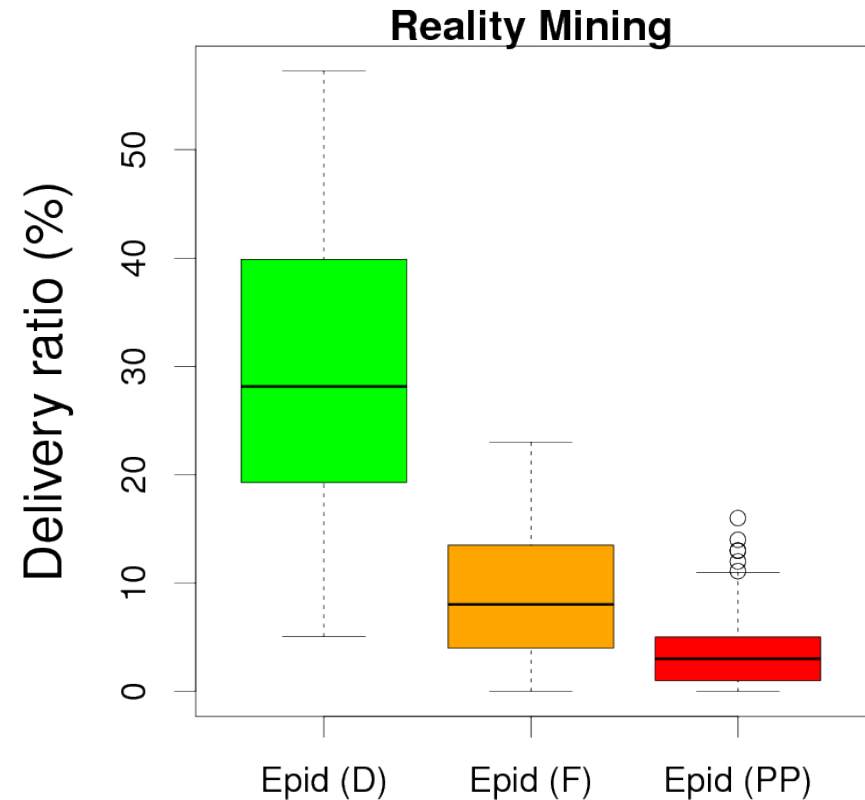
**Delivery ratio:**

$$\frac{\text{Number of messages that arrive at destination}}{\text{Number of messages sent}}$$

# Results – Delivery Ratio (Epid)



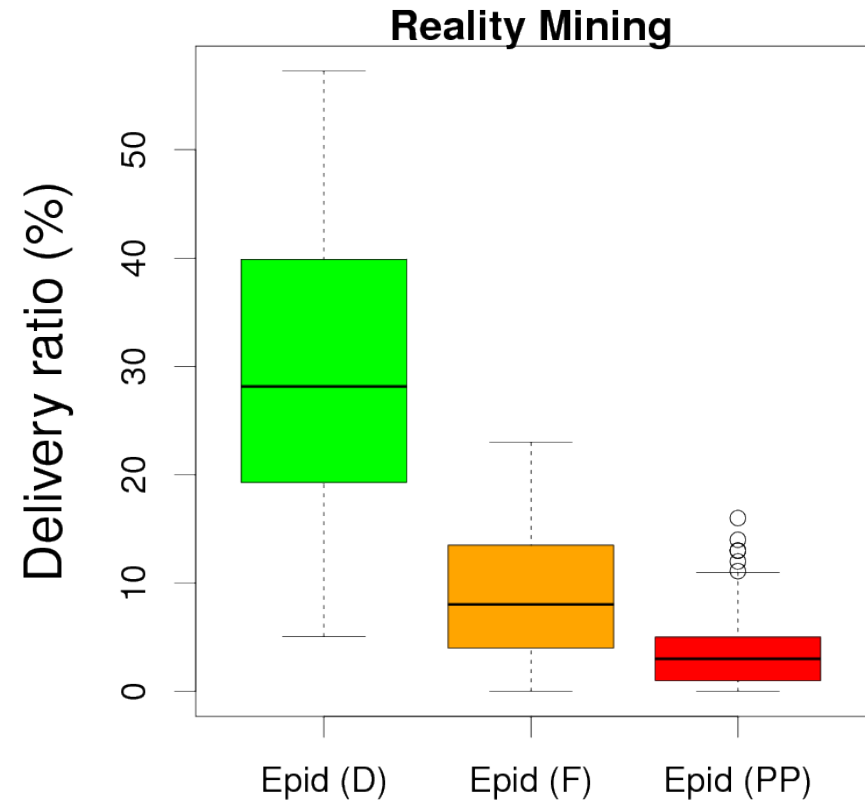
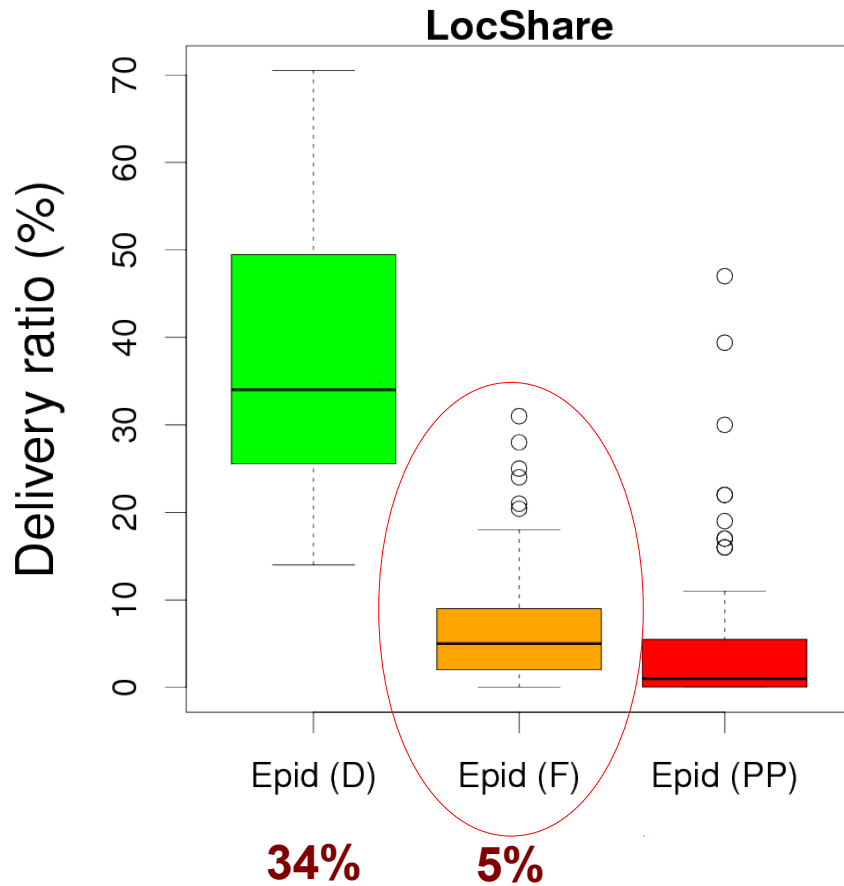
**34%**



