

## 1. Introduction

Opportunistic networks have been the study of much research – in particular on making end-to-end routing efficient.

Social network information is often exploited in opportunistic network routing, but **simple social network routing schemes broadcast social network information**. This introduces privacy concerns.

We are interested in studying these oft-overlooked inherent **privacy issues**.

### Opportunistic Networks

Mobile devices, such as mobile phones, are commonly carried around by people during their daily lives.

Messages may be **directly exchanged between devices when they are in physical proximity** to each other in an ad-hoc manner.

In this way, an **opportunistic network** may be formed, where people send messages to each other via intermediary devices utilising a **disconnected store-and-forward** architecture.

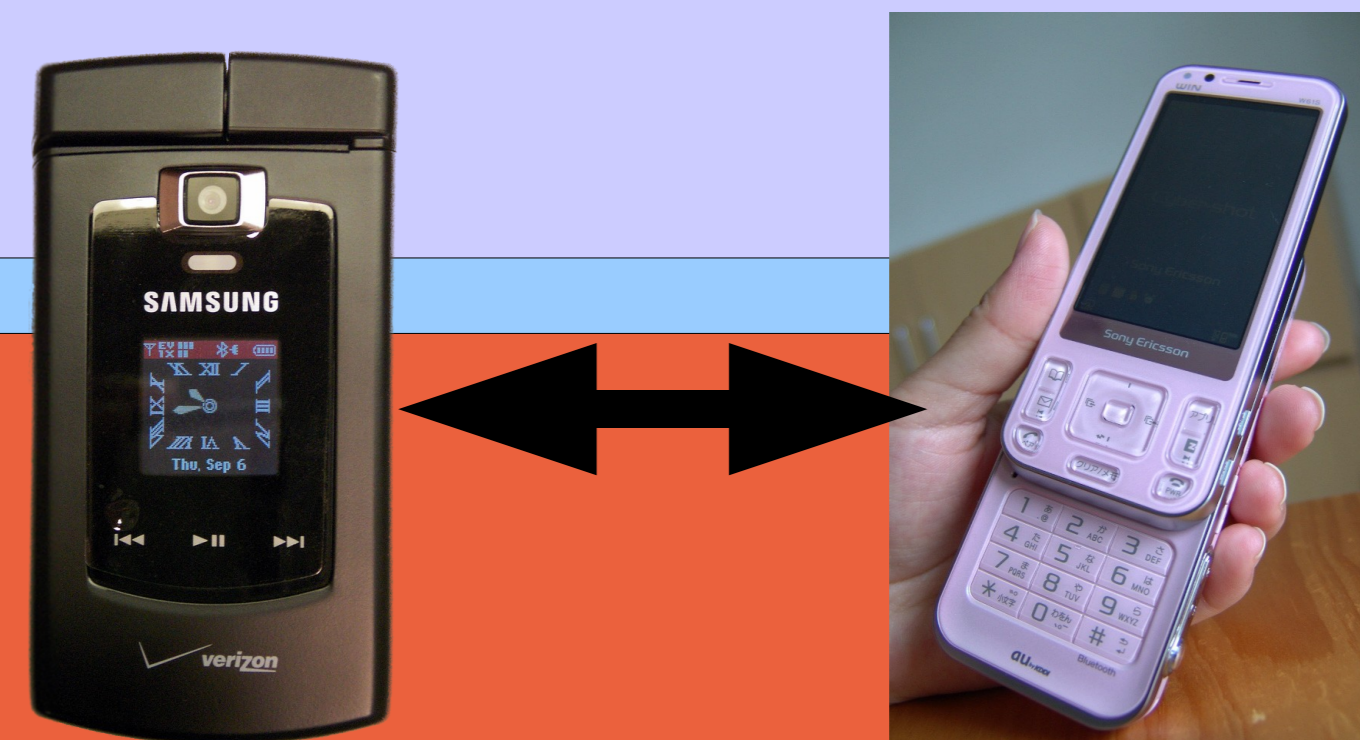


Image credits:  
<http://www.flickr.com/photos/cobalt>  
<http://flickr.com/photos/mujitra>

### Research Questions

Is it **possible to add privacy** features to opportunistic networks without degrading the user experience?

