

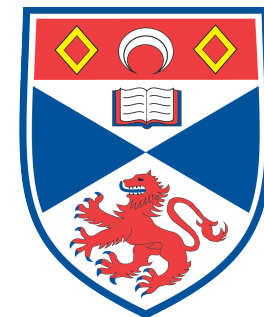
# Practical privacy-aware opportunistic networking

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



“Hello, I am eating a pizza.”

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**.



Overlap of research areas:

- **Networking: routing**
- **HCI: privacy**

# Problem: 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.

# Privacy: social graph

SSNR:

- Message includes the **sender's complete social network** as a message header.
- **Privacy problem:** Everyone who sees the message must know who else is in the sender's social network.



**Google admits Buzz social network testing flaws**

By Jonathan Fildes  
Technology reporter, BBC News

**Google has admitted to BBC News that testing of its controversial social network Buzz was insufficient.**

The firm has had to make a series of changes to the service after a ferocious backlash from users concerned about intrusions of privacy.

The BBC understands that Buzz was only tested internally and bypassed more extensive trials with external testers - used for many other Google services.


Google said that it was now working "extremely hard" to fix the problems.

"We're very early in this space. This was one of our first big attempts," Todd Jackson, Buzz product manager, told BBC News.

"We've been testing Buzz internally at Google for a while. Of course, getting feedback from 20,000 Googlers isn't quite the same as letting Gmail users play with Buzz in the wild."

Many of the firm's new services are tested by the so-called Google Trusted Tester program, a network of friends and family of Google employees who are given confidential access to products before they launch.

Buzz was not tested by this program.



The screenshot shows a user profile for "Ted Tase" with 0 connected sites and 12 followers. Below the profile is a "Welcome to Google Buzz" message stating the user is set up to follow 21 people. A list of 12 people is shown, with a note that 12 people are already following the user. At the bottom, there is a "Following 21 people" link and a "Refresh" button.

**SEE ALSO**

- ▶ Google unveils new social network 09 Feb 10 | Technology
- ▶ Google invites users to join Wave 30 Sep 09 | Technology
- ▶ Strong reception for Google Wave 01 Jun 09 | Technology
- ▶ US calls for China Google probe 21 Jan 10 | Americas
- ▶ Google drops Gmail address in UK 19 Oct 05 | Business
- ▶ Google mobile phone expected 05 Jan 10 | Technology

**RELATED INTERNET LINKS**

- ▶ Google
- ▶ Buzz
- ▶ Facebook
- ▶ Evgeny Morozov' post

The BBC is not responsible for the content of external internet sites

**FROM OTHER NEWS SITES**

- ▶ Guardian.co.uk Green light: Cruel meat, Copenhagen conspiracies and iPhone climate war - 1 hr ago
- ▶ CIO CEO denies Google wants to take on mobile operators - 2 hrs ago
- ▶ Times Online Google forced into Buzz revamp over privacy row - 3 hrs ago
- ▶ New Statesman\* Google advised to make Buzz opt-in service - 4 hrs ago

<http://news.bbc.co.uk/1/hi/8517613.stm>

# Privacy: location



**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/>

# Research questions

- What **privacy concerns** do opportunistic network users have?
- Given the disconnect between what people say and what people do with respect to privacy, how might we **measure users' concerns for systems that do not yet exist?**
- Is it possible to build opportunistic networks that can mitigate users' concerns while maintaining routing **performance?**

Thesis: *It is possible to maintain opportunistic networking performance after adding the privacy-preserving features that users desire.*

# Summary of current results

**Users behave differently when participating in a real system**, compared to a simulated system: more privacy-concerned in real system.

**Users' location-privacy preferences may significantly impact opportunistic-network performance.**

**Significant obfuscation of social-network information is possible**, while maintaining good SSNR performance.

# HCI experiment: the user

We already know that users are concerned about location privacy.

Are they also concerned about **social graph privacy**?



# Planned experiment

Simulated opportunistic network application (*MobiAd* for advertising) runs on participants' personal **Android** smartphones, for one week.

**Half of the participants made aware of threats** to social graph privacy (*encounters*).

Look for **differences in behaviour** between participants.



# Outcome of pilot run

In a pilot run, a minority of users did self-report privacy concerns.

But they did not (seem to) change their application usage.

→ **Plan to make privacy threat more prominent.**



# Some questions for discussion

How can we best present threats to social graph privacy to users?

Should participants interact to differing degrees with the simulated application, then what are the implications for interpretation of the results?

How many participants should take part? And how should they be selected?



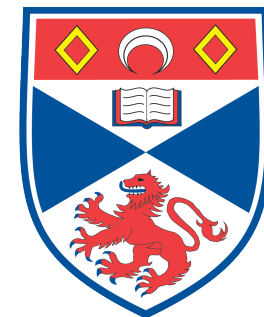
# Practical privacy-aware opportunistic networking

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:

- Anton Fomkin – Duracell battery AA type: <<http://www.flickr.com/photos/antonfomkin/3046002213/>>
- cobalt123 – SamsungSCH-u740 Cellphone: <<http://www.flickr.com/photos/cobalt/1339314355>>
- James Offer – CCTV Heads - d\*base: <<http://www.flickr.com/photos/joffley/135053360/>>
- mujitra – Cyber-shot cellphone "W61S" (2008): <<http://www.flickr.com/photos/mujitra/2723986495>>

Logos:

- Google Buzz, <<http://www.google.com/buzz>>