**Delivery ratio:**

$$\frac{\text{Number of messages that arrive at destination}}{\text{Number of messages sent}}$$

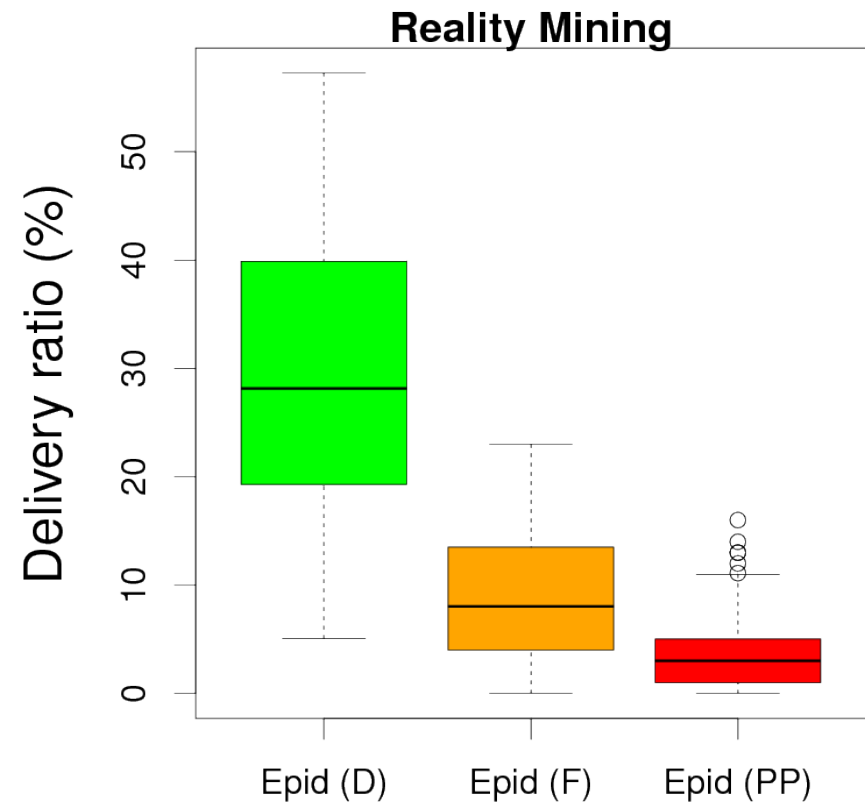
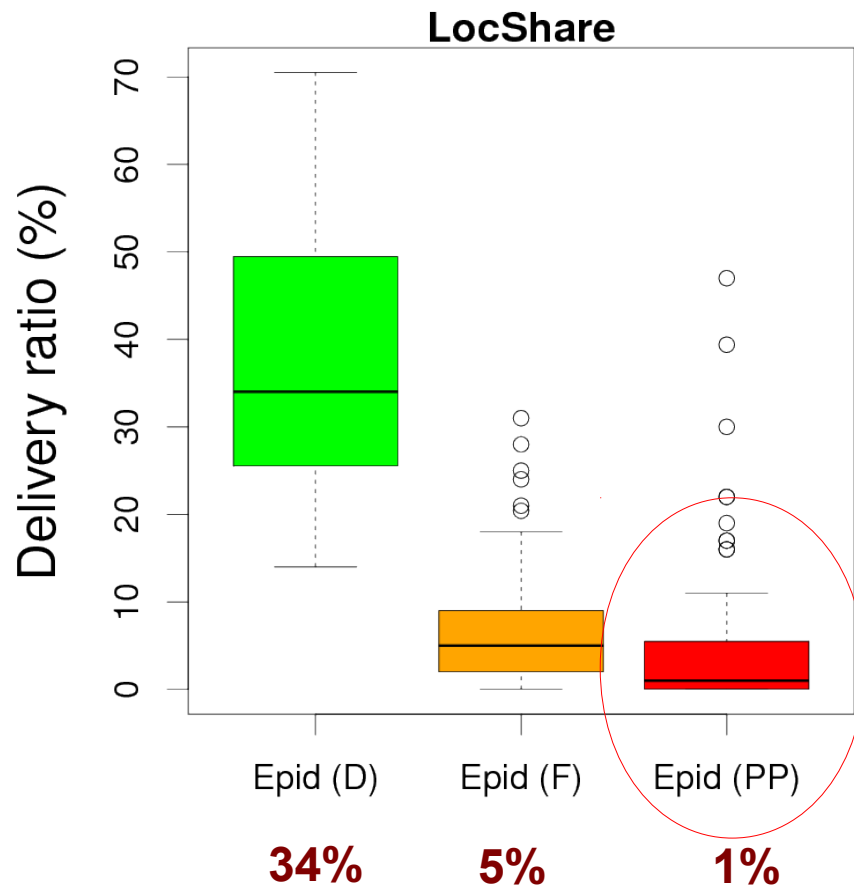
# Results – Delivery Ratio (Epid)