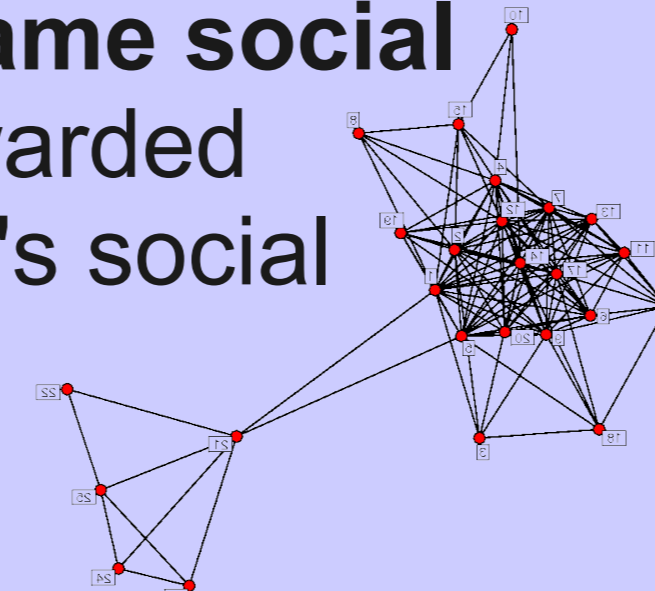
What **privacy concerns** do users have?

How might we **build an opportunistic network that can mitigate users' concerns** while efficiently delivering data?

### Social Network Routing

How can we route messages in an opportunistic network? Flooding messages to all encountered devices would be costly, draining battery life rapidly. Messages should be **selectively forwarded** during encounters.

Making the assumption that **encounters between mobile devices are more likely to occur between people in the same social network**, messages may be forwarded selectively only within the sender's social network.



## 2. Privacy Threats

In simple social network routing, **social network information is broadcast in the clear**. Encrypting end-to-end is not possible because this information is utilised by intermediate nodes to inform their routing decisions.

But what of **privacy**?

Users of the opportunistic network might have an embarrassing friend which they do not wish the world to know about. Or a user may be happy with the social network information informing routing decisions, but not with their whole network being world-viewable: it is one thing for a curious person to be able to infer some of the social network based on forwarded messages, but another to distribute the potentially-sensitive information[2] freely.

### References

- [1] G. Bigwood, D. Rehunathan, M. Bateman, T. Henderson, and S. Bhatti. Exploiting self-reported social networks for routing in ubiquitous computing environments. In *Proc. of the 1st International Workshop on Social Aspects of Ubiquitous Computing Environments (SAUCE 2008)*, pages 484–489, Avignon, France, Oct 2008. DOI 10.1109/WiMob.2008.86.
- [2] L. Backstrom, C. Dwork, and J. Kleinberg. Wherefore art thou r3579x?: anonymized social networks, hidden patterns, and structural steganography. In *Proc. of the 16th International Conference on World Wide Web (WWW 2007)*, pages 181–190, Banff, Alberta, Canada, May 2007. DOI 10.1145/1242572.1242598.
- [3] I. Parris, G. Bigwood and T. Henderson. Privacy-enhanced social network routing in opportunistic networks. In *Proc. of the IEEE International Workshop on Security and Social Networking (SESOC 2010)*, Mannheim, Germany, Mar 2010. To appear.

## 3. Our Privacy-enhanced Routing Schemes

We attempt to target the social network routing privacy threats by **obfuscating a sender's social network**.

### Statisticulated Social Network Routing (SSNR)

For each message transmitted, the sender makes changes to the message's copy of their social network - **adding or removing nodes**. An element of **plausible deniability** is introduced.

### Obfuscated Social Network Routing (OSNR)

Instead of transmitting the sender's social network as a list of nodes, we embed the social network information within a **Bloom filter** (a probabilistic data structure allowing probabilistic querying for set membership). We may regard the Bloom filter itself as a **non-trivially-reversible hash** of this social network information.

## 4. Results

To evaluate the impact of our schemes on opportunistic network performance, we performed trace-driven simulation with two real-world datasets: one collected in a previous experiment (the SASSY dataset[1]), and the well-known Reality Mining dataset collected at MIT. For further details, see [3].

We find that:

(1) It is possible to **obfuscate a sender's social network by removing up to 50% of the nodes** from the social network, while still maintaining a delivery ratio of 90% of unaltered social network routing.

(2) Applying **OSNR** (using Bloom filters) we can prevent eavesdropping of social network information with a **minimal effect on network performance**.