**Delivery ratio:**

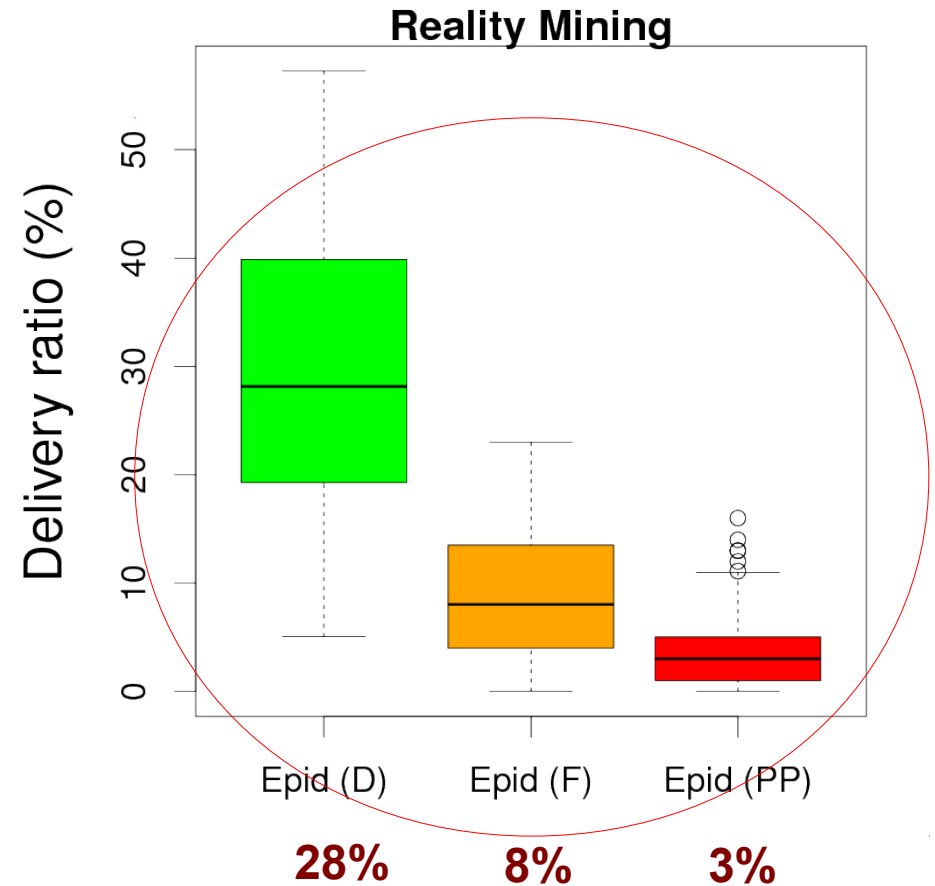
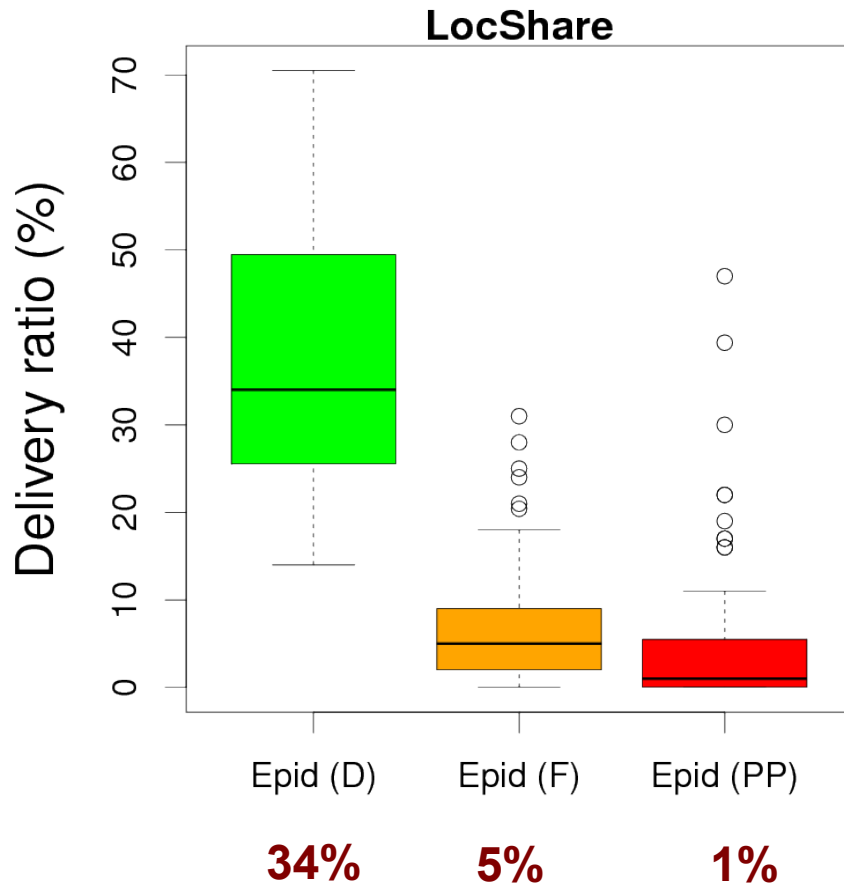
$$\frac{\text{Number of messages that arrive at destination}}{\text{Number of messages sent}}$$

# Results – Delivery Ratio (Epid)



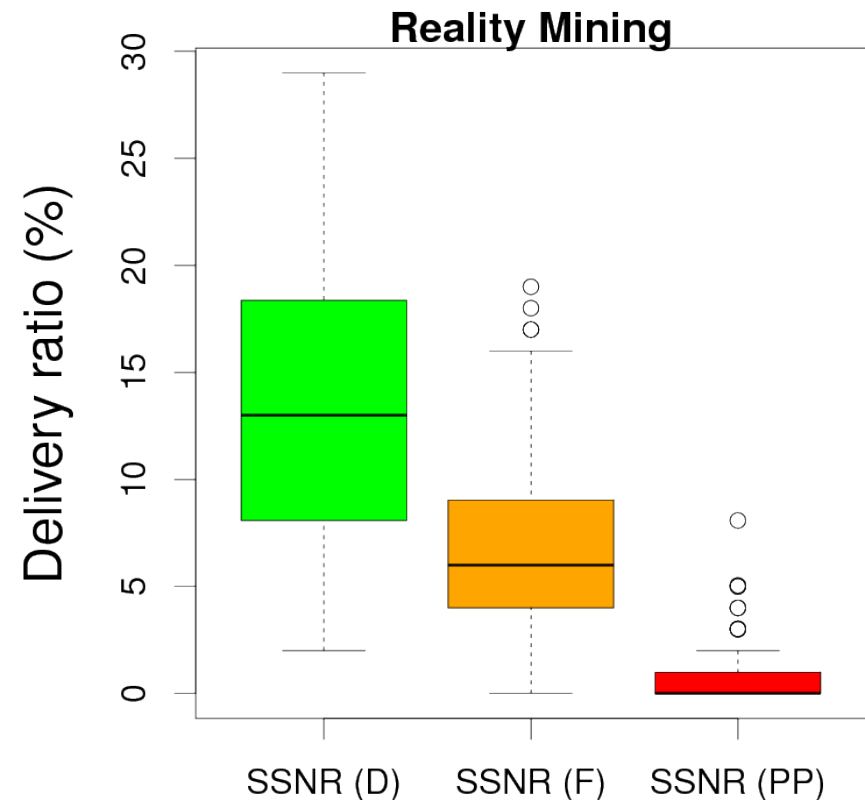
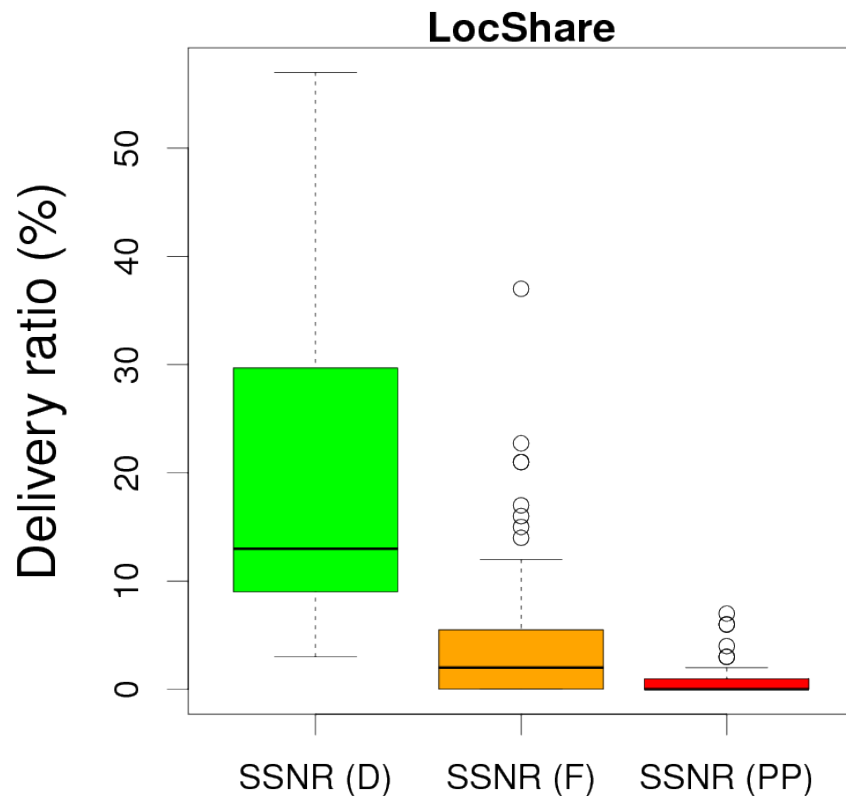
**Delivery ratio:**  
$$\frac{\text{Number of messages that arrive at destination}}{\text{Number of messages sent}}$$