Figure 1: SASSY dataset. Delivery ratio vs target percentage modification of each message sender's social network.

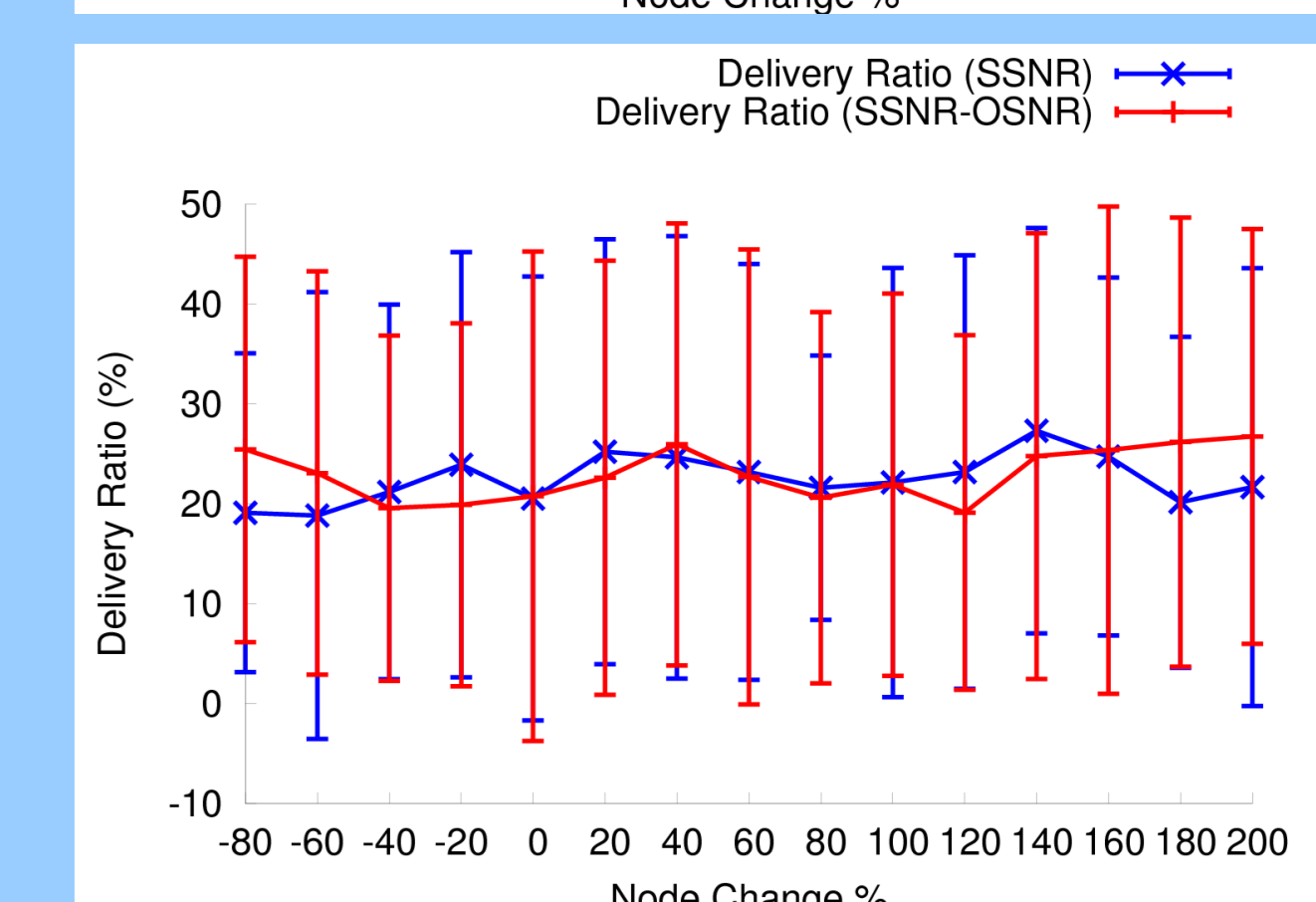
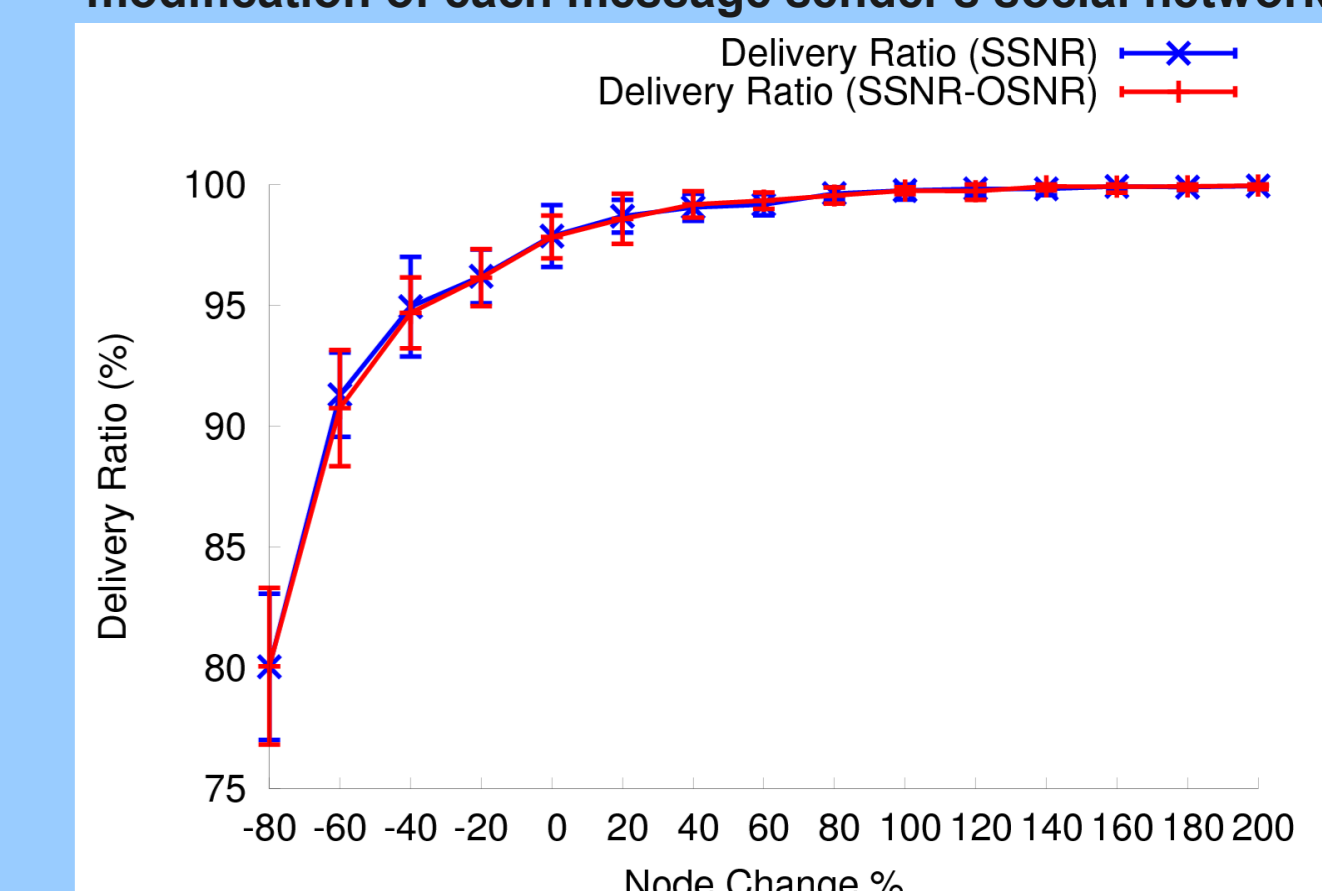


Figure 2: Reality Mining dataset. Delivery ratio vs target percentage modification of each message sender's social network.

## 5. Future Work

Our initial results suggest that it is possible to add privacy-enhancing features to social network routing in opportunistic networks (though we are actively looking for more datasets to further evaluate our schemes).

To explore what privacy users actually want, we are planning a user study. We intend to simulate opportunistic network applications using Facebook, which is widely used and provides access to a wealth of real social network data. Participants will carry sensor-equipped smartphones tied to a custom Facebook application. We will ask users in various contexts what information they would be comfortable publishing via Facebook, and to whom.

We hope to gain understanding of users' privacy concerns in different contexts, and to use this new understanding to inform opportunistic network design. We are working towards creating a social network routing protocol which may dynamically adapt to users' privacy requirements.