# Results – Delivery Ratio (Epid)



**Delivery ratio:**  
$$\frac{\text{Number of messages that arrive at destination}}{\text{Number of messages sent}}$$

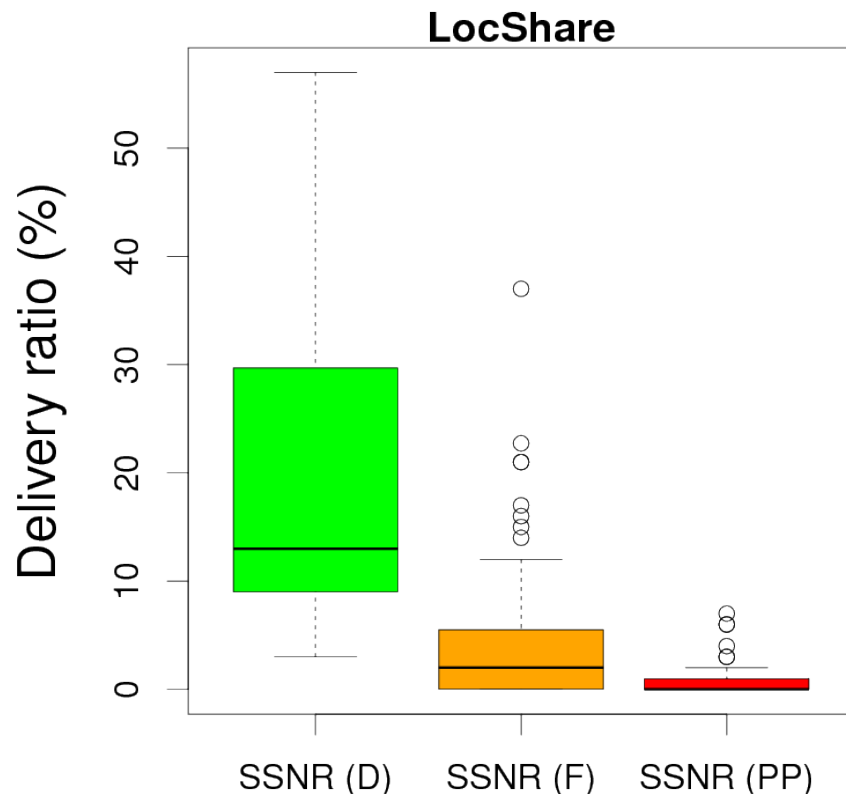
# Results – Delivery Ratio (SSNR)



## Delivery ratio:

$$\frac{\text{Number of messages that arrive at destination}}{\text{Number of messages sent}}$$

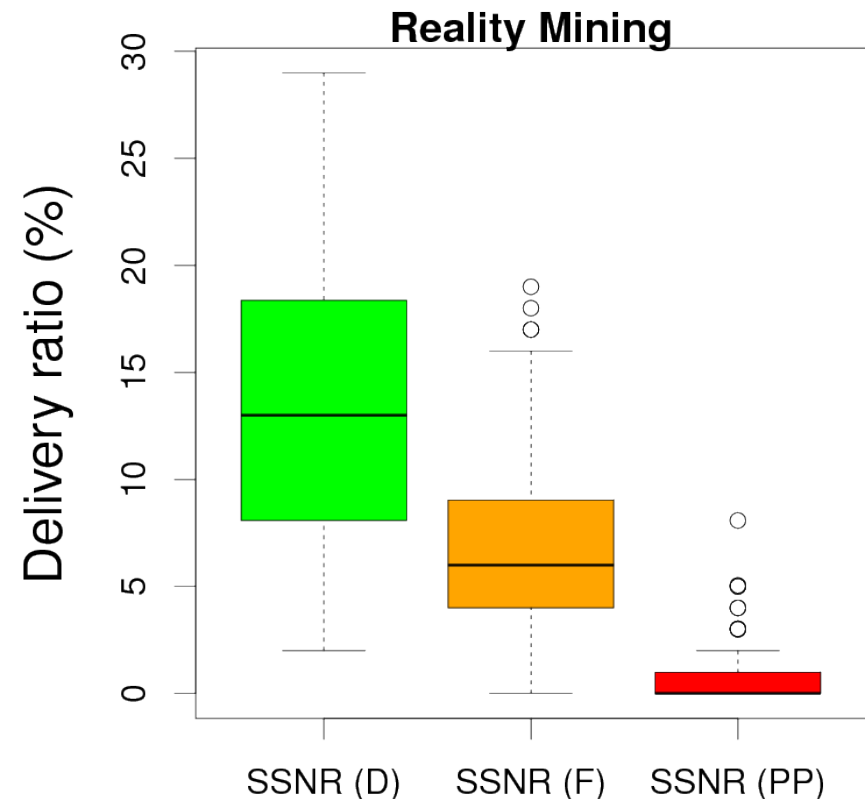
# Results – Delivery Ratio (SSNR)



**13%**

**2%**

**0%**



**13%**

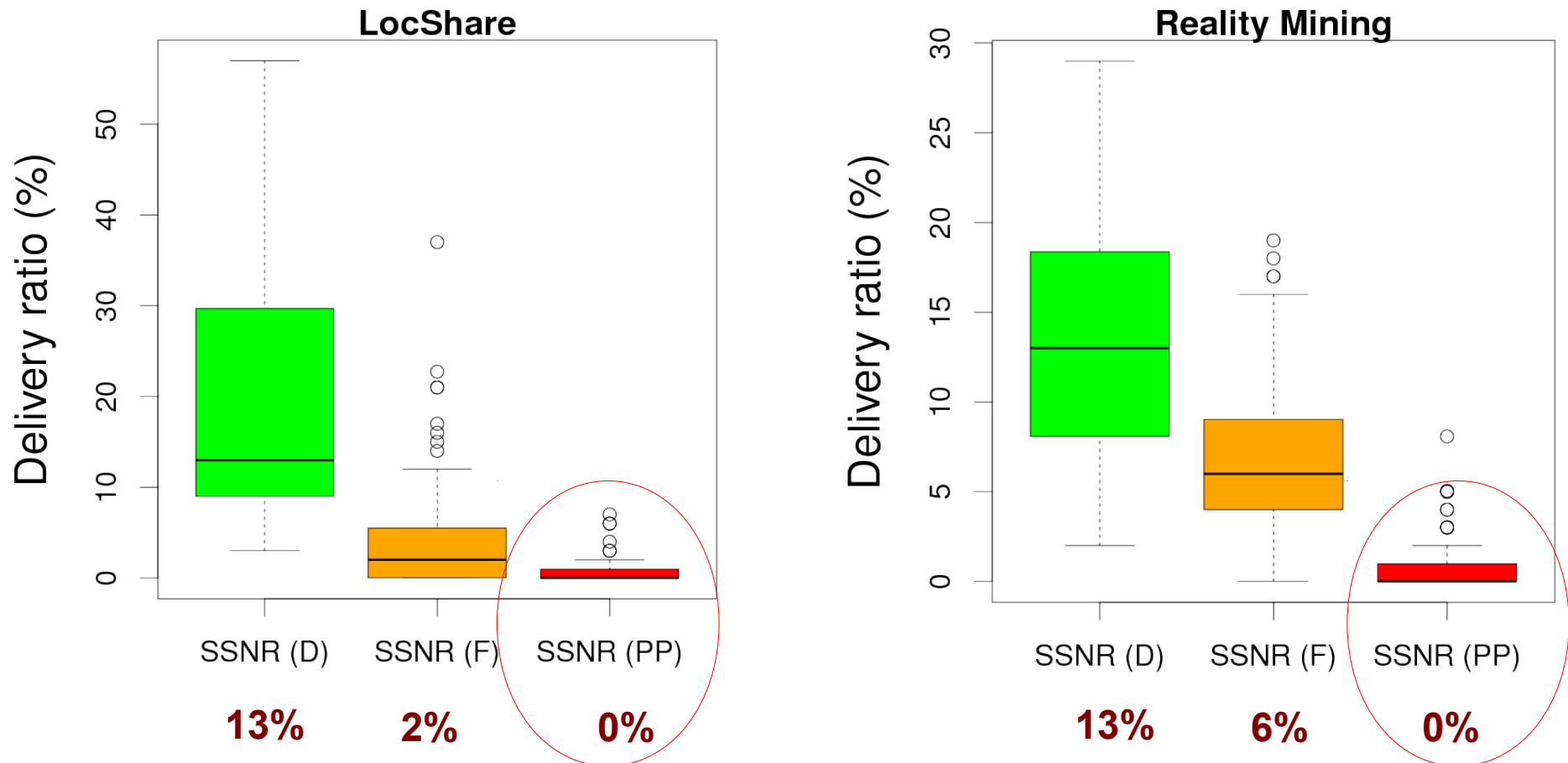
**6%**

**0%**

**Delivery ratio:**

$$\frac{\text{Number of messages that arrive at destination}}{\text{Number of messages sent}}$$

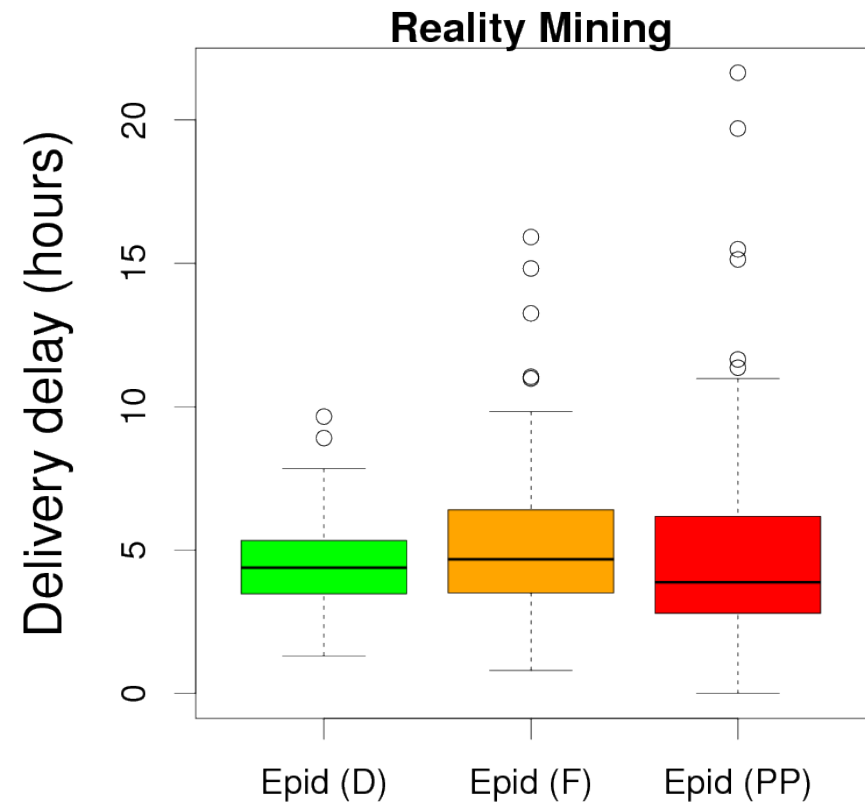
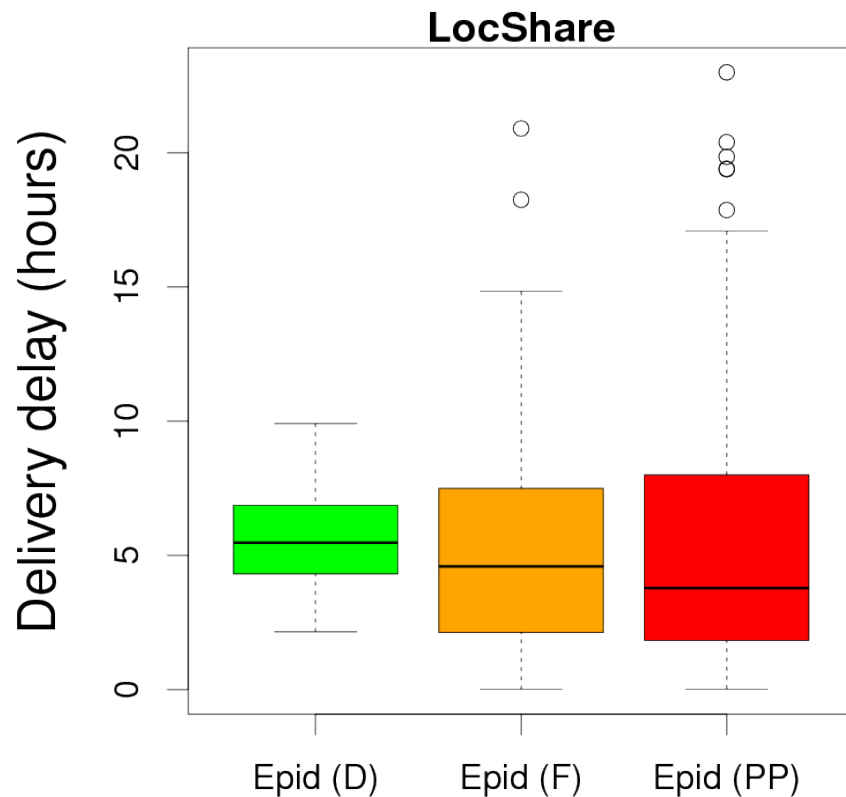
# Results – Delivery Ratio (SSNR)



**Delivery ratio:**

$$\frac{\text{Number of messages that arrive at destination}}{\text{Number of messages sent}}$$

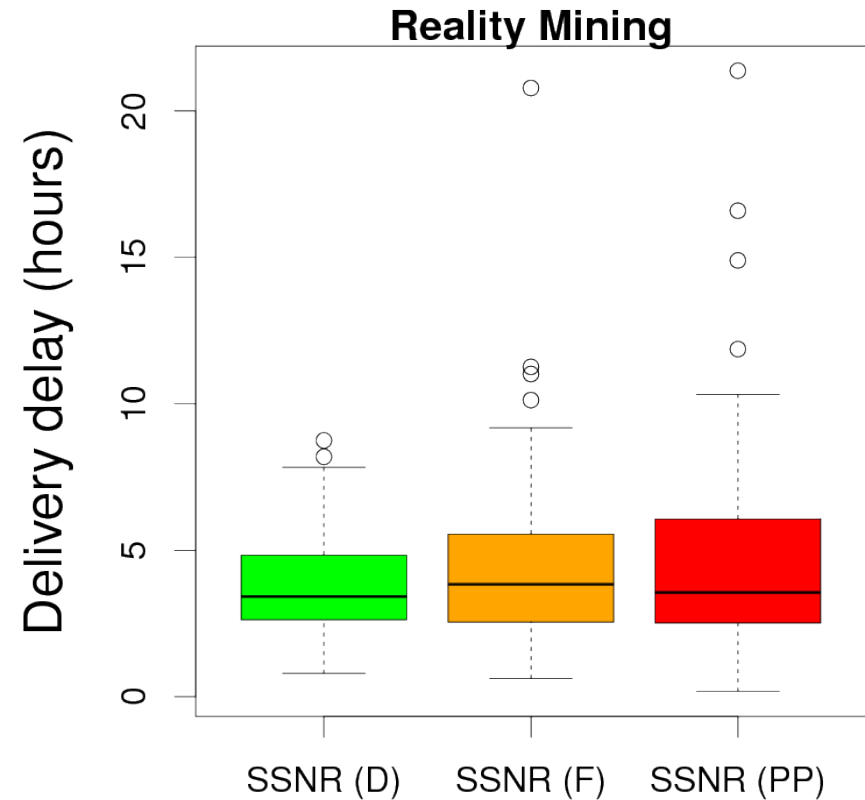
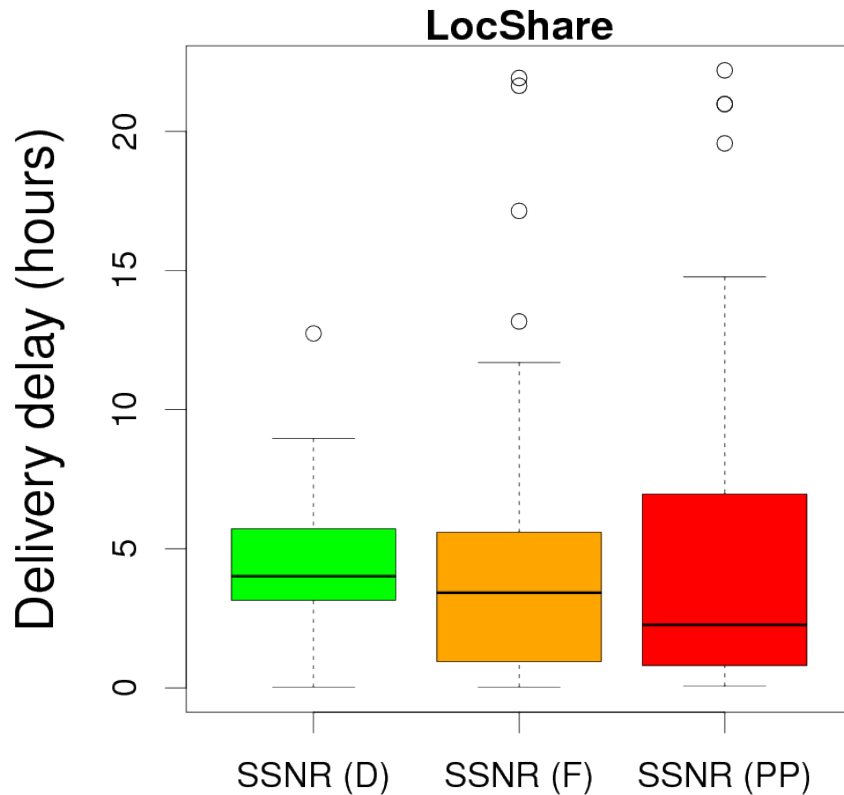
# Results – Delivery Delay (Epid)



## Delivery delay:

For those messages which arrive, the mean time for a message to arrive at destination.

# Results – Delivery Delay (SSNR)



**Delivery delay:**

For those messages which arrive, the mean time for a message to arrive at destination.

# Take home messages

Users' privacy concerns may lead to **dramatically-lower routing performance.**

Need to find ways to **avoid users acting as in the PubPriv mode** (where performance fell to zero) – perhaps by allaying concerns.

# What next?

## Future refinement

- Other **datasets**.
- More sophisticated **privacy models**.
  - Correlation between privacy preference and encounter location?
- **Test assumption**.
  - Privacy behaviour of heavy Facebook users corresponds to opportunistic network users?
- Other **privacy concerns**.

# What next?

## The big picture

- Performance of **privacy-preserving protocols**.
  - Protocols designed to alleviate users' concerns.
  - But this may involve an inherent performance cost.
- **Incentives** to participate
  - Might incentives outweigh privacy concerns, for some or all users?
  - e.g., Altruism, reputation, barter.

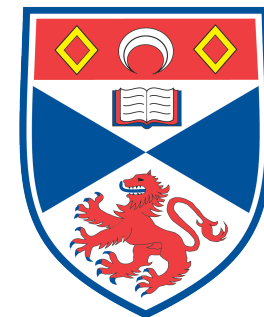
# The impact of location privacy on opportunistic networks

Iain Parris and Tristan Henderson

{isp3,tnhh}@st-andrews.ac.uk

<http://www.cs.st-andrews.ac.uk/~ip/>

<http://www.cs.st-andrews.ac.uk/~tristan/>



University  
of  
St Andrews

# Credits

Images used under the Creative Commons license:

- Bogenfreund – The Mechanic Eye: <<http://www.flickr.com/photos/bogenfreund/1808719569>>
- cobalt123 – SamsungSCH-u740 Cellphone: <<http://www.flickr.com/photos/cobalt/1339314355>>
- Jamison Judd – Server rack: <<http://www.flickr.com/photos/jamisonjudd/2433102356>>
- mujitra – Cyber-shot cellphone "W61S" (2008): <<http://www.flickr.com/photos/mujitra/2723986495>>

Logos:

- Facebook, <<http://www.facebook.com/